



Comodo Client - Security for Linux

Software Version 2.2

User Guide Guide Version 2.2.070219

> Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Client - Security for Linux	4
1.1.Features	6
1.2.System Requirements	6
1.3.Install Comodo Client - Security for Linux	6
1.4.Start CCS for Linux	14
1.5.Understand CCS Alerts	16
2.The Summary Screen	17
3. Antivirus Tasks - Introduction	19
3.1.Run a Scan	
3.2.Update Virus Database	27
3.3.Scheduled Scans	
3.4.Quarantined Items	
3.5.Scan Profiles	
3.6.Scanner Settings	
3.6.1.Real Time Scan	
3.6.2.Manual Scan	
3.6.3.Scheduled Scan	
3.6.4.Exclusions	
4. More Options - Introduction	
4.1.Preferences	44
4.1.1.Language Settings	
4.1.2.Log Settings	
4.1.3.Connection Settings	
4.1.4.Update Settings	
4.1.5.External Device Control Settings	50
4.2.Manage My Configurations	54
4.2.1.Comodo Preset Configuration	54
4.2.2.Import /Export and Manage Personal Configurations	
4.3.Diagnostics	62
4.4.View Antivirus Events	63
4.4.1.Log Viewer Module	64
4.4.1.1.Antivirus Logs	65
4.4.1.1.1.Filter Antivirus Logs	67
4.4.1.2.Device Control Logs	69
4.4.1.2.1.Filter Device Control Logs	71
4.4.1.3.'Alerts Displayed' Logs	72
4.4.1.3.1.Filter 'Alerts Displayed' Logs	73
4.4.1.4.'Tasks Launched' Logs	76
4.4.1.4.1.Filter 'Tasks Launched' Logs	
4.4.1.5.Configuration Change Logs	81
4.4.1.5.1.Filter 'Configuration Change' Logs	82
4.5.Browse Support Forums	

4.6.Help	
4.7.About	
Appendix 1 - CCS for Linux How To Tutorials	88
Scan your Computer for Viruses	
View Antivirus Events	94
Configure Database Updates	
Quickly Set up Security Levels	
Change CCS Language Settings	
Run an Instant Antivirus Scan on Selected Items	
Create a Scheduled Scan	
Restore Incorrectly Quarantined Item(s)	
Switch off Automatic Antivirus Updates	
Control External Device Accessibility	
About Comodo Security Solutions	

COMODO Creating Trust Online

1. Introduction to Comodo Client - Security for Linux

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

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

Features

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



Guide Structure

Click the links below to jump to the section that you need help with. Introduction - An overview of Comodo Client - Security for Linux.

Features



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

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

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

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

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

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

Appendix 1 CCS for Linux How to... Tutorials

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



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

1.1. Features

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

1.2. System Requirements

Supported Operating Systems

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

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

1.3. Install Comodo Client - Security for Linux

- The section describes how to use Endpoint Manager (EM) to deploy Comodo Client Security (CCS) on your Linux endpoints.
- You can purchase EM as stand-alone application or as a part of the Comodo One (C1) / ITarian suite.

This section covers how to:

- Subscribe for Endpoint Manager
- Enroll users
- Add devices
- Deploy CCS on Linux endpoints

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

Subscribe for Endpoint Manager

You can purchase Endpoint Manager as stand-alone application or as part of the Comodo One (C1) / ITarian suite:

• C1 / ITarian

Comodo Client - Security for Linux User Guide | © 2019 Comodo Security Solutions Inc. | All rights reserved.



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

Enroll Users

You can only deploy CCS to endpoints after adding users to Endpoint Manager.

- Comodo One/ITarian users You can create multiple companies in the C1/ITarian interface, and can enroll
 users to any of these companies.
- Endpoint Manager Users 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'.

Endpoint Manager	≡ User List	e ي 🔁
DASHBOARD		Create User
DEVICES		Enroll Device
(A USERS	Enroll Device Creat Hiser Manage	
User List	NAME	
User Groups		
Role Management	johnsmith	

The create user form will open:

COMODO Creating Trust Online*

Create New User	×
User Name*	
John	
Email*	
fiatliena@gmail.com	
Phone Number	
Phone Number	
Company"	
Star Inc.	•
Assign Role	
Users	٠
Submi	

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Company The organization to which you want to add the user.
 - C1 MSP / ITarian MSP users The drop-down shows all companies you have added to C1/ITarian. Choose the company under which you want to enroll the user.
 - All other users Leave the selection as 'Default Company'. This includes stand-alone Endpoint Manager customers, and customers of the 'Enterprise' versions of C1/ITarian.
- Assign Role A role determines user permissions within the Endpoint Manager console itself. EM ships with two default roles:
 - Administrator Full administrative privileges in the Endpoint Manager console. The permissions for this role are not editable.
 - User In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

A confirmation message is shown:

COMODO Creating Trust Online*



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

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

Enroll Devices

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

Enroll devices

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

Enroll Device Create User Manage Profiles	Send Pa Recover
NAME	EMAIL
John aueen@voomail.com	fiatliena@o



COMODO Creating Trust Online

You will next send out device enrollment instructions to the users you selected:

Enroll Devices	×
Please choose the device owner(s)	
Show Enrollment Instructions	Email Enrollment Instructions

The 'Enroll Devices' screen opens, pre-populated with the users you selected:

- You can add more users by typing the first few letters of their username and choosing from the suggestions.
- **Show Enrollment Instructions** Displays enrollment advice in a pop-up. Useful for admins who want to enroll their own devices.
- Email Enrollment Instructions Will send device enrollment instructions to all selected users. Users
 must enroll their own devices by following the instructions in the email. The following confirmation is
 shown after clicking this button:

Enroll Devices	×
Instruction email has been sent to selected user(s). The user should navigate to the a device that is going to be enrolled.	link on
Show Enrollment Instructions	Ok

An example mail is shown below:

COMODO Creating Trust Online*

Endpoint Manager

Welcome to Endpoint Manager!

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

Note:

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

Device Enrollment:

Click this link to enroll your device

Sincerely, Endpoint Manager team.

- Users must open the mail on the device itself. They need to click the enrollment link to register their device.
- The user is then taken to a web page containing the agent download link.
- Click the enroll link under 'For Linux Devices' and save the setup file.

COMODO



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

NOTE:

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

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

5 FOR LINUX DEVICES

Download and install Communication Client by tapping the following link:

https://saddle_and_pedals-herculespopular-msp.cmdm.comodo.c om:443/enroll/linux/run/token/1af023ed02699f6fe25c06e96dd8e6 c8

Use the same link for manual enrollment if required.

1) Change installer mode to executable:

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

Use the command terminal to install the agent. Change installer mode to executable and run the installer with root privileges, as follows:

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

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

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

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

For example:

chmod +x itsm_TNZgu2FL_installer.run sudo./itsm_TNZgu2FL_installer.run

COMODO Creating Trust Online*



That's it. The device is enrolled and listed in 'Devices' > 'Device List'. The next step is to **install CCS** onto the endpoint.

Background note on the agent:

- The agent is a small application installed on endpoints to facilitate communication between the endpoint and the Endpoint Manager server.
- The agent receives tasks from Endpoint Manager and passes them to Comodo Client Security.
 - Example tasks include run a virus scan, update the antivirus database, change the security policy, or generate a report.
- For security reasons, agents can only communicate with the instance of Endpoint Manager which provisioned the agent. This means the agent cannot be reconfigured to connect to any other Endpoint Manager service.

Deploy Comodo Client Security

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

Install CCS

- Log into Comodo One / ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
 - Click the funnel icon on the right and select 'Linux', to see only Linux endpoints
 - Click 'All Devices' to view every device in Endpoint Manager
- · Select your target Linux devices using the check-boxes on the left

COMODO Creating Trust Online

Click 'Install or Update Packages':

.

, <mark>1</mark> 8	Gro	up Management	Device	Management	Discovered	Devices BETA							
æ			12	2	20	Ē,		Q	5	1	2		
Enroll De	vice	Remote Control	File Transfer	Remote Tools	Run Procedure	Manage Profiles	Install or Update Packages	Refresh Inform	Device ation	Reboot	Owner	More	
р s	earch	n for devices					Install Addit	ional Como	odo Pa ckage:	ickages s	0	0	
	0S	NAME		ACTIVE COMPO	NENTS PA	TCH STATUS	Install mac0	S Package	25		VITY		
Ο	٥	comodo	F	AGAV		(Install Linux Update Addi	Packages tional Pacl	kages		05:11:53 PM		
		e comodo	L	AGAV			Saddle and	comodo	ġ3	2019/05/09	05:11:44 PM		
	1	DESKTO	u 🤹	AG (AV) FW (0 8	2	Saddle and	DESKT	ō,	2019/05/02	05:28:24 PM		
		DESKTO	- 😲	AG CCS		1	herculespop	DESKT					

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

Install Linux Packages	×
Install COMODO Client - Security	
	Install

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

The application will become effective immediately after installation.

- You can configure CCS settings in the Endpoint Manager profile which is applied to the endpoint.
- See https://help.comodo.com/topic-399-1-786-12989-Profiles-For-Linux-Devices.html for more details on this.

1.4. Start CCS for Linux

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

There are three ways you can open the interface:

- Applications Menu
- Desktop Menu

COMODO Creating Trust Online*

Dock Icon

Applications Menu

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



The applications menu provides shortcuts to:

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

Desktop Menu

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



Dock icon

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



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



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

1.5. Understand CCS Alerts

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

Antivirus Alert				
A malicious item has been detected!				
Name:	TroiWare HTML Iframe v@286974125			
Name.	Indjware.html.iname.x@200914125			
Location:	/home/tester/Documents/test se			
More information: Unavailable				
How should I answer?				

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

Answer an antivirus alert

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

You can clean the threat or ignore it:



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

Antivirus Ale	ert	
	A malicious item has been detected!	
Name:	TrojWare.JS.TrojanDownloader.A	
Location: /home/tester/Documents/test se		
More informat	ion: Unavailable	
How should	I answer? 😵 Clean 🔂 Ignore 🔻	
	Once Add to Exclusi	ions

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

Antivirus Notification

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

COMODO Client - Security /	Alert	
Malware@#13tm1ukrdwdg0		
malware found and stopped		
/home/comodo/Downloads/2409fb21fe377f7		
Hide these alerts	Close	

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

2. The Summary Screen

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

COMODO

😕 🗐 🗊 COMODO Client - S	ecurity for Linux		
COMODO	Summary	S Antivirus	More
V	Antivirus The virus databa	On Access se has been updated on Fri May 10 13:35:17 19 detected so far	,
All systems are active and running.			
		Scan Now	
	D	prop files here to scan by virus scanner	
	D	brop files here to scan by virus scanner	

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

The summary screen contains the following information:

1. System Status

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

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

2. Antivirus

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

- **On Access:** Real-time virus protection is enabled. All files you open or download are scanned before they are allowed to open.
- **Disabled:** Real-time protection is switched off. Click the status link to configure real-time protection.

See Scanner Settings for more help with this area.

Database Updates

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

Number of Detected Threats

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



screen.

Scan Now

- Click the 'Scan Now' link to start a virus scan.
- 3. Scan Box
 - Drag any file, folder or drive into the box to run an instant virus scan on it.
 - The results screen has controls that let you deal with any identified threats.

3. Antivirus Tasks - Introduction

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



Background - How antivirus scans work

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

Tip: The logs area contains a record of all virus events, tasks, scans and configuration changes. Click 'More' > 'View Antivirus Events' to open it. See **View Antivirus Events** if you need help.

COMODO Creating Trust Online*

The following sections explain more about each task:

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

3.1. Run a Scan

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

Run an on-demand virus scan

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

My Computer Predefined Critical Areas Predefined Suspicious Files User	Profile t	Profile name
Critical Areas Predefined	Predefined	1y Computer
Suspicious Files User	Predefined	ritical Areas
ober ober	User	uspicious Files
Media Files User	User	1edia Files

Choose one of the following options:

Profile name - A scan profile defines the folders, drives or areas that are covered by the scan.

CCS ships with two pre-defined scan profiles - 'My Computer' and 'Critical Areas'. These cannot be edited or removed:

- My Computer Scans every drive, folder and file on your system, including external connected devices
- Critical Areas A targeted scan of important operating system files and folders.
- Profile type Shows whether the profile is predefined (created by Comodo) or user-defined.
- Create New Scan Create your own custom scan of specific files, folders or drives.

COMODO Creating Trust Online*

Click 'Scan' after making your selection.

Custom Scan

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

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

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

Scan Progress and Results

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

🐵 Virus Database Update (90%)	
Please wait while the virus database is being updated. This might take a few minutes	
Finalizing	
90%	
What do these settings do? Hide	

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

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

COMODO Creating Trust Online*

🙆 🖨 Scanning: My Computer	
Scanning: My Computer Status: /usr/include/stdio.h	
Objects Scanned: 3742	Start Time: Mon Aug 20 12:03:13 2018
Threats Found: 0	Duration: 00:00:26
X Show on top	
What do these settings do?	Pause Stop Scan
 Click 'Pause' to suspend the scan Click 'Resume' to recommence the scan Click 'Stop Scan' to abort the scan altogether. Results are shown at the end of the scan:	
😢 😑 Scanning: My Computer - Complete	ed
Scanning: My Computer Status: Scan Completed	
Objects Scanned: 157561	Start Time: Mon Aug 20 12:03:13 2018
Threats Found: 3	Duration: 00:08:50
Show on top	
What do these settings do?	Results
 Click the 'Results' button to see detailed file inform 	nation.

• The results window lists all threats discovered by the scan and provides controls which let you deal with the them:

Comodo Client - Security for Linux User Guide | © 2019 Comodo Security Solutions Inc. | All rights reserved.

COMODO

🖉 All ?	 Threat Name 	Risk
,	ApplicUnsaf@#1dkvp9e72akc	- Low
\checkmark	/home/tester/Documents/test_set/b93a5bb200a87b9728f949ffe10c68fcb93a5bb20	
,	ApplicUnwnt@(#2tplrp9u1mcvu, #2oto6pyf1czwd)	- Low
\checkmark	/home/tester/Documents/test_set/c12a5bbe438820ee42915e3ebdde0bd9	
\checkmark	/home/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39	
,	Application.Win32.Agent.BUNE@318931415	- Low
\checkmark	/home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511	
\checkmark	/home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6	
*	Application.Win32.Agent.Z@306475545	- Low
\checkmark	/home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc	
7	Application.Win32.Bundlore.C@321284137	- Low
\checkmark	/home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f	
\checkmark	/home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232	
7	Application.Win32.IBryte.X@318641596	- Low
\checkmark	/home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229	
r	Application.Win32.InstalleRex.DP@362046738	- Low
\checkmark	/home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b	
-	Application.Win32.Multiplug.GETF@323611884	- Low
\leq	/home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba	
·	Backdoor.HTML.EMO.E@283889604	High
\leq	/home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34	
\checkmark	/home/tester/Documents/test_set/671ff798d81f9540c4e1e8ba0372112e671ff798d8	
	/hama/tastas/Dacumaats/tast_sat/04s433h0h341a371h7fE1140ahf30303	
What d	these settings do? Save Results Clean Ignore	Close
	Once	2
	bbA	to Evolusions

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

Create a Scan Profile

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

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

COMODO Creating Trust Online*

at do these settings do?	Create New Sc	an Scan	Clo
😣 Scan Profile	******		95959595959595959
Name:			
List of items to be scanned:			
Path			7

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

COMODO Creating Trust Online*

			+
xisting items			Selected items
Name	Size Type Drive Folder Fol	->	

You can add items in two ways:

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

COMODO Creating Trust Online

😣 Scan Profile	
Name:	
Weekly Custom Scan Profile	
List of items to be scanned:	
Path /usr/share/misc/ /proc/11/map_files/	
	Add Remove
What do these settings do?	Apply Cancel

Click 'Apply' in the scan profile dialog

•

Profile nam	ie 🗸 🗸	Profile type
My Computer		Predefined
Critical Areas		Predefined
media plus		User
Weekly Custom Scan Profile		User
Suspicious Files		User

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

COMODO Creating Trust Online*

Instantly Scan Objects

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

🙆 🖨 🗇 COMODO Clien	t - Security for Linux			XA-
COMODO Client - Security	Summary	8 Antivirus	o More	A
V	Antivirus of The virus databa	On Access ase has been updated on Mon Aug 2 detected so far	7 08:23:09 2018	JJ mp3
All systems are active and running.		.	Scan Now	
		Drop files here to scan by virus scann	er .	

3.2. Update Virus Database

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

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

- Download update manually
- Download update automatically

Manually check for and download the latest updates

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

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

The following notifications are shown during the update process:

😣 Virus Database Update (90%)	
Please wait while the virus database is b This might take a few minutes Finalizing	eing updated.
90%	
What do these settings do?	Hide



CCS shows a warning on the home-screen if the database has not been updated for a long time.

Automatic updates

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

3.3. Scheduled Scans

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

See the following help to create a schedule in CCS:

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

Create a scheduled scan

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

COMODO Creating Trust Online*

8 Scheduled Scans	
Schedule Name	Add
Weekly Virus Scanning	
	Edit
	Remove
	J
What do these settings do? Apply	Cancel

Configure your schedule in the following settings screen:

•

😣 Scan Schedule	
Name:	
Profile:	
My Computer	-
Days of the week:	
🗙 Monday	
🗙 Tuesday	
🗙 Wednesday	
🗙 Thursday	
🗙 Friday	
🗙 Saturday	
🗙 Sunday	
Start time:	12:00 AM 🗘
	Apply Cancel

- Name Enter a label for the new schedule. E.g. 'Daily scan of external devices'
- Profile The profile determines which areas of your computer are scanned. 'Full Scan' and 'Quick



Scan' are the default options. You can also create your own profile of specific targets.

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

Scheduled Scans	
Schedule Name	
Weekly Virus Scanning Weekly Custom Schedule	Edit
	Remove
What do these settings do?	Apply Cancel

Repeat the process to create more scan schedules.

Edit a scheduled scan

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

Remove a scheduled scan

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

3.4. Quarantined Items

- 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.

The quarantine interface lets you:

- View quarantined items
- Manually quarantine files
- Delete quarantined items from your computer

COMODO Creating Trust Online*

- Restore a quarantined item
- Delete all quarantined items

View quarantined items

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

Quarantined Items

Item 🗸	Location	Add
TrojWare.VBS.StartPage.mh@285031810 TrojWare.JS.Agent.rm@283500528 TrojWare.HTML Iframe.y@286974125	/home/tester/Docum /home/tester/Docum /home/tester/Docum	Delete
Malware@#3pnqisdffm6ml Exploit.JS.Pdfka.cljk@279346659	/home/tester/Docum /home/tester/Docum	Restore
Backdoor.PHP.Pbot.A@189232624	/home/tester/Docum	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 CCS > Click 'Antivirus' > 'Quarantined Items'
- Click 'Add'
- Browse to the file you want to quarantine and click 'Open'

Delete quarantined items from your system

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

This deletes the file from your computer permanently.

Restore a quarantined item to its original location

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



Permanently delete all quarantined items

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

This deletes all quarantined items permanently.

3.5. Scan Profiles

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

Open the Scan Profiles interface

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

👂 Scan Profiles

Profile Name	Profile type 🖉	Add
Critical Areas	Predefined	Edit
My Computer	Predefined	Luita
		Remove

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

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

The following sections explain how to:

- Create a scan profile
- Edit a scan profile



• Remove a custom scan profile

Create a new scan profile

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

🤕 Scan Profile	
Name:	
Custom Profile	
List of items to be scanned:	
Path	6
	Add Remove
What do these settings do?	Apply Cancel

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

COMODO Creating Trust Online*

		+
xisting items		Selected items
Name Siz	ze Type Drive Folder	

There are two ways to add scan locations:

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

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

COMODO Creating Trust Online*

Prorite Name	Profile type 🛆 🛛 Ad	d
Critical Areas	Predefined	iŀ
My Computer	Predefined	IC
Custom Profile	User	nove

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

😣 Scan Schedule	
Name:	
Profile:	\sim
My Computer Critical Areas	Ċ
Custom Profile	
Wednesday	
X Thursday	
× Friday	

Edit a custom scan profile

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

Remove custom scan profiles

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



- Click 'Scan Profiles'
- · Select the profile you want to remove from the list and click 'Remove'

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

3.6. Scanner Settings

• Click 'Antivirus' > 'Scanner Settings'

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

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

Open Scanner Settings

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

	Manual Scanning	Scheduled Scanning	Exclusions	
Real-Time Scanning On Access	3			
	- Real-ti - Everyt - Threat do any h	me scanner is enabled hing is scanned on-acco s are going to be deteo harm	ess tted before they	/ car
Disabled				
Automatically u	update virus databa	se ound during scanning		
 Automatically of the second sec				
 Automatically of Show notificati Heuristics Scannin 	on messages g Level	Low		
 Automatically of Show notification Heuristics Scannin Do not scan files lateral 	on messages g Level arger than (MB)	Low -		

Antivirus settings are broken down into the following areas:

- Real Time Scan Configure the 'always-on' virus monitor
- Manual Scan Configure on-demand scans


- Scheduled Scan Configure a scan schedule
- Exclusions View and manage items which will be skipped by virus scans.

3.6.1. Real Time Scan

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

Configure real time scan settings

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

•	Virus Scanner Se	ttings								
	Real Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions						
	Real-Time Scanning	I								
		- Real-time scanner is enabled - Everything is scanned on-access - Threats are going to be detected before they can do any harm								
	Disabled									
	Detection									
	X Automatically u	ipdate virus databa	se							
	X Automatically of X Show potification	juarantine threats f	ound during scanning							
1000 - 1000 -	Heuristics Scanning	g Level	Low							
0.000	Do not scan files la	rger than (MB)	20							
	Keep an alert on th	ne screen for (secor	nds) 120							
	What do these set	tings do?		OK Cancel						

Real-Time Scanning

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

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

Detection Settings

 Automatically update virus database - CCS checks for and downloads the latest database at system start-up and regular intervals thereafter (*Default = Disabled*).

However, some people like to have control over what gets downloaded and when it gets downloaded Automatic updates may be inconvenient if you have a slower connection, or have many downloads going at the same time. Network admins may not want automatic downloads because they take up to much bandwidth during the day.

If you disable this option then you need to periodically select 'Update Virus Database'.

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

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

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

3.6.2. Manual Scan

- Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning'.
- Note: Managed endpoints scanner settings should be configured in an Endpoint Manager profile.

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

COMODO Creating Trust Online*

used when:

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

Configure manual scan settings

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

😣 Virus Scanner Se	ttings		
Real Time Scanning	Manual Scannin	g Scheduled Scanning	Exclusions
Detection Scan archive file	es (e.g. *.zip, *.rar)	
 Automatically u Enable cloud sci 	pdate virus datal anning	base before scanning	
Heuristics Scanning	g Level	Low	
Do not scan files la	arger than (MB)	20	
What do these set	tings do?		OK Cancel

- Scan archive files The scan will include compressed file formats such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (*Default = Enabled*).
- Automatically update virus database before scanning Check for and download the latest virus signature database prior to running a scan (*Default = Enabled*).
- Enable cloud scanning Improves scan accuracy by augmenting the local scan with an online lookup of Comodo's latest virus database. Cloud Scanning means CCS can detect the latest malware even if your database is out-dated. (*Default = Disabled*).
 - Note This setting needs to be enabled if you want to submit unknown files to Valkyrie for analysis. Valkyrie is configured in an Endpoint Manager profile.
- Heuristics Scanning Level Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly

matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the virus database.

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

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

3.6.3. Scheduled Scan

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

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

• Note: Managed endpoints – scanner settings should be configured in an Endpoint Manager profile. **Configure schedule scan settings**

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

COMODO Creating Trust Online*

al Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions
Detection			
 Scan archive file Automatically q Automatically u Show scanning Enable cloud scan 	es (e.g. *.zip, *.rar) uarantine threats fo pdate virus databas progress anning	ound during scanning se before scanning	
Heuristics Scanning	g Level Lo	ww	
Do not scan files la	arger than (MB) 20		

The detection settings are as follows:

- Scan archive files The scan will include compressed file formats such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives. (Default = Enabled).
- Automatically quarantine threats found during scanning Whether or not CCS should automatically take action against malware found by the scan. (Default = Disabled)
 - **Enabled** = CCS moves detected malware into an encrypted holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system.
 - Click 'Antivirus' > 'Quarantined Items' to review quarantined files. You can restore items to their original location or permanently delete them.
 - Disabled = CCS shows a results screen at the end of the scan. The results screen lists all threats discovered by the scan and provides controls for you to deal with them. See Scan Progress and Results screen in Run a Scan for more details.
- Automatically update virus database before scanning Check for and download the latest virus database prior to running a scan. (*Default = Enabled*).
- Show scanning progress A progress bar is shown on start of a scheduled scan. Clear this box if you do not want to see the scan progress status. (*Default = Enabled*).
- Enable cloud scanning Improves scan accuracy by augmenting the local scan with an online lookup of Comodo's latest virus database. Cloud Scanning means CCS can detect the latest malware even if your virus database is out-dated. (*Default = Enabled*).
 - Note This setting needs to be enabled if you want to submit unknown files to Valkyrie for analysis. Valkyrie is configured in an Endpoint Manager profile.

• Heuristics Scanning Level - Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the virus database.

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

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

3.6.4. Exclusions

- Click 'Antivirus' > 'Scanner Settings' > 'Exclusions'.
- The exclusions area shows files and paths that you have chosen to skip during virus scans.
- CCS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.
- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.
- Use this interface to add or remove exceptions.

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

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

COMODO Creating Trust Online*

leal Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions
Exclusions /opt/COMODO/C			Remove
What de these set			

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



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

Click 'OK' to register your exclusions.

COMODO Creating Trust Online*

4. More Options - Introduction

The 'More' area lets you configure various program settings, view event logs and diagnostics, and more.



The following sections explain about each option in detail:

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

4.1. Preferences

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

			P	references	
Language	Logging	Connection	Update	Device Control	
Language:		English(I	Jnited Sta	tes) - Default	

Click the following for more information:

- Language
- Logging
- Connection
- Update
- Device Control

4.1.1. Language Settings

• Click 'More' > 'Preferences' > 'Language'.

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

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

Configure interface language for CCS

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

COMODO Creating Trust Online*

			Р	references			
Language	Logging	Connection	Update	Device Control			
Language	:	English(U 中文(简体 中文(简体 中文(繁麗 Русский Türkçe - Гволгарс Българс Čeština (Jnited Sta Jnited Sta I) - By COI - By COM By COMO By COMO y Commu ès (Brasil) ки - By Co - By Comn Czech) - B	ates) - Default tes) - Default MODO MODO ODO DO noity - By Community mmunity nunity y Community			
What do	these sett	ings do?			(ОК	Cancel

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

4.1.2. Log Settings

- Click 'More' > 'Preferences' > 'Logging'.
- Logs are a record of antivirus events. For example, a log entry is created when CCS detects a piece of malware.
- CCS logs all events by default. You can view the logs themselves in 'More' > 'View Antivirus Events'.
 - Note: Managed endpoints log settings should be configured in an Endpoint Manager profile.

The log settings area lets you:

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

Configure logging settings

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



			P	references
Language	Logging	Connection	Update	Device Control
Logging op	otions allow	w you to mana	ge record	ing of critical events like malware events, etc.
¥ Write to) Local Log) Syslog Se	Database (CC rver (CEF Forn	MODO Fo	ormat)
Host Write to) Log File (CEF Format)		Port 514
Path				Browse
Log fil	e managm	ent		
When log f	ile reache	s 100 M	В	
 Keep or 	updating	it removing th	ie oldest r	ecords
O Move it	to <u>the sp</u>	ecified folder	and start	new one
What do	these sett	ings do?		OK Cancel

General Log File Options

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

Log File Management

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

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



			P	references	8
Language	Logging	Connection	Update	Device Control	
Logging o	ptions allow	w you to mana	ge record	ing of critical even	ts like malware events, etc.
× Write to	o Local Log	Database (CC	MODO Fo	ormat)	
Write to	o Syslog Se	rver (CEF Forn	nat)		
Host				Port 5	14
Write to	o Log File (CEF Format)			
Path				Brows	se
— Log fi	e managm	ent			
When log	file reache	s 100 M	В		
О Кеер о	n updating	it removing th	ne oldest r	ecords	
• Move it	to <u>/home</u>	e/susan/como	do/Log Ard	chive and start new	wone
😵 <u>What do</u>	these sett	ings do?			OK Cancel

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

• Click 'OK' to save your settings.

4.1.3. Connection Settings

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

Configure proxy connection settings to receive virus signature database updates

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



			P	references	
Language	Logging	Connection	Update	Device Control	
Use htt	р ргоху				
Server:				Port:	
Proxy s	erver requi	res authorizat	ion		
Login:				Password:	

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

4.1.4. Update Settings

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

The update area lets you:

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

Configure update settings

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

COMODO Creating Trust Online*

			P	references	
anguage	Logging	Connection	Update	Device Control	
Enable	Host http:	//download.cc	modo.cor	n	Add
					Remove
					Move Up
					 Move Dowr
What do	these sett	ings do?			OK Cancel

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

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

- Download the setup file from https://drive.google.com/file/d/0B4gKr5xfENWBS0FOUHM2VDFQMnc/view.
- Run the setup file on a Windows server and follow the wizard to install the application
- Ensure that the service has started:
 - 'Run' > Enter 'services.msc' > locate 'Apache2.2'
 - Click the 'Start' link on the left if the service is not running

To add a host

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

4.1.5. External Device Control Settings

- Click 'More' > 'Preferences' > 'Device Control'
- Device control lets you block access to external devices like USB sticks and external drives.

COMODO Creating Trust Online*

 You can also define exclusions for selected devices. The selected devices will be allowed to connect, but all others will be blocked.

Configure device control

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

		Р	references			•
Language Log	ging Connection	Update	Device Contro	ol		
Enable Devic This optio Log detected Exclusions	e Control n blocks devices of a l devices	client com	outer from acces	sing, such as US	5B Storage	devices
Devi	ce Name	/Ide	ntification			Add • Edit Remove
What do these	settings do?				OK	Cancel

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

Add exclusions

You can specify the exceptions in two ways:

- Select from currently connected devices
- Specify a custom device

Connect a device then create an exclusion for it

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

• Make sure the external device is connected to the computer



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

			P	references	, (
guage	Logging	Connection	Update	Device Control	
Enable I This	Device Cor	ntrol cks devices of a	client com	outer from accessing, such as USB	Storage devices
.og det	ected devi	ces			
lasions	Device Na	ame	/ Ide	ntification	Add Existing dev
Device	Name		S	select devices	
× v	150w			usb\VID03f0&PID7d	40\E60072816EFE3A39

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

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

COMODO Creating Trust Online*

anguage	Logging	Connection	Update	Device Control	
Enable This Log del	Device Con s option bloc tected devi s	ntrol cks devices of a ces	client com	outer from accessing, such as USB Storage devices	
	Device Na	me /		Identification Add	
v150w	I		usb\VI	003f0&PID7d40\E60072816EFE3A39 Edit	
				Remove	e

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

Specify custom devices to be excluded

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

			P	eferences			8
anguage	Logging	Connection	Update	Device Control			
Enable This × Log det	Device Cor option bloce ected devi	ntrol cks devices of a ices	client com	outer from accessing, such	1 as USE	B Storage de	evices
exclusions							
	Device Na	ame	/ Ide	ntification		[Add -
							Existing device
							Custom device
			Ac	d Custom Device		«	
		Enter device	identifica PID \	or (e.g. usb\VIDxxxx&F	IDxxx	x\serial)	
		What do the second s	nese settir	gs do? App	ly	Cancel	

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

4.2. Manage My Configurations

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

Configurations

My Configurations 🗸 🗸 Active	Activate
COMODO Client - Security Active	Remove
	Import
	Export
What do these settings do?	Close

See the following sections for more details about:

- Comodo Preset Configurations
- Import / Export and Manage Personal Configurations

4.2.1. Comodo Preset Configuration

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



COMODO Creating Trust Online*

	Setting	Value
Langua	age	English (US)
Loggin	g Settings:	
•	Write to Local Log Database	Enabled
•	Write to Syslog Server (CEF Format)	Disabled
•	Write to Log File (CEF Format)	Disabled
•	Maximum log file size	100 MB
•	Log file size action	Keep on updating it removing the oldest records
Conneo	ction Settings:	
•	Use http proxy	Disabled
Update	Settings:	
•	Update Server	http://download.comodo.com
	Scanner Setting	S
Realtim	ne Scanning Settings:	
•	Enable Real-time Scan	Enabled
•	Automatically quarantine threats found during scanning	Disabled
•	Automatically update virus database	Enabled
•	Show notification messages	Disabled
•	Heuristics Scanning Level	LOW
•	Do not scan files larger than	20 MB
•	Keep an alert on the screen for	120 Seconds
Manua	I Scanning Settings:	
•	Scan archive files (e.g. *.zip, *.rar)	Enabled
•	Automatically update virus database before scanning	Enabled
•	Enable cloud scanning	Disabled
•	Heuristics Scanning Level	LOW
•	Do not scan files larger than	20 MB
Schedu	uled Scanning Settings:	1
•	Scan archive files (e.g. *.zip, *.rar)	Enabled
•	Automatically quarantine threats found during scanning	Disabled

Setting	Value
Automatically update virus database before scanning	Enabled
Show scanning progress	Enabled
Enable cloud scanning	Disabled
Heuristics Scanning Level	LOW
Do not scan files larger than	20 MB
Scan Profiles:	
Predefined Scan Profiles	My Computer, Critical Areas
Custom Scan Profiles	None
Scan Schedules:	
Weekly Virus Scanning	
Scan Profile	'My Computer' profile
Schedule	Weekly, on Sunday at 12:00 AM.

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

4.2.2. Import /Export and Manage Personal Configurations

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

Open the configurations interface

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

COMODO Creating Trust Online*

ty Active Remove Import Export
Import Export
Export

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

Click the area on which you would like more information:

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

Export your current configuration to a file

- Open Comodo Client Security
- Click 'More' > 'Manage My Configurations'
- Select the currently active configuration and click 'Export'

COMODO Creating Trust Online*

😣 Configurat	ions									
My Configura	ations Client - Security	Active Active						Ac Re Im Ex	tivato movo port. port.	e
Save As				:	0	0	0			
Computer comodo	bin boot cdrom dev etc home lib lib64 lost+found media	mnt opt proc root run sbin snap srv sys tmp	usr var							
File <u>n</u> ame:	AV xml configurati	on file (*.cf	gx)				¢		Save Cance	el

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

A confirmation dialog will appear if the export is successful:



Import a saved configuration from a file

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

To import a configuration file

COMODO Creating Trust Online*

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

Look in: /home/tester/DocuCCS Configuration Computer tester Custom CCS Profile.cfgx	😣 🗐 Open		
Computer tester Custom CCS Profile.cfgx	Look in:	/home/tester/DocuCCS Configuration 2 3 3	🛤 🗉 🗉
	Compute	Custom CCS Profile.cfgx	
File name: Custom CCS Profile.cfgx Files of type: All Files (# #)	File <u>n</u> ame:	Custom CCS Profile.cfgx	<u>Open</u>

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



• You will see the following confirmation after import:



The profile is now available for activation if required:

COMODO Creating Trust Online*

My Configurations	Active 🖉	Activate
Custom CCS Profile - Importe	d	Remove
como bo cache becanty	Active	In a set
		import
		Export

Select and implement a different configuration profile

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

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

You will see the following confirmation dialog:



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

COMODO Creating Trust Online*

Configurations		
My Configurations	Active	Activate
COMODO Client - Security Custom CCS Profile - Imported	Active	Remove
		Import
		Export
What do these settings do?		Close

Delete an inactive configuration profile

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

Remove an unwanted profile

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



The profile will be removed from your computer:





4.3. Diagnostics

Click 'More' > 'Diagnostics'

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

It checks:

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

Open the diagnostics tool

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

OR



Click 'Run Diagnostics' **Encounter**.
Note: diagnostics can only be run by root users (admins). If you are not logged in as root, then you will

need to provide	the root password before proceeding:
😣 🖨 🔺	uthenticate
S	Authentication is required for CCS Diagnostics application An application is attempting to perform an action that requires privileges. Authentication is required to perform this action. Password:
▶ Details	Cancel Authenticate

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



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



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

COMODO Creating Trust Online*



4.4. View Antivirus Events

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

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

The log viewer tells you:

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

View Antivirus Events

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

Date	Location	Malware Name	Action	Status
06/27/2019 12:32:16	/home/susan/Doubtful/Files/Adylkuz	Malware@#1ie	Detect	Success
06/27/2019 12:33:34	/home/susan/Doubtful/Files/Adylkuz	Malware@#1ie	Quarantine	Success
06/27/2019 12:36:17	/home/susan/Doubtful/Files/Bitcoin	TrojWare.Win3	Quarantine	Success
06/27/2019 12:36:59	/home/susan/Doubtful/Files/Bitcoin	TrojWare.Win3	Quarantine	Success
06/27/2019 12:37:28	/home/susan/Doubtful/Files/Bitcoin	TrojWare.Win3	Detect	Success
06/27/2019 12:37:29	/home/susan/Doubtful/Files/Bitcoin	TrojWare.Win3	Quarantine	Success
06/27/2019 13:08:24	/home/susan/Doubtful/Files/Ranso	Malware@#3o	Detect	Success
06/27/2019 13:08:24	/home/susan/Doubtful/Files/Ranso	Malware@#2r	Detect	Success

Antivirus Events

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



Action	How CCS attempted to deal with the malware
Status	Whether or not the action was successful

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

4.4.1. Log Viewer Module

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

Open log viewer panel

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

									Log Vie	ewer	*****				3
<u>F</u> ile	View														
्रे 🗰 T	oday	Ē	Cur	rent V	Veek	= 0	Curre	ent Month	🛗 Entire I	Period					
1010101010101		an Lo	ogs 🔗	n na serie de la compañía de la comp		× Bx	•	🗎 Antivirus E	vents 🔀						
	Logs	per M	lodule IS Eve	e ents				Da	ite		Loc	ation		Malware	N
		evice	Contr	ol Eve	ents		1	06/27/2019	12:32:16	/home/s	susan/Doubtfu	ul/Files/Adylkuzz/8	32	Malware@#1ienpeux	.rv
		erts D	Displa	yed			2	06/27/2019	12:33:34	/home/s	susan/Doubtfu	ul/Files/Adylkuzz/8	82	Malware@#1ienpeux	.rv
		onfigu	ratio	n Chai	nges		3	06/27/2019	12:36:17	/home/s	susan/Doubtfu	ul/Files/Bitcoin mi	ne	TrojWare.Win32.CoinM	٩iı
							4	06/27/2019	12:36:59	/home/s	susan/Doubtfu	ul/Files/Bitcoin mi	ne	TrojWare.Win32.CoinM	٩iı
							5	06/27/2019	12:37:28	/home/s	susan/Doubtfu	ul/Files/Bitcoin mii	ne	TrojWare.Win32.CoinM	٩iı
							6	06/27/2019	12:37:29	/home/s	susan/Doubtfu	ıl/Files/Bitcoin miı	ne	TrojWare.Win32.CoinM	٩iı
							7	06/27/2019	13:08:24	/home/s	susan/Doubtfu	ul/Files/Ransomwa	are	Malware@#3o4z9hhl	vr
							8	06/27/2019	13:08:24	/home/s	susan/Doubtfu	ul/Files/Ransomwa	are	Malware@#2rnh8t18	of
хорнанияна															
vlogvie	ewer	Date	Filter			- Bx									
•		June	e , 2	019		•									
10	11	12	13	14	15	16									
17	18	19	20	21	22	23									
24	25	26	27	28	29	30									
÷		July	/ <u> </u>	019		•									
8	9	10	11	12	13	14									
15	16	17	18	19	20	21									
22	23	24	25	26	27	28	•							•	
							_							Records: 8	

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

• Antivirus Events - Shows logs generated by the antivirus module. For example, a log is created when

COMODO Creating Trust Online*

malware is found, when an alert is generated, and when an item is guarantined.

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

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

Export Log Files

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

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

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

4.4.1.1. Antivirus Logs

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

COMODO Creating Trust Online

							ererere		Log V	iewer) 😣
<u>F</u> ile	View														
् हे 🗰 T	īoday	Ê	Curi	rent V	Veek	i	Curr	ent Month	🛗 Entire	Period					
**********		en Lo	gs 🔗			s f x		🔋 Antivirus I	Events 区						
	Logs	per M	odule Is Eve	nts				D	ate		L	ocation		Malw	are N
	e D	evice	Contr	ol Eve	ents		1	06/27/2019	12:32:16	/home/su	isan/Doul	otful/Files/Adylk	uzz/82	Malware@#1ienpe	euxrv
	Other	r Logs erts D	Displa	yed			2	06/27/2019	12:33:34	/home/su	isan/Doul	otful/Files/Adylk	uzz/82	Malware@#1ienpe	euxrv
	📑 Ta	sks Li onfigu	aunch Iratior	ied 1 Chai	nges		З	06/27/2019	12:36:17	/home/su	isan/Doul	otful/Files/Bitcoi	n mine	TrojWare.Win32.Co	oinMi
							4	06/27/2019	12:36:59	/home/su	isan/Doul	otful/Files/Bitcoi	n mine	TrojWare.Win32.Co	oinMiı
							5	06/27/2019	12:37:28	/home/su	isan/Doul	otful/Files/Bitcoi	n mine	TrojWare.Win32.Co	oinMiı
							6	06/27/2019	12:37:29	/home/su	isan/Doul	otful/Files/Bitcoi	n mine	TrojWare.Win32.Co	oinMiı
							7	06/27/2019	13:08:24	/home/su	isan/Doul	otful/Files/Ranso	mware	Malware@#3o4z9	hhlvr
							8	06/27/2019	13:08:24	/home/su	isan/Doul	otful/Files/Ranso	mware	Malware@#2rnh8	t18of
		Date	Filter	10100		- PX									
e		June	e 2	019		•	2								
10	11	12	13	14	15	16									
17	18	19	20	21	22	23									
24	25	26	27	28	29	30									
÷		July	, 2	019		•									
8	9	10	11	12	13	14									
15	16	17	18	19	20	21									
22	23	24	25	26	27	28	•			en el					••
														Pocordo	. 0

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

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

40 :36		/home/como	do/L
41:15	Refr	/home/comr esh (F5)	do/I
35:17	<u>Adv</u>	anced Filter	
35:17	<u> </u>	(home / com	
:35:17		/nome/como	000/1



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

4.4.1.1.1. Filter Antivirus Logs

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

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

Configure Event Filters

- Open CCS.
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Antivirus Events' in the left-menu
- · Right-click inside the log viewer module and select 'Advanced Filter'
 - ... or click 'View' on the menu bar and select 'Advanced Filter'

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

Select a filter criteria and click 'Add'



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

8 🖲 🖲 Lo	g Vlewer					
File View						
📸 Today	🗮 Current Week	🗯 Current Month	😁 Entire Period			
ennennennen				Advanced Filter		
Action					• -1-	Bemoue
				Guarantine Ignore) Grantine Ignore)	ASK.	
						- 6
	Logs https://www.	🗗 🏹 🥎 Antivirus	Events 🔯			
🔁 📷 Logs pe	r Module Virus Events		Date	Location	Malware Name	Act*
🕒 📑 Other L	ogs	1 05/10/20	19 12:18:41	/home/comodo/Downloads/02ab39d5ef83ffd0	Malware@#vigyaoklh7gw	Detect
- 😝 Aler	is Launched	2 05/10/2	19 17:18:41	/home/comodo/Downloads/D636d8749ech285	Malware@#jgft8mtlykervk	Detect
OP Con	figuration Changes	2007 2007	Red Color	6. A.		

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

🧐 🖨 🕞 Lo	g Viewer							
<u>File</u> View								
😤 Today	😤 Current Week	🗮 Current Month	😁 Entire Period					
				Advanced Filter 10				- Bx
Location				Contains -			Remove	n F
				Contains				
Location				Does Not Contain				
Location								•
aningan	Logs	🖉 🐑 🕥 Antivirus	Events 🔟					
This Logs of	er Module		Date		ocation	Malware	Name	Acti *

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

🔒 🗇 🗉 Log Vlewer			
File View			
🖀 Today 🚔 Current Week 🖀 Cu	urrent Month 🛛 😁 Entire Perio	d	
		Advanced Filter Contractor Contractor Contractor Contractor	🗃 🗵
Malware Name		Contains V	Remove
Malware Name 🔹 Add		Does Not Contain	* *
Logs 🖉 🛪	📢 Antivirus Events 🔟		
Logs per Module Antivirus Events	Date	Location Malv	rare Name Actio
Other Logs Merts Disclosed	05/24/2019 14:49:25	AnonexiconedotDevenhoaris 02.dc3945.e563945 - 553333333333	

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

😝 🖨 🕘 Log Vlewer							
File View							
😤 Today 🗮 Current Week 🛛 🗮 C	urren	t Month 🛛 😁 Entire Period					
· · · · · · · · · · · · · · · · · · ·			Advanced Filter				
Status	Status Found + F Surcess						
			Fegual				
Logs	•	Antivirus Events					
🕀 🌆 Logs per Module		Date	Location	Malware Name	Actio *		
E Cother Logs	1	05/14/2019 14:49:25	/home/comodo/Downloads/02ab39d5ef83ffd0	Malware@#vigyaoklh7gw	Detect		
Alerts Displayed Alerts Launched	2	05/14/2019 14:49:26	/home/comodo/Downloads/0636d8749ecb285	Malware@#jglt8m0jxmvk	Detect		
• 00 Configuration Changes	3	05/14/2019 14:49:26	, /home/comodo/Downloads/9c2848962733846	Makwaret@#3pfwc807ovnFc			

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

4.4.1.2. Device Control Logs

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

View external device connection logs

Click 'More' > 'View Antivirus Events'

COMODO Creating Trust Online

- Click the 'More' button to open the log viewer module
- Select 'Device Control Events' in the left-menu

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

	or to to to t	Lo	g Viewer		
<u>F</u> ile View					
🗮 Today 🗮 Current Week 🗮 C	urren	nt Month 🛗 Entire I	Period		
		Antivirus Events 📧	Oevice Control	Events 🗵	
E- III Logs per Module		Date 🛆	Name	Identifier	State 📤
Device Control Events	1	06/27/2019 14:11:44	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
Other Logs Alerts Displayed	2	06/27/2019 14:13:58	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
Configuration Changes	3	06/27/2019 14:14:46	v150w	usb\VID03f0&PID7d40\E600728	Disconnected
	4	06/27/2019 14:15:54	Firebird6Sp9 (Cr	usb\VID0781&PID5530\012345	Connected/Blocked
	5	06/27/2019 14:17:30	Firebird6Sp9 (Cr	usb\VID0781&PID5530\012345	Disconnected
	6	06/27/2019 15:41:36	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
	7	06/27/2019 15:41:44	v150w	usb\VID03f0&PID7d40\E600728	Disconnected
nonononono Date Filter nonononono 🗗 🗙	8	06/27/2019 15:41:51	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
6 June 2019	9	06/27/2019 15:45:20	v150w	usb\VID03f0&PID7d40\E600728	Disconnected
10 11 12 13 14 15 16	10	06/27/2019 15:52:57	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
17 18 19 20 21 22 23	11	06/27/2019 15:55:00	v150w	usb\VID03f0&PID7d40\E600728	Disconnected
🗧 July_ 2019 🌖	12	06/27/2019 16:18:37	v150w	usb\VID03f0&PID7d40\E600728	Connected/Allowed
8 9 10 11 12 13 14 15 16 17 18 19 20 21	13	06/27/2019 16:22:22	v150w	usb\VID03f0&PID7d40\E600728	Disconnected
	•				

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

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



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



4.4.1.2.1. Filter Device Control Logs

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

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

Configure event filters

- Open CCS.
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Device Control Events' in the left-menu
- · Right-click inside the log viewer module and select 'Advanced Filter'
 - ... or click 'View' on the menu bar and select 'Advanced Filter'

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

Select a filter criteria and click 'Add'

	_	
Name 🕞 Add		
Name	5	
Identifier		
State		

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

Name	Contains	Remove
	Contains	
Name 🔻 Add	Does Not Contain	

- Select 'Contains' or 'Does Not Contain' from the second drop-down:
 - Contains Show only events which concern device name you specify.
 - Does Not Contain Inverts your choice. Show all events except those involving the device name you specify.
 - Enter your filter criteria in the text field
- 2. Identifier: Filter entries based on the device ID of the external device.

••••••••••••••••••••••••••••••••••••••	dvanced Filter	
Identifier	Contains 👻	Remove
	Contains	
Identifier 🔻 Add	Does Not Contain	

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



- 3. State: Filter events based on whether the device connection attempt was allowed or blocked.
 - Select 'Equal' or 'Not Equal' from the drop-down.
 - Equal Show only events that meet the criteria you select.
 - Not Equal Inverts your choice. For example, select 'Not Equal' + 'Allowed' to view every event except those where devices were allowed.
- Now select the state from 'Allowed' or 'Blocked'

4.4.1.3. 'Alerts Displayed' Logs

•

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

									Log V	iewer					🖶 💷 😣
<u>F</u> ile	View														
) 🗰 т	📅 Today 🗮 Current Week 🗮 Current Month 🛗 Entire Period														
100000000		on Lo	gs 👳			ðx		4	Antivirus E	vents 🙁 🤇	Aler	ts Displa	yed 🔝		
	Logs	per M tiviru	lodule Is Eve	ents					Date	Δ	Ту	pe		Descriptio	n
Device Control Events				1	0	06/27/2019	12:32:16	Antiviru	s Alert	Malware	e@#1ienpe	ıxrw2dy			
□ □ □ □ Other Logs □ □ □ □ Alerts Displayed				2	(06/27/2019	12:33:34	Antiviru	s Alert	Malware	e@#1ienpe	uxrw2dy			
	📑 Ta	sks La onfigu	aunch	ied 1 Chai	naes										
		gu			ges										
		Date	Filter			ðx									
e		June	e_ 2	019		•	2								
10	11	12	13	14	15	16									
17	18	19	20	21	22	23									
24	25	26	27	2.5	29	30									
	0	July	20	019	13	•									
15	9 16	10	18	12	20	21									
22	23	24	25	26	27	28	-			:::::					
							Ľ							Rec	ords: 2

'Alerts Displayed' Logs - Column Descriptions					
Column Header	Descriptions				
Date	The time the alert was shown.				
Туре	The alert category. Currently, 'Antivirus' is the only alert type.				
Description	Malware name.				


Advice	Location where the malware was detected.
Answered	Whether the user responded to the alert. If yes, you will see the date and time of the response.
Answer	The response provided by the user.
Flags	Not used
Treat as	Not used
Event	Click 'Related Event' to view details of the event that triggered the alert. You'll also see the action taken by CCS on the event. See 'Antivirus Logs ' for more details.

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

Туре		Description		
ivirus Al	ort F	Malwaro@#vigyaok Re <u>f</u> resh (F5)		
ivirus Al	Advanced Filter 8m0			
ivirus Al	Export wc8			
virus Al	ert	Malware@#3fxg8e		

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

4.4.1.3.1. Filter 'Alerts Displayed' Logs

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

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

Configure Event Filters

- Open CCS.
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Alerts Displayed' in the left-menu
- Right-click inside the log viewer module and select 'Advanced Filter'



... or click 'View' on the menu bar and select 'Advanced Filter'

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

• Select a filter criteria and click 'Add'

•

😣 🗖 🗊 Log	Viewer		
<u>F</u> ile View			
🗮 Today	🗮 Current Week	🗎 Current Month	E E
		nananan karanan da	
Advice Advice Answer	Add		
Answered Description	ogs and an and a second	🗗 🏹 Antiviru	s Evento
© Flags Treat As	lodule Js Events		Date
Туре	J	1 05/10/	201 9 1
Alerts Tasks	Displayed Launched	2 05/10/	2019 l.
Conne	guration Changes	3 05/10/	2018

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

😣 🔿 🗊 Log Viewer							
File View							
🛅 Today 🛛 🗮 Current Week 🛛 🗮 🕻	Current Month	😁 Entire Period					
			Advanced Filter	Ø			
Advice Contains Advice Add							
Logs	Alerts Disp	played 🔀					
E Logs per Module		Туре	Description	Advice			
d - Other Logs	1 Antivirus	Alert Ma	lware@#vigyaoklh7gw	/home/comodo/Downloads/02ab39d5ef83ffd09e3774a67b78			
Alerts Displayed Alerts Displayed Alerts Displayed Alerts Displayed	2 Antivirus	Alert Ma	lware@#vigyaoklh7gw	/home/comodo/Downloads/02ab39d5ef83ffd09e3774a67b78			
··· de Configuration changes	Antivirus	s Alert Ma	byare@43gft8m0ixmob				

- Select 'Contains' or 'Does Not Contain' option from the drop-down.
 - Contains Show only alerts which concern items at the location you specify. You can add multiple locations.
 - Does Not Contain Inverts your choice. Show all alerts except those about items in the location you specify.
- 2. **Answer**: Filter logs by the action taken by the user at the alert. You can then filter by a specific type of action. For example, show events where the threat was quarantined.

😑 😑 🛛 Log Viewer								
File View								
A Taxiau A Current Mark A	Current Month	rind						
Content Week	Current Month	nod						
		Advanced	d Filter Antonio					
Annuar	()							
Answer	Equal						Remove	e
		Unknow	m 🔽 Deny	Sandbox	Disinfect	Skip Once	- x	2
			Treat As	Time-out	C Quarantine	Add To Exclusion	sio	-
				1		,		
Logs 🗗 🗶	🌖 🚺 Alerts Displayed 💟							
🕞 🧱 Logs per Module	Descriptio	in.			Advice			-
Antivirus Events				-	1.20.10.00.00.000	2224 621 2621 C 3		05
Other Logs	1 Malware@#vigyaoklh7	gw	/home/comode	Downloads/02	ab39d5et83ttd09	e3774a67b783bta34	45505d3cb8	14
Alerts Displayed	2 Malware@#vigvaoklh7	aw	, /home/comodo	Downloads/02	ab39d5ef83ffd09	e3774a67b783bfa3	45505d3cb8	05///
Configuration Changes		2						10.1

- Select 'Equal' or 'Not Equal' from the drop-down.
 - Equal Show only events which feature the action you select. You can select multiple actions.
 - **Not Equal** Inverts your choice. For example, select 'Not Equal' + 'Quarantine' to view every alert *except* those that where the threat was quarantined.
- Select the action you want to view:
 - Unknown Events where the user did not respond to the alert.
 - Quarantine Events where the user chose to place the threat in quarantine
 - Skip Once Events where the user chose to allow the threat.
 - Add to Exclusions Events where the user created an exception for the threat at the alert.
 - Note Other actions shown in the screen are not applicable.
- 3. **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:

🧑 🖨 🗊 Log Viewer						
<u>F</u> ile View						
📸 Today 🗮 Current Week 🖀 Current Month 🛗 Entire Period						
Ā	dvanced filter					
Answered Equal 01/01/00 C Remove						
Answered - Add	Greater than or Equal					
Alerts Displayed 🗵	Less than or Equal					
Eugs per Module Description	Advice					
O T Other Logs 1 Malware⊕≠vigyaoklh7gw	/home/comodo/Downloads/02ab39d5ef83ffd09e3774a67b783bfa345505d3cb8 05					

- Select any of the following options in the drop-down:
 - Equal Show only events that occurred on the specified date
 - · Greater than Show only events that occurred later than the specified date
 - · Greater than or Equal Show only events that occurred on, or after, the specified date
 - · Less than Show only events that occurred before the specified date
 - Less than or Equal Show only events that occurred on, or before, the specified date
 - Not Equal Show events that occurred at any time except the specified date
- 4. **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					
<u>File</u> View					
🕆 Today 🛛 🗎 Current Week 🖀	Current Month	😁 Entire Per	iod		
		ann an	Advanced Filter		
Description			Contains Des Not Contain	арр	Remove
Logs	Alerts Disp	olayed 🔝			
Logs per Module Antivirus Events	0)ate	Ларана Туре	Description	
Cher Logs	1 05/10/2019	14:22:15	Antivirus Alert	ApplicUnwnt@#2975xfk8s2pq1	/home/comodo/Downloads/eicar.com
Alerts Displayed Tasks Launched OP Configuration Changes	2 05/10/2019	14:22:33	Antivirus Alert	ApplicUnwnt@#2975xfk8s2pq1	/home/comodo/Downloads/eicar.com

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

😣 🗇 💿 Log Viewer						
File View			3			
😤 Today 🛛 🗮 Current Week 🖀	Current Month	🗂 Entire Period				
			Advanced Filter		(B)×	
Type						
🗈 🔟 Logs per Module		Date /	Type	Description		
E C Other Logs	1 05/10/201	9 14:20:47	Antivirus Alert	Malware@#vigyaoklh7gw	/home/comodo/Downloads/02a	
Alerts Displayed Tasks Launched	2 05/10/201	9 14:21:02	Antivirus Alert	Malware@#vigyaoklh7gw	/home/comodo/Downloads/02a	
de Configuration Changes	05/10/203	9 14:21:02	Antiv:rus Alert	Malware@#jgft8m0jxmvk	/home/comodo/Downloads/063	

- Select 'Equal' or 'Not Equal' from the drop-down.
 - Equal Show only events which feature the alert type you select.
 - Not Equal Inverts your choice.
- 4.4.1.4. 'Tasks Launched' Logs
 - Click 'More' > 'Preferences' > 'View Antivirus Events' > 'More' > 'Tasks Launched'
 - Task logs show all activities run by either CCS or the user.
 - Example tasks are virus database updates and virus scans. Each row shows the type of task and various other details.

COMODO Creating Trust Online*

1999-1999-199	Log Viewer 💮 🗐 😣														
<u>F</u> ile	<u>F</u> ile View														
🗄 Today 🚔 Current Week 🗮 Current Month 🛗 Entire Period															
10000000	ana ana ana ang ang ang ang ang ang ang	on Lo	gs 👳			- BX		Antivirus I	Events 💌	📑 Tas	sks Launched 🖸	3			
	Logs	per M ntiviru	odule Is Eve	nts					Date	\square	Туре		Parameter	Complete	ed 📤
	Cthou	evice	Contr	ol Eve	ents		1	06/27/201	9 11:59:38		Antivirus Upda	te		06/27/2019 12:05:	03
		erts D	isplay	yed			2	06/27/201	9 12:33:30		Antivirus Upda	te		06/27/2019 12:33:	42
	•• Co	sks La onfigu	ratior	ied i Chai	nges		3	06/27/201	9 12:40:06		Antivirus Upda	te		06/27/2019 12:40:	14
							4	06/27/201	9 12:40:15		Antivirus Scan		Critical Areas	06/27/2019 12:45:	08
							5	06/27/201	9 12:54:55		Antivirus Upda	te		06/27/2019 12:55:	01
							6	06/27/201	9 12:55:01		Antivirus Scan		My Computer	06/27/2019 13:08:	27
							7	06/27/201	9 13:28:58		Antivirus Upda	te		06/27/2019 13:29:	00
							8	06/27/201	9 14:02:22		Antivirus Upda	te		06/27/2019 14:02:	24
							9	06/27/201	9 14:11:02		Antivirus Upda	te		06/27/2019 14:11:	09
10000000	nnon.	Date	Filter	14141414		- BX	10	06/27/201	9 14:41:09		Antivirus Upda	te		06/27/2019 14:41:	14
logvie	wer	June	e 2	019		•	11	06/27/201	9 15:11:15		Antivirus Upda	te		06/27/2019 15:11:	17
10	11	12	13	14	15	16	12	06/27/201	9 15:41:17		Antivirus Upda	te		06/27/2019 15:41:	19
24	25	26	20 27	23	22	30	13	06/27/201	9 16:11:19		Antivirus Upda	te		06/27/2019 16:11:	21
÷		July	, 20	019		•	14	06/28/201	9 10:07:10		Antivirus Upda	te		06/28/2019 10:14:	37
8	9 16	10 17	11 18	12	13 20	14	15	06/28/201	9 10:44:38		Antivirus Upda	te		06/28/2019 10:44:	45
22	23	24	25	26	27	28	16	06/28/201	9 11-14-46		Antivirus Unda	te		06/28/2019 11-14-	50 -
														Decer	

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

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



уре		Parameter			
late				05/ 15/2	
late	Re	fresh (F5)		05/15/2	
late	<u>A</u> d	vanced Filter		05/15/2	
	Ex	Export			
late				05/ 15/2	
into				05/15/D	

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

4.4.1.4.1. Filter 'Tasks Launched' Logs

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

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

Configure Event Filters

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

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

Select a filter criteria and click 'Add'

COMODO Creating Trust Online*

🤒 🖨 🗊 🛛 Lo	g Viewer	
<u>F</u> ile View		
📸 Today	🛗 Current Week	🗎 Current Month
		0000000000000000000000000000000000000
Type Code Completed Parameter Type Logs pe Logs pe Code Data Completed Parameter Type Code Completed Parameter Type Code Completed Parameter Type Logs pe Code Completed Parameter Type Logs pe Code Completed Parameter Type Code Completed Parameter Type Code Completed Parameter Type Code Completed Parameter Type Code Completed Parameter Type Code Completed Code Completed Parameter Type Code Code Code Code Code Completed Code Code Code Code Code Code Code Co	Add ogs 1000000000000000000000000000000000000	Tasks Launcher Da 1

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

🧧 🗇 🗇 Log Viewer							
File View							
😁 Today 🛛 🚔 Current Week 🗮 🕻	Current Month	😁 Entire Period					
			6 Advanced Filter Secondaria				ðx
Code		Equal Greate Greate Less th	r than r than or Equal			Remove	
Cogs Brance Brance	Tasks Laur	Not Eq	ual				
Antivirus Events		Date	Туре	Parameter	Completed	Code	-
🖻 📰 Other Logs	1 05/09/20	19 17:47:30	Antivirus Update		05/09/2019 17:52:57	0x00000000	
Alerts Displayed Tasks Launched of Configuration Changes	2 05/09/20	19 18:22:57	Antivirus Update		05/09/2019 18:23:03	0×00000001	

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

😸 🔿 🗊 Log Viewer File View							
🛪 Today 🗮 Current Week 🚆	Current Month	😁 Entire Period	Advanced Filter				- 81
Completed				Equal Greater t Greater t Less that	han han or Equal	1/01/00 🖨 Remove	
Logs 🖉	🗵 🔚 Tasks Lau	unched 🔀		Less than Not Equa	n or Equal		
Logs per Module Logs Antivinus Events		Date /	Туре	Parameter	Completed	d Code	
E Other Logs	1 05/09/2	019 17:47:30	Antivirus Update		05/09/2019 17:52:5	57 0x0000000	¢
- () Alerts Displayed	2 05/09/2	019 18:22:57	Antivirus Update		05/09/2019 18:23:0	0x0000001	c
- 🕫 Configuration Changes	3 05/09/2	019 18:53:03	Antivirus Update		05/09/2019 18:53:0	9 0x00000001	C
	a 05/09/2	019 39:25:09	Antomias Opdatio				

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

😣 🗇 🗇 Log Viewer							
<u>File</u> View							
😁 Today 🛛 🚔 Current Week 🗮 🕅	Current Month	😁 Entire Period					
			Advanced Filter				- E ×
Parameter Parameter		Cor Cor Doc	itains 🕞 🔹			Remove	
Logs	💽 Tasks Laun	ched 🔀					
Logs per Module Logs Antivirus Events		Date 🛆	Туре	Parameter	Completed	Code	
Other Logs	1 05/09/20	19 17:47:30	Antivirus Update		05/09/2019 17:52:57	0x00000000	¢
Tasks Launched	2 05/09/20	19 18:22:57	Antivirus Update		05/09/2019 18:23:03	0x00000001	c
00 Configuration Changes	3.0000000	19-18-51-63	Astivius Hodahi		02/0303039 (8.23.86		¢

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

😑 🔍 🕕 Log Viewer								
File View								
🗮 Today 🛛 🗮 Current	Week 🛛 🗮 🤇	Current Month	😁 Entire Period	1				
				Advanced filter				ð×
Туре				qual T Av Update qual T Av Scan I ot Equal	E IT Log Clearing	🖺 Upgrade ation	Remove	
Logs	6×	🔚 Tasks Laur	nched 🔀					
Logs per Module Logs per Module Logs per Module			Date 🔨	Туре	Parameter	Completed	Code	- I
E Cther Logs		1 05/09/20	19 17:47:30	Antivirus Update		05/09/2019 17:52:57	0x00000000	¢
Tode Lancted		2 05/09/20	19 18:22:57	Antivirus Update		05/09/2019 18:23:03	0x00000001	- Contraction

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

4.4.1.5. Configuration Change Logs

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

Le déserventes									Log ۱	/iewer		0	8
<u>F</u> ile	View												
🕴 🗰 те	oday	Ê	Cur	rent V	Veek	= 0	Curre	nt Month	🛗 Entire Pe	eriod			
10000000		ere Lo	ogs 👳			st. BX		Antivirus I	Events 🔣	o Configuration C	hanges 区		
Ē 🏢	Logs	per M	lodule Is Eve	e ents				Da	ate 🛆	Action	Modifier	Object	
		evice	Contr	rol Eve	ents		1	06/27/201	9 12:07:56	Option Changed	User	Antivirus: Mode	
		erts D	Displa	yed			2	06/27/201	9 12:31:01	Option Changed	User	Antivirus: Mode	
	📲 Ta	isks Li onfigu	aunch Iratior	ned n Chai	nges		3	06/27/201	9 12:34:43	Option Changed	User	Antivirus: Real-Time Auto Quarantine	
							4	06/27/201	9 12:37:09	Option Changed	User	Antivirus: Real-Time Show Alerts	
							5	06/27/201	9 14:12:52	Object Added	User	Device Control: Exclusion	us
1000000	nnnn.	Date	Filter			- BX	6	06/27/201	9 14:13:57	Option Changed	User	Device Control: Enable Device Con	
e		June	e , 2	019		•	7	06/27/201	9 15:23:24	Object Removed	User	Device Control: Exclusion	us
10	11	12	13	14	15	16	8	06/27/201	9 15:23:24	Option Changed	User	Device Control: Enable Device Con	
17 24	18 25	19 26	20 27	21 28	22 29	23 30	9	06/27/201	9 15:45:00	Object Added	User	Device Control: Exclusion	us
e		July	/ 2	019		•	10	06/28/201	9 15:37:49	Option Changed	User	Antivirus: Real-Time Auto Quarantine	
8	9	10	11	12	13	14	11	06/28/201	9 15:37:49	Option Changed	User	Antivirus: Real-Time Show Alerts	
15	16 23	17 24	18 25	19 26	20 27	21 28				I		-	
	2.5	27		20	21	20						[1	Þ
												Records: 1	

COMODO Creating Trust Online

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

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



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

4.4.1.5.1. Filter 'Configuration Change' Logs

You can filter logged events by the following criteria:

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

Configure Event Filters

- Open CCS.
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Configuration changes' in the left-menu
- · Right-click inside the log viewer module and select 'Advanced Filter'
 - ... or click 'View' on the menu bar and select 'Advanced Filter'

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

Select a filter criteria and click 'Add'

COMODO Creating Trust Online



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

😣 😑 🐵 Log Viewer					
Eile View					
😤 Today 🛛 🗮 Current Week 🛛 🗮 🤇	Current Month 👚 Entire Po	eriod			
s. 		Advanced	Filter		ð x
Action		Foual	E object Added E object Demond E of	ion Added	Remove
		Eduar	Cobject Added 1 Object Removed 1 St	ring Added	Heinove
			I. Object Changed J. Option Changed J.	String Removed	-
Logs &X	O Configuration Changes	8			
Logs per Module Logs Antivinus Events	Action	Modifier	Object	Name	*
E- Con Other Logs	1 Option Changed	User	Antivirus: Mode		d
Alerts Displayed Tasks Faunched	2 Option Changed	User	Antivirus: Mode		
Configuration Changes					

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

🙆 🖲 🕕 Log Viewer								
File View								
😤 Today 🗮 Current Week 🗮 O	Current Month	😤 Entire Perio	bd					
			Advanced	Filter Management				e x
Madifiar			(m	773			``````````````````````````````````````	
Modifier			Equal		E Antivirur	Alast E Defenset Alast E Everytic	Remove	
				1 User	I. Antivirus	Alert Defense+ Alert Executio		
				F Auto	Learn F Fire	ewall Alert F BO Alert		
economication Logs	00 Configurat	ion Changes 🔝	1					
Logs per Module		Date	AA	ction	Modifier	Object		
Cher Logs	1 05/10/201	9 10:20:38	Option Ch	anged U	ser	Antivirus: Mode		
- U Alerts Displayed	2 05/10/2019	9 10:22:47	Option Ch	anged U	ser	Antivirus: Mode		
Configuration Changes								

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

•

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

😸 🖨 🗈 Log Viewer					
Today 🗮 Current Week	🖹 Current Month	😁 Entire Period			
Name Add		Contains Contains Does Not Cont	ain		Remove
Logs	🗵 👓 Configura	tion Changes 💟			
Logs per Module Antivirus Events		Object	Name	Old Value	1
🗈 💮 Other Logs	1 Antivirus:	Mode		On Access	C
 Image: State of the second seco	2 Antivirus	Mode		On Access	c
waan 🖓 Geobouration Changes	$= \frac{1}{2} \sum_{i=1}^{n-1} A_i (z_i x_i) = \frac{1}{2} b_i$		Chwek dawnloads		1

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

COMODO Creating Trust Online

🧧 🖨 🕤 Log Viewer					
File View	🖀 Current Month 📑 Entire Per	iod Advanced	Filter		e x
Object	Equal Figure Not Equal	4	Antivirus: Scheduled Scar	n Rootkit	emove
Logs	3 Configuration Changes	3			
Logs per Module Antivirus Events Dther Logs	Action 1 Option Changed	Modifier User	Object Antivirus: Mode	Name	
Averts Displayed	12 Option Changed	User	Antivirus. Mode	Week en anticipado	¢.

- The following list shows all available object types:
 - Antivirus Mode
 - Antivirus Timeout
 - Antivirus Realtime AutoUpdate
 - Antivirus Realtime Auto Quarantine
 - Antivirus Realtime Heuristics Level
 - Antivirus Realtime Size Limit
 - Antivirus Realtime Time Limit
 - Antivirus Manual Scan Archives
 - Antivirus Manual Auto Update
 - Antivirus Manual Heuristics Level
 - Antivirus Manual Size Limit
 - Antivirus Manual Scan Cloud
 - Antivirus Scheduled Scan Archives
 - Antivirus Scheduled AutoUpdate
 - Antivirus Scheduled Auto Quarantine,
 - Antivirus Scheduled Heuristics Level
 - Antivirus Scheduled Size Limit
 - Antivirus Scheduled Scan Cloud
 - Antivirus Profile
 - Antivirus Schedule
 - Antivirus Exclusion
 - Antivirus Disable Logging
 - Active Configuration Index
 - Password Protection
 - Use Proxy
 - Proxy Authentication
 - Proxy Server
 - Proxy Port
 - Proxy Login
 - Proxy Password
 - GUI Language
 - Password



- Updates Host
- Log File Size Limit
- Log overflow handling
- Log Backup Folder

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

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

4.5. Browse Support Forums

- Click 'More' > 'Browse Support Forums'
- You can any post questions and suggestions you have about CCS in our community forums, a message board for users to discuss any aspect of our products.
- Registration is free, and you'll benefit from the expert contributions of developers and fellow users alike.

Visit the forum

- Open Comodo Client Security
- Click 'More' > 'Browse Support Forums'
- · You will be taken to the community pages at https://forum.itarian.com

- C	①	//forum.itarian.com	··· 🖂 🖓 🔤
			Login or Sign Up 🔹
		ITarian noun Itarian 1-ter-6-an • Definition of <i>ITarian</i> 1 The IT Gurus that develop and master the power of IT to solve the world's most pressing challenges	
F	Forums		
1	Today's Posts Mark Channels Read Member List Caler	ndar	
	If this is your first visit, be sure to check out the FAQ by citic select the forum that you want to visit from the selection being the selection	king the link above. You may have to register before you can post; click the register link ow.	k above to proceed. To start viewing messages,
	If this is your first visit, be sure to check out the FAQ by cite select the forum that you want to visit from the selection bein	king the link above. You may have to register before you can post: click the register Init ow.	k above to proceed. To start viewing messages.
	If this is your first visit, be sure to check out the FAQ by cities select the forum that you want to visit from the selection beer Forums	king the link above. You may have to register before you can post: click the register ind ow.	k above to proceed. To start viewing messages.
	If this is your first visit, be sure to check out the FAD by cite select the forum that you want to visit from the selection bein Forums FORUMS LATEST ACTIVITY MY SUBSCRIPTIONS Directory	king the link above. You may have to register before you can post: click the register link ow. Topics Posts Last Post	k above to proceed. To start viewing messages.
	If this is your find visit, be sure to check out the FAQ by cite select the forum that you want to visit from the selection bein Forums FORUMS LATEST ACTIVITY MY SUBSCRIPTIONS Directory	king the link above. You may have to register before you can post: click the register tra ow. Topics Posts Last Post	A above to proceed. To start viewing messages.
	If this is your final visit, be sure to check out the FAQ by cite select the forum that you want to visit from the selection bein Forums ronues LATEST ACTIVITY MY SUBSCRIPTIONS Directory Products Citectes anything seland to products taked, ask for help or cor- new clease to improve all the products for the community	king the link above. You may have to register before you can post: circk the register link Topics Posts Last Post 3,053 17,911 Dy Rick C Today: Ge 31 MJ	A above to proceed. To start viewing messages.

Online Knowledge Base

An online knowledge base and support ticketing system is available at http://support.comodo.com. Registration is free.

4.6.Help

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

Open the online guide

COMODO Creating Trust Online

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



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

4.7.About

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

View product information

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



COMODO

Comodo Client - Security for Linux - User Guide

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

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

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

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

Scan your Computer for Viruses

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

Run an on-demand virus scan

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

Ay Computer Predefined Predefined Predefined	Prorite name	Profile type
Critical Areas Predefined	puter	Predefined
	Areas	Predefined
uspicious Files User	us Files	User
Nedia Files User	iles	User

CCS ships with two pre-defined scan profiles

- My Computer Scans every drive, folder and file on your system, including external devices.
- Critical Areas A targeted scan of important files and folders.

Select the profile you want to use then click 'Scan'.

 Create New Scan. Create your own custom scan of specific files, folders or drives. See custom scan to find out more.

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

😑 😑 Scanning: My (Computer	
Scanning: Status:	My Computer /usr/src/linux-head	ders-4.10.0-40/arch/arm/lib/Makefile
Objects Scanned:	14776	Start Time: Wed Apr 4 16:26:27 2018
Threats Found:	0	Duration: 00:00:13
Show on top		
What do these set	tings do?	🕕 Pause 🔾 Stop Scan

Results are shown at the end of the scan:

😣 🔵 Scanning: My Con	nputer - Comp	leted	
Scanning: My Status: Sca	Computer In Completed		
🔘 Objects Scanned:	157561	Start Time: Mon Aug 20 1	12:03:13 2018
🏶 Threats Found:	3	Duration: 00:08:50	
Show on top			
What do these setting]s do?		Results

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

COMODO Creating Trust Online

ApplicUnsaf@#1dkvp9e72akc — Lot Øhome/tester/Documents/test_set/b93a5bb200a87b9728f949ffe10c68fcb93a5bb20 ApplicUnwnt@(#2tplrp9u1mcvu, #2oto6pyf1czwd) — Lot Øhome/tester/Documents/test_set/c12a5bbe438820ee42915e3ebdde0bd9 — Lot Øhome/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39 — Lot Application.Win32.Agent.BUNE@318931415 — Lot Øhome/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511 — Lot Øhome/tester/Documents/test_set/2@306475545 — Lot Øhome/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc — Lot Application.Win32.Bundlore.C@321284137 — Lot Øhome/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f — Lot Øhome/tester/Documents/test_set/79a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 — Lot Øhome/tester/Documents/test_set/75351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.InstalleRex.DP@362046738 — Lot Øhome/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba — Lot _ Mome/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba _ _ Lot _	All ?	 Threat Name 	Risk
 /home/tester/Documents/test_set/b93a5bb200a87b9728f949ffe10c68fcb93a5bb20 ApplicUnwnt@(#2tplrp9u1mcvu, #2oto6pyf1czwd) /home/tester/Documents/test_set/c12a5bbe438820ee42915e3ebdde0bd9 /home/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39 Application.Win32.Agent.BUNE@318931415 /home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511 /home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6 Application.Win32.Agent.Z@306475545 /home/tester/Documents/test_set/044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/79a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		ApplicUnsaf@#1dkvp9e72akc	- Low
ApplicUnwnt@(#2tplrp9u1mcvu, #2oto6pyf1czwd)	\checkmark	/home/tester/Documents/test_set/b93a5bb200a87b9728f949ffe10c68fcb93a5bb20	
 /home/tester/Documents/test_set/c12a5bbe438820ee42915e3ebdde0bd9 /home/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39 Application.Win32.Agent.BUNE@318931415 /home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511 /home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6 Application.Win32.Agent.Z@306475545 /home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		ApplicUnwnt@(#2tplrp9u1mcvu, #2oto6pyf1czwd)	- Low
 /home/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39 Application.Win32.Agent.BUNE@318931415 /home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511 /home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6 Application.Win32.Agent.Z@306475545 /home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 	\checkmark	/home/tester/Documents/test_set/c12a5bbe438820ee42915e3ebdde0bd9	
Application.Win32.Agent.BUNE@318931415 — Low Image: Model of Control of Co	\checkmark	/home/tester/Documents/test_set/f4a89a5755f6b725fc424cd809938d39	
 /home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511 /home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6 Application.Win32.Agent.Z@306475545 /home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		Application.Win32.Agent.BUNE@318931415	- Low
 /home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6 Application.Win32.Agent.Z@306475545 /home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 	\checkmark	/home/tester/Documents/test_set/7ed1051de7f0fb53e14bcfe03fe68511	
Application.Win32.Agent.Z@306475545	\checkmark	/home/tester/Documents/test_set/beda0bea87cecd432080a6d01b146aa6	
 /home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc Application.Win32.Bundlore.C@321284137 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		Application.Win32.Agent.Z@306475545	- Low
Application.Win32.Bundlore.C@321284137	\checkmark	/home/tester/Documents/test_set/0044ecaeed7db1632130cd903fb82bdc	
 /home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		Application.Win32.Bundlore.C@321284137	- Low
 /home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232 Application.Win32.IBryte.X@318641596 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 	\sim	/home/tester/Documents/test_set/69bd6d466aa87773d484cc3e6accc39f	
Application.Win32.IBryte.X@318641596	\checkmark	/home/tester/Documents/test_set/7f9a04d232135f4ebf33ab7f082f6d557f9a04d232	
 /home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229 Application.Win32.InstalleRex.DP@362046738 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		Application.Win32.IBryte.X@318641596	- Low
Application.Win32.InstalleRex.DP@362046738	\checkmark	/home/tester/Documents/test_set/35eaa02294035feaf5b5bef8831535ce35eaa0229	
 /home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b Application.Win32.Multiplug.GETF@323611884 /home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Backdoor.HTML.EMO.E@283889604 /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 		Application.Win32.InstalleRex.DP@362046738	- Low
Application.Win32.Multiplug.GETF@323611884 Low Image: Mome/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba Hig Image: Backdoor.HTML.EMO.E@283889604 Hig Image: Mome/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34 Hig	\checkmark	/home/tester/Documents/test_set/7f351473b7fd2c71416d7e27f5839cc27f351473b	
Image: Marked control of the sector of th		Application.Win32.Multiplug.GETF@323611884	- Low
Backdoor.HTML.EMO.E@283889604 Hig /home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34	\checkmark	/home/tester/Documents/test_set/d89acc6e33d43de2fdd94bdabe1c4dba	
/home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34		Backdoor.HTML.EMO.E@283889604	High
	\checkmark	/home/tester/Documents/test_set/66a7ce7fdb4c46982dc66db6acb48a34	
/home/tester/Documents/test_set/671ff798d81f9540c4e1e8ba0372112e671ff798d8	\checkmark	/home/tester/Documents/test_set/671ff798d81f9540c4e1e8ba0372112e671ff798d8	

- **Clean** If a disinfection routine exists, CCS will remove the infection and retain the original file. If no routine exists, CCS will move the file to **Quarantine**.
- Ignore Two options:

Once - The file is removed from the threat results and remains in its current location. The file will be detected as a threat again by the next scan.

Add to Exclusions – Creates an exception for the file. The virus scanner will skip the file in future and not consider it to be a threat. The file is added to the Exclusions list.

- Save Results Export the scan results to a text file.
- Select 'All' if you want to apply 'Clean' or 'Ignore' actions to every threat.

Create a new scan profile

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

COMODO Creating Trust Online*

nat do these settings do?	Creat	e New Scan	Scan Clo
😣 Scan Profile 🗲		*****	
Name:			
List of items to be scan	ined:		
Path			7

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

COMODO Creating Trust Online*

		+
xisting items		Selected items
Name ! Image: Second	Size Type Drive Folder	

There are two ways to add items:

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

OR

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

COMODO Creating Trust Online*

🛞 Scan Profile	
Name:	
Weekly Custom Scan Profile	
List of items to be scanned:	
Path /usr/share/misc/	7
/proc/11/map_files/	
	Add Remove
What do these settings do?	Apply Cancel

• Click 'Apply' again to save the profile.

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

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

Instantly Scan Objects

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

COMODO Creating Trust Online*



See Run an Instant Antivirus Scan on Selected Items for more help with this.

View Antivirus Events

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

The basic event viewer shows:

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

View antivirus events

- Go to the home screen of CCS
- Click the number in front of 'threat(s) detected so far' on the home screen
 - Or
- Click 'More' > 'View Antivirus Events'

COMODO

COMODO Client -	Security					
OMODO	Summary	- Antivirus	0		More	
V	Antivirus State The virus database has bee attabase database has bee	ful n updated on Fri Apr 6 11:56:00 2 so far	018			
ems are active nning.	\checkmark		<u>© s</u>	can Now		
1	😣 🖻 💿 Antivirus Events					
	Location 🛆	Malware Name	Action	Status	Date	
	/home/tester/Documents	Malware@#34papd4xq0	Ignore	Success	17:52:30	
	/home/tester/Documents	TrojWare.HTML.Iframe.x	Ignore	Success	17:52:33	
	/home/tester/Documents	TrojWare.BAT.Agent.wa	Block	Success	17:54:33	1
	/home/tester/Documents	TrojWare.JS.TrojanDownl	Block	Success	17:56:33	
	/home/tester/Documents	Malware@#1e8yudwsrokrr	Ignore	Success	17:57:43	
	/home/tester/Documents	TrojWare.JS.Redirect.brn	Add To E	Success	17:57:49	
	/home/tester/Documents	Virus.VBS.Ramnit.c@298	Add To E	Success	17:57:53	
	/home/tester/Documents	TrojWare.VBS.StartPage	Quarantine	Success	17:57:55	
	/home/tester/Documents	Backdoor.PHP.Pbot.A@1	Quarantine	Success	17:57:56	
	/home/tester/Documents	Exploit.JS.Pdfka.cljk@27	Quarantine	Success	17:57:57	
	/home/tester/Documents	TrojWare.JS.Agent.rm@2	Quarantine	Success	17:57:58	
	/home/tester/Documents	TrojWare.HTML.Iframe.x	Quarantine	Success	17:58:04	
	,,,					

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

Configure Database Updates

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

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

The default policy of CCS for Linux:

i. Periodically check for and download database updates

ii. Automatically update the virus database before starting a scan.

See the following links for more details:

- Manually update the virus database
- Configure automatic database updates

Manually update the virus database

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

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

COMODO Creating Trust Online*



Configure automatic database updates

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

COMODO Creating Trust Online*

😣 Virus Scanner Settings						
Real Time Scanning	Manual Scanning	Scheduled Scanning	Exclusions			
Real-Time Scanning	Real-Time Scanning					
On Access	Dealt					
	- Real-ti - Everyt	hing is scanned on-acc	ess			
	- Threat do any l	s are going to be dete harm	cted before they can			
	2					
Disabled						
Detection						
💙 Automatically u	ipdate virus databa	se				
Automatically of	uarantine threats f	ound during scanning				
Show notificati	on messages					
Heuristics Scannin	g Level	Low -				
Do not scan files larger than (MB)		20				
Keep an alert on th	ne screen for (secor	ds) 120				
What do these set	tings do?		OK Cancel			

• Note - You can enable or disable pre-scan updates for manual and scheduled antivirus scan types.

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

Quickly Set up Security Levels

Right-click on the system tray icon:



Move your mouse cursor over 'Antivirus Security Level'



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

You can also access these settings from the summary screen.

Change CCS Language Settings

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

	COMODO Client - Security for	Linux 🕒 🗊 🥹
COMODO Client - Security	Summary 😵 Ar	ntivirus 😺 More
	Preferences	Browse Support Forums
All systems are active	This section lets you configure general settings like password protection, update options, language, theme etc.	Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.
and running.	Manage My Configurations	🚱 Help
And	This section allows you to import/export/delete your COMODO Client - Security configuration settings.	Do you want to learn more about your COMODO Client - Security? You can use this section to view the help file.
	Preferences	×
\bigcirc		_
Language Logging	Connection Update Device Control	
Language:	English(United States) - Default	
What do these set	tings do?	OK Cancel

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

сомодо

COMODO Creating Trust Online*



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

Run an Instant Antivirus Scan on Selected Items

You can instantly scan a file, folder or drive by dragging it into the scan box on the summary screen.

Instantly scan items:

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



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



The scan will begin immediately after the updates are installed.

😣 🖨 Scanning: My Cor	nputer	
Scanning: My Status: /us	Computer sr/src/linux-head	ers-4.10.0-40/arch/arm/lib/Makefile
Objects Scanned:	14776	Start Time: Wed Apr 4 16:26:27 2018
Threats Found:	0	Duration: 00:00:13
Show on top		
What do these setting	gs 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 multiple schedules.
- You can run scans at daily, weekly, monthly or custom intervals.
- Note: Managed endpoints You should configure scan schedules in an Endpoint Manager profile.

Create an antivirus scan schedule

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

COMODO Creating Trust Online*

🥮 🖨 🕘 COMODO Client - S	ecurity for Linux			
сомодо 【	Summary	Antivirus	\bigcirc	More
Client - Security All systems are active and running. Schedu Schedu Wee	Summary Run a Scan This section allows you to scan your have a scan spyware. Scheduled Scans This section allows you to modify the your scanning settings in order to have periodically scanned. Uled Scans le Name kly Virus Scanning Scan Schedule Name: Weekly Custom Schedule Deapfile:	Antivirus Update ard drive for This se databa Quarar scheduled ve your PC Use this quaran Use this quaran	e Virus Database ction allows you to o se and download th atined items s section to see and tined by the virus so	More theck for the latest virus e updates if any. manage the threats anner. Add Edit Remove
What o	Profile: My Computer Days of the week: Monday Tuesday Wednesday Friday Saturday Start time: 1 • : 00 • AN App	1 - ly Cancel	Apply	Cancel

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

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

COMODO Creating Trust Online*

Scheduled Scans	
Schedule Name Weekly Virus Scanning	Add
Weekly Custom Schedule	Edit Remove
What do these settings do? Appl	y Cancel

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

Restore Incorrectly Quarantined Item(s)

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

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

COMODO Creating Trust Online*



Click 'Restore'

All selected files will be moved back to their original locations. See Quarantined Items for more details.

Switch off Automatic Antivirus Updates

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

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

- Switch off automatic updates in general
- Switch off updates prior to manual scans
- Switch off updates prior to scheduled scans

Switch off automatic updates in general

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

Open Comodo Client Security

COMODO Creating Trust Online*

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



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

Switch off updates prior to manual scans

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

COMODO Creating Trust Online*

Se Security for Linux					
		Summary	Antivir	us More	
Cilent - Security		Run a Scan	2	Update Virus Database	
		This section allows you to scan your hard malware, viruses and spyware.	drive for	This section allows you to check for the latest virus database and download the updates if any.	
All systems are active		Scheduled Scans	٠	Quarantined Items	
and running.		This section allows you to modify the sch virus scanning settings in order to have y periodically scanned.	neduled Your PC	Use this section to see and manage the threats quarantined by the virus scanner.	
	- 8	Scan Profiles		Scanner Settings	
		Use this section to add/remove new scan profiles which are used by the virus scan determine the objects to be scanned	nning ner to	This section allows you to change the advanced settings that affect how the virus scanner works.	
8 Virus Scanner Settings					
6					
la P	Real I In	ne Scanning Manual Scannir	Schedule	ed Scanning Exclusions	
	Detec	tion			
	× Sca	n archive files (e.g. *.zip, *.ra)		
 Automatically update virus database before scanning Enable cloud scanning 					
	Do no	t scan files larger than (MB)	20		
0	What	do these settings do?		OK Cancel	

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

Switch off updates prior to scheduled scans

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

COMODO Creating Trust Online*



• Click 'OK'.

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

Control External Device Accessibility

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

Configure device control

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

COMODO Creating Trust Online*

	COMODO Client - Security for L	inux 😑 🖻
	Summary 🔯 Ant	civirus 😺 More
	Preferences	Browse Support Forums
Il systems are active	This section lets you configure general sattings like password protection, update options, language, theme etc.	Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.
nd running.	Manage My Configurations	👰 Help
	This section flows you to import/export/delete your COMODO Client - Security onfiguration settings.	Do you want to learn more about your COMODO Client - Security? You can use this section to view the help file.
	Preserences	
Language Logging	Connection Update Device Control)
Enable Device Con This option bloc Log detected devi	ntrol cks devices of a client computer from accessin ces	ng, such as USB Storage devices
Exclusions Device Na	me / Identification	- bbA
		Edit
		Remove
		Keniove
1		[1] Þ
What do these sett	ings do?	

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

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street Clifton, NJ 07013 United States Tel : +1.877.712.1309 Tel : +1.888.551.1531 https://www.comodo.com Email: EnterpriseSolutions@Comodo.com