

COMODO
CYBERSECURITY



Comodo Client Security

Software Version 12.5

Quick Start Guide

Guide Version 12.5.111820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013
United States

Comodo Client Security - Quick Start Guide

This tutorial explains how to setup and use Comodo Client Security (CCS).

- **Installation**
- **Start CCS**
- **The main interface**
- **Scan and clean your computer**
- **Run an instant antivirus scan on selected items**
- **Set up the Firewall for maximum security and usability**
- **Set up HIPS for maximum security and usability**
- **Run untrusted programs in the container**
- **More Help**

Installation

You can deploy Comodo Client Security on to your endpoints, through the Dragon Enterprise interface.

- Sign up for Dragon Enterprise at <https://enterprise.platform.comodo.com/signup>, if you haven't done so.
OR
- Login to your Dragon Enterprise account at <https://enterprise.platform.comodo.com/login>.

The following tutorial covers user and device enrollment before moving onto CCS installation:

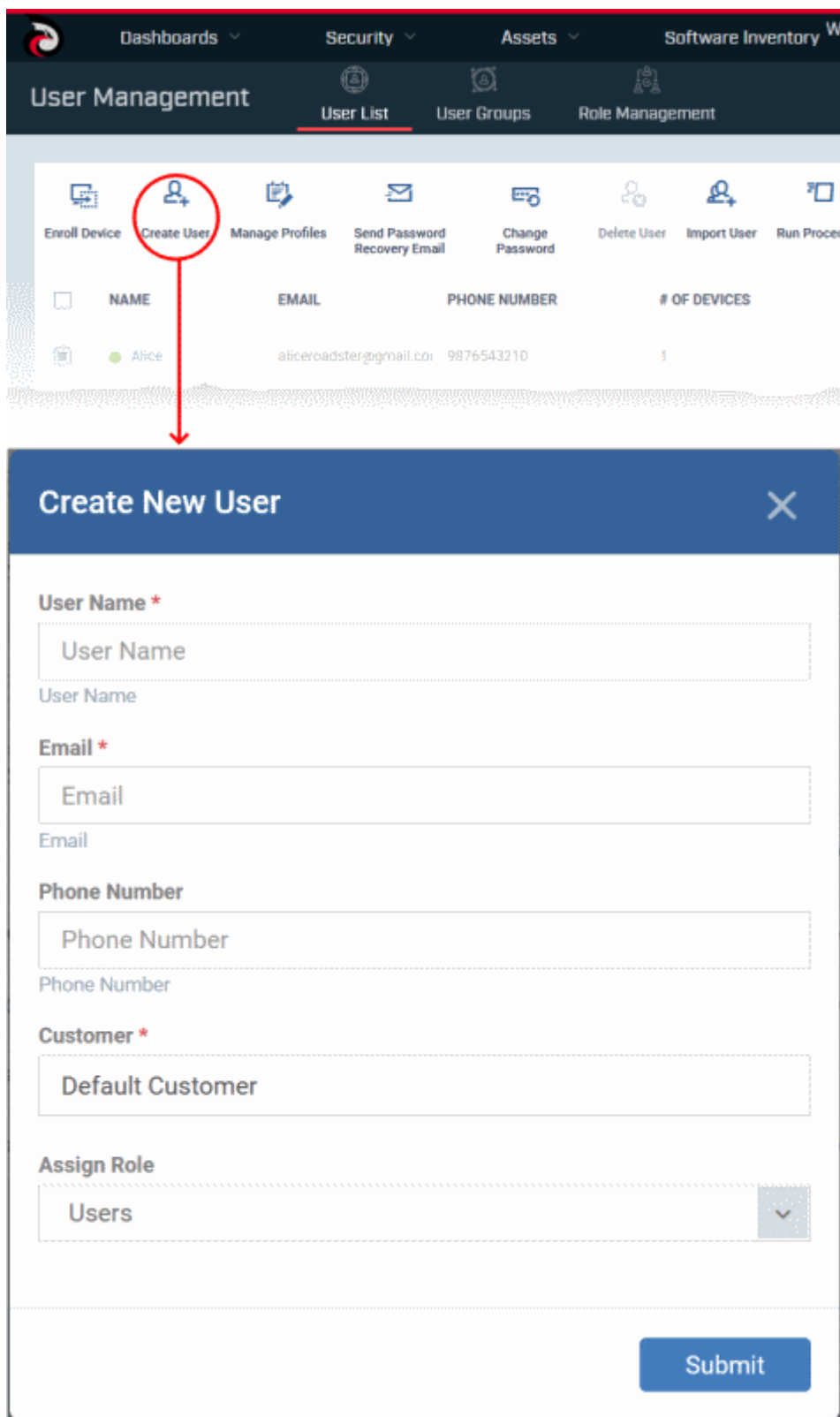
- **Enroll users**
- **Enroll devices**

Enroll Users

You must add users to Dragon Enterprise before you can deploy CCS to their endpoints.

Add a user

- Click 'Assets' > 'User Management' > 'User List'
- Click the 'Create User' button



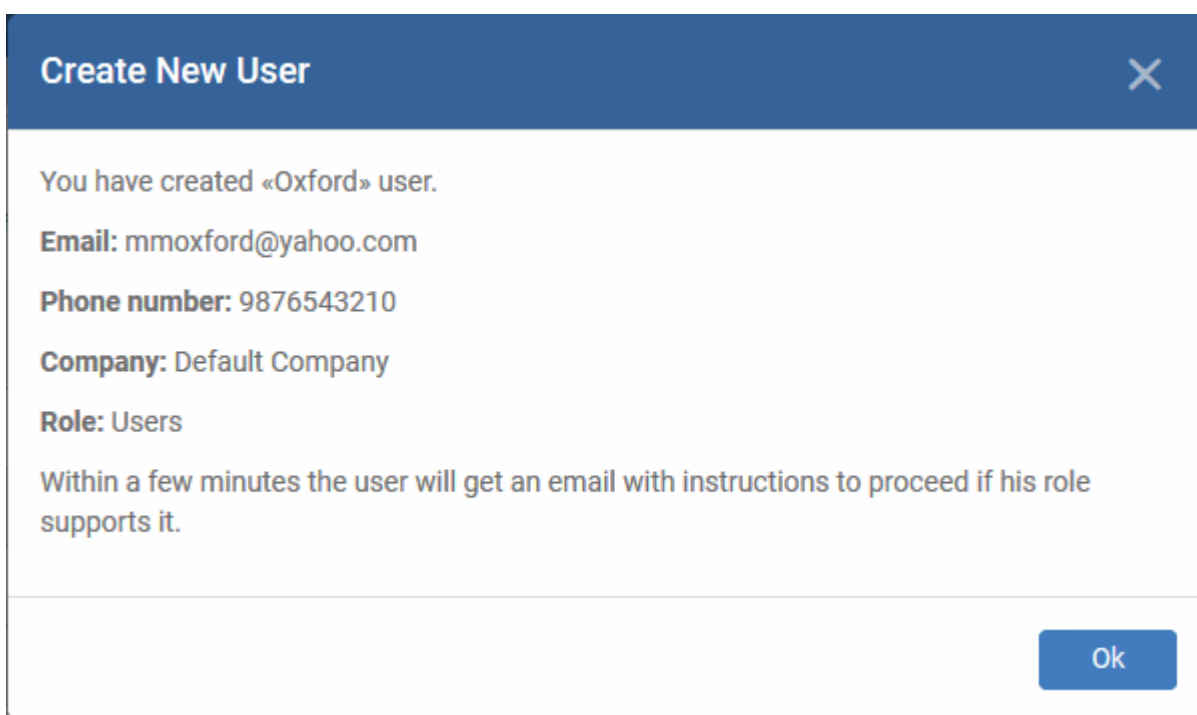
Complete the new user form:

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- **Customer** - The company to which the user belongs. Leave the customer as 'Default Customer'
- **Role**

A 'role' determines user permissions within the Dragon Enterprise console itself. Dragon Enterprise ships with four default roles:

- **Administrators** - Can login to Dragon and access all management interfaces. This role can be edited as required.
- **Technician** - Can login to Dragon and access all management interfaces. The technician role has fewer privileges than the administrator role. This role can be edited as required.
- **Login permission** - Can login to Dragon. Users with role cannot access any management interface by default. You can edit the role to assign access to required management interfaces.
- **Users** - In most cases, a user is simply an owner of a managed device. They should not require access to the Dragon Enterprise console. Under default settings, users cannot login to Dragon Enterprise.
- Users assigned with roles that provide login to the Dragon console will receive an account activation mail for activating their account. See **Configure Role Based Access Control for Users** for more details.
- Click 'Submit' to add the user to Dragon Enterprise.

A confirmation is shown:



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

Tip: You can also bulk import users from a .csv file. See <https://help.comodo.com/topic-463-1-1029-15558-Import-Users-from-a-CSV-File.html> for more details.

Enroll Devices

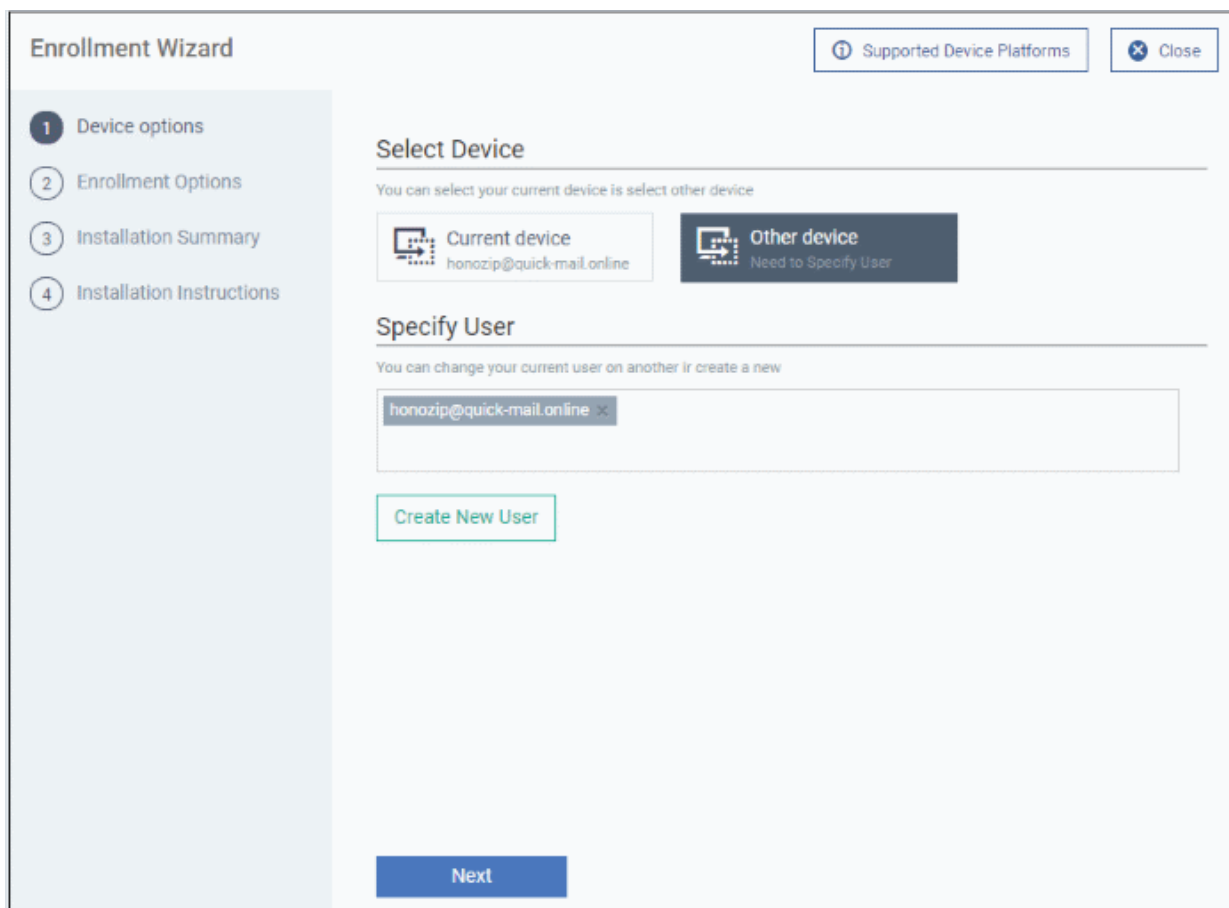
The next step is to add user devices so you can manage them with Dragon Enterprise.

- Click 'Assets' > 'User Management' > 'User List'
- Select the users whose devices you want to add then click 'Enroll Device'.

This starts step 1 of the device enrollment wizard:

Step 1 - Device Options

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



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

Step 2 - Enrollment Options

Enrollment Type

Applies to Windows, Mac and Linux devices.

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

Background. There are two types of client:

- **Communication Client** - Connects the device to Dragon Enterprise for central management. It is mandatory to install this client.
- **Security Client** - This is the security software, CCS.

Enrollment Wizard

Supported Device Platforms | Enrollment Instruction | Close

1 Device options
2 Enrollment Options
3 Installation Summary
4 Installation Instructions

Select Operating System of The Device

Windows | Linux | macOS | iOS
Android | Not Specified

Select Enrollment Type

Notice, Enroll and Protect require device reboot and Enroll doesn't require.

Enroll and Protect (Recommended) | Just Enroll

Choose platform: Windows x64

Additional options:
 Include initial Antivirus signature database (will apply only if a profile contains Antivirus section)

Configuration Profile *
Windows - Security Level 1 Profile v.6.38

By default Installation Package will be prepared with «Windows - Security Level 1 Profile v.6.38». If you want change it input profile name into the field

Set Reboot Options

TLDR

- Click 'Not Specified' if you only want to install the communication client on target devices. The wizard will detect the target operating system and send the appropriate client to the device user.
- Click one of the operating system tiles if you also want to install the security client. Make sure the target devices use the operating system you selected.

Option 1 - Enroll + Protect - Single Operating System

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

Option 2 - Enroll Only - Multiple Operating Systems

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

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

OR

See the tables below for more information about the options on this page:

Setting	Description
Choose platform	Select Window OS version. 64 bit, 32 bit, or hybrid. The hybrid package will auto-detect and install the correct version.
Use default Communication Client version	This client enrolls the endpoint for central management. <ul style="list-style-type: none"> • You can only change the CCC version if enabled in portal settings. If the option is not enabled then the 'Default version' is deployed.
Use default Comodo Client Security version	This client installs security software such as antivirus, firewall and auto-containment. <ul style="list-style-type: none"> • You can only change the CCS version if enabled in portal settings. If the option is not enabled then the 'Default version' is deployed.
Additional options	AV Database - Choose whether to include the latest virus database with the installation package. This increases the size of the package. If disabled, the client will download the latest database anyway when you run the first virus scan.
Configuration Profile	A configuration profile is a collection of settings which specify a device's network access rights, security settings, antivirus scan schedule, and more. The default is 'Windows - Security Level 1' profile. Choose a different profile if required. <ul style="list-style-type: none"> • The default profile is recommended for most users and can always be changed later if required. • If you want to change it, type the first few characters of a profile name and choose from the suggestions that appear. • You can view the settings in a profile at 'Configuration Templates' > 'Profiles'.
Set Reboot Options	Endpoints need to be restarted to complete CCS installation. You have the following restart options: <ul style="list-style-type: none"> • Force the reboot in... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message is shown to the user prior to the restart. • Suppress reboot - Endpoint is not auto-restarted. The installation is finalized when the user next restarts the endpoint. • Warn about reboot and let users postpone it - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens.

	Optional. Type a custom message in the 'Reboot Message' field.
Device Name Options	<ul style="list-style-type: none"> Do Not Change - The device's existing name is used to identify the device in Dragon Enterprise. Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.

- Click 'Next' to proceed to step 3

Step 3 - Installation Summary

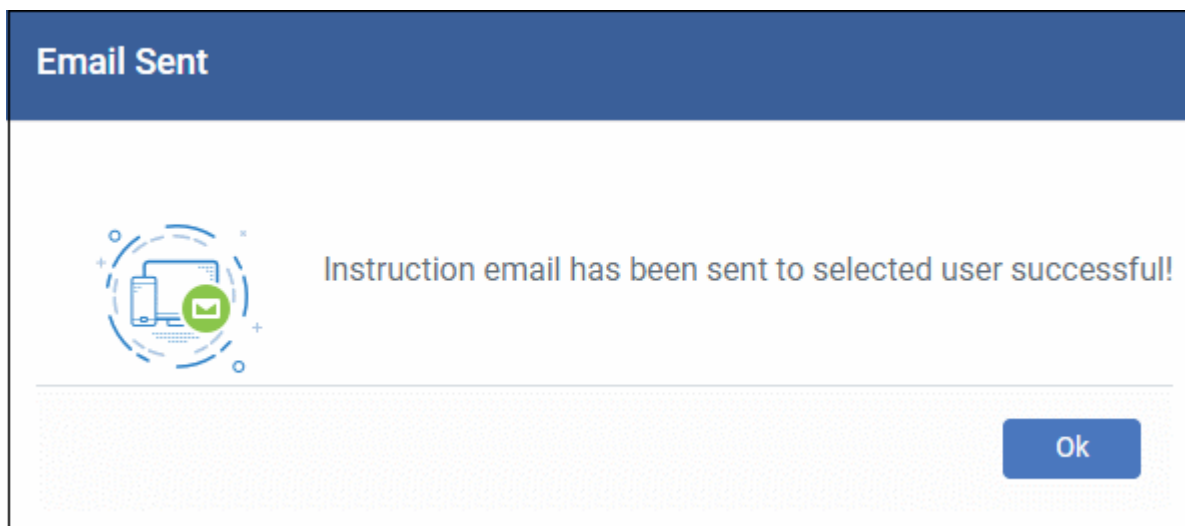
Review your choices so far.

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

Step 4 - Installation Instructions

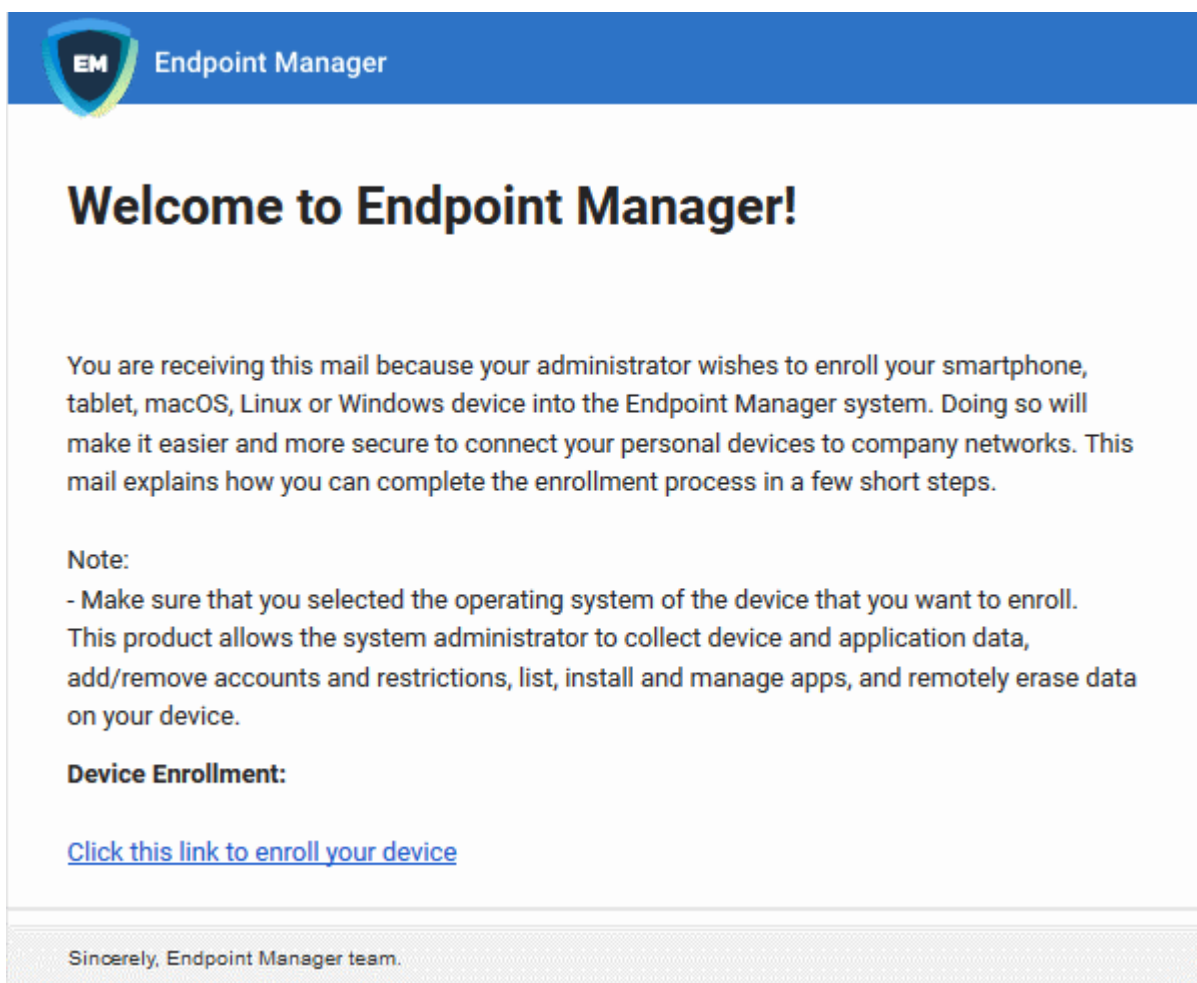
The final step is to send out the enrollment emails to the device owners:

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



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

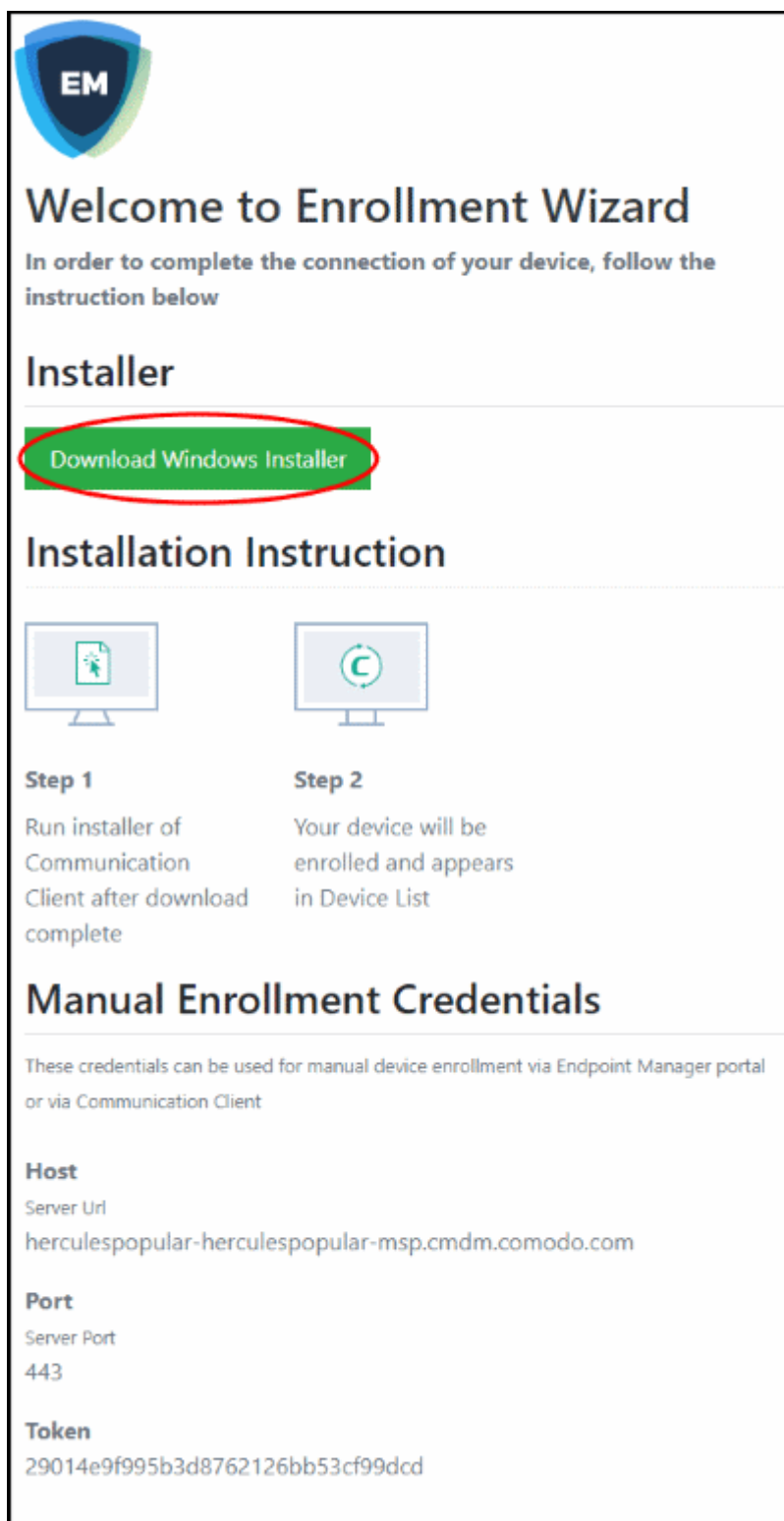
An example mail is shown below:



The user experience is as follows:

- User opens the email on the Windows endpoint you want to enroll.
- Click the enrollment link in the email to open the device enrollment page

- Click the 'Download Windows Installer' button:



EM



Welcome to Enrollment Wizard

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

Installer

Download Windows Installer

Installation Instruction

	
Step 1	Step 2
Run installer of Communication Client after download complete	Your device will be enrolled and appears in Device List


Manual Enrollment Credentials

These credentials can be used for manual device enrollment via Endpoint Manager portal or via Communication Client

Host
Server Url
herculespopular-herculespopular-msp.cmdm.comodo.com

Port
Server Port
443

Token
29014e9f995b3d8762126bb53cf99dcd

- The Dragon client setup file gets downloaded.
- Run the setup file to install the client on the endpoint.
- The device is automatically added to Dragon Enterprise once installation is complete. The Dragon Enterprise communication client icon  appears at the bottom-right of the endpoint screen.
- If the client is not automatically enrolled after installation, you can manually enroll the device at a later time. This might happen if, for example, there are connectivity issues.

- You will need to enter the host, port and token ID to manually enroll. You can find these items at the end of the device enrollment page.
- Protection is effective immediately after the computer restarts.

A Dragon Enterprise security profile is applied to the device.

- If the user is already associated with a configuration profile in Dragon Enterprise, then those profiles will be applied to the device. See '[Assign Configuration Profile\(s\) to User Devices](#)' and '[Assign Configuration Profiles to a User Group](#)' for more details.
- If no profiles are defined for the user then the default Windows profile(s) will be applied to the device. See '[Manage Default Profiles](#)' for more details.

The device can now be remotely managed from the Dragon Enterprise console.

Start CCS

- After installation, CCS will automatically load whenever the endpoint starts.
- Real-time protection is enabled by default, so endpoints are protected immediately after the restart.
- We recommend you use a Dragon Enterprise configuration template to manage CCS settings:
 - Log into Dragon Enterprise, click 'Assets' > 'Configuration Templates' > 'Profiles'
 - See <https://help.comodo.com/topic-463-1-1029-15670-Profiles-for-Windows-Devices.html> for help to build and deploy a configuration profile.
- However, you can also configure the application at a local machine should you wish. The rest of this guide addresses how to use configure and use the application locally.

What is a Dragon Enterprise profile?

- Dragon Enterprise is a product which allows admins to manage Comodo Client Security on network endpoints.
- A Dragon Enterprise profile is a template which contains all the security settings and privileges that the admin wants to implement on the endpoint.
- Admins can allow local changes to CCS by activating 'Enable local user to override profile configuration'. See <https://help.comodo.com/topic-463-1-1029-15686-Client-Access-Control.html> for help with this.

CCS has two modes:

- **Normal Mode** - Allows you to access the entire CCS interface.
- **Virtual Desktop Only Mode** - You can only open the Virtual Desktop and Virtual Desktop settings.

The mode available to you depends on the Dragon Enterprise profile active on the device.

Normal Mode

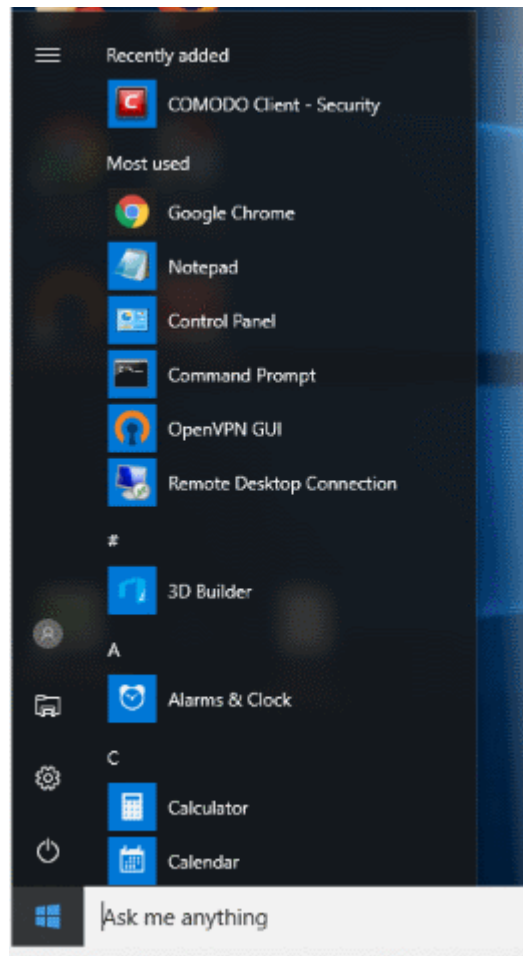
There are 5 different ways to open CCS on an endpoint:

- **Windows Start Menu**
- **Windows Desktop**
- **Widget**
- **System Tray Icon**
- **Windows Defender**

Start Menu

- Click **Start** and select **All Apps > Comodo > Comodo Client Security**

Note - the start menu varies slightly for different versions of Windows:



Windows Desktop

- Double-click the CCS desktop shortcut to open the app.
- Note - The shortcut is only visible if 'Show Desktop Shortcut' is enabled in the Dragon Enterprise profile applied to the endpoint.



Widget

- Just click the information bar in the widget to start CCS. The widget is only visible if 'Show Desktop Widget' is enabled in the Dragon Enterprise profile applied to the endpoint.



The widget also contains other useful data and features. See '[The Widget](#)' for more details.

CCS Tray Icon

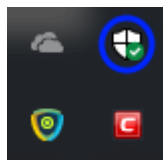
- Double-click the shield icon to open the application:



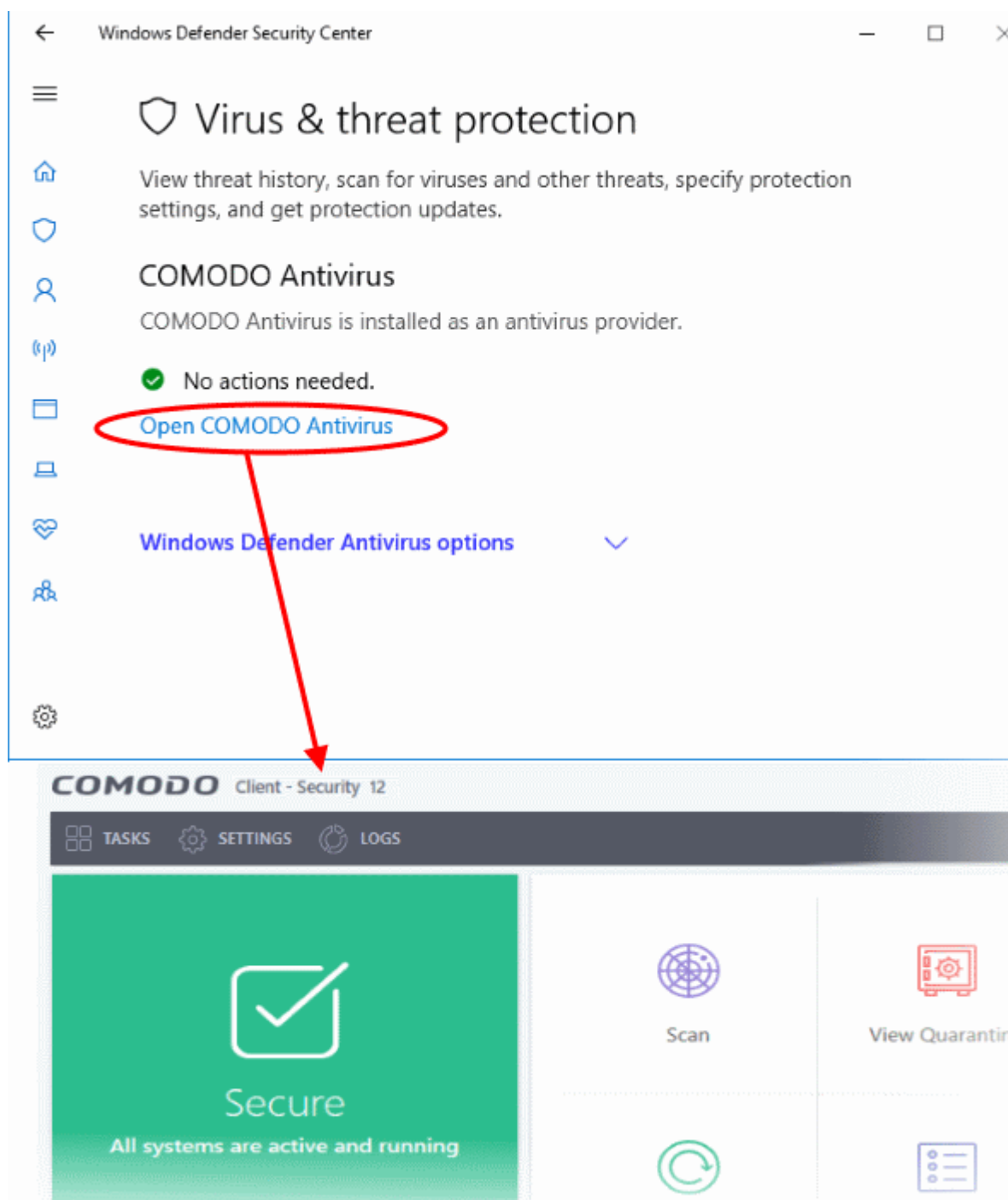
You can also right-click on the tray icon and select 'Open...!'

Windows Defender

- Double-click on the Windows Defender icon to open the application
OR
- Right-click on the tray icon and select 'Open...!'



- Click the 'Virus & threat protection' tile
- Click 'Open COMODO Antivirus':

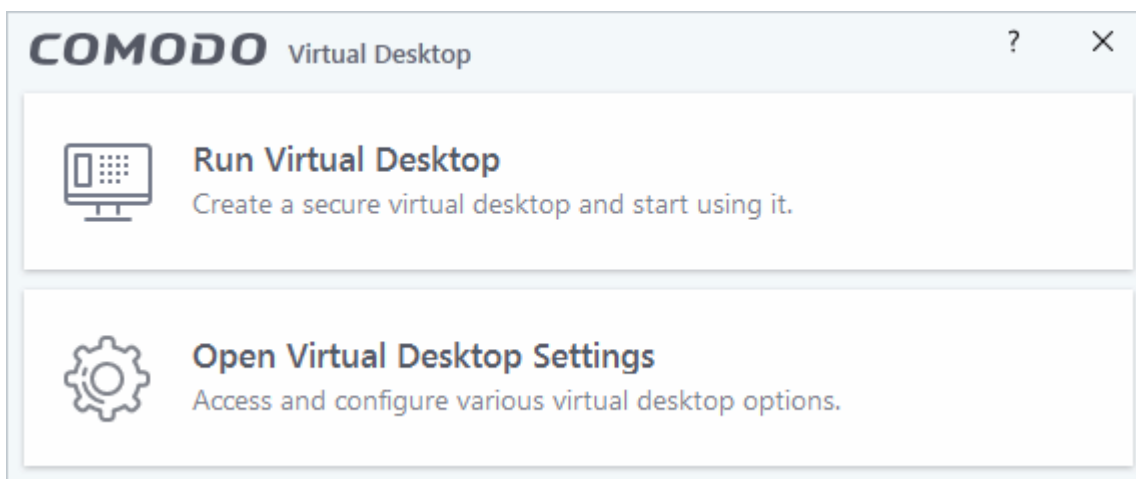


Virtual Desktop Only mode

- This mode means you can only open the Virtual Desktop and access Virtual Desktop settings. You cannot access any other areas of the CCS interface.
 - Dragon Enterprise admins - You can enable or disable this setting in the 'UI Settings' section of a profile.
 - See <https://help.comodo.com/topic-463-1-1029-15684-Communication-Client-and-Comodo-Client---Security-Application-UI-Settings.html> if you want to read more on this.

In 'Virtual Desktop Only' mode:

- The system tray icon and the desktop widget are hidden
- The CCS desktop shortcut and Windows start menu entry lead to the following menu:

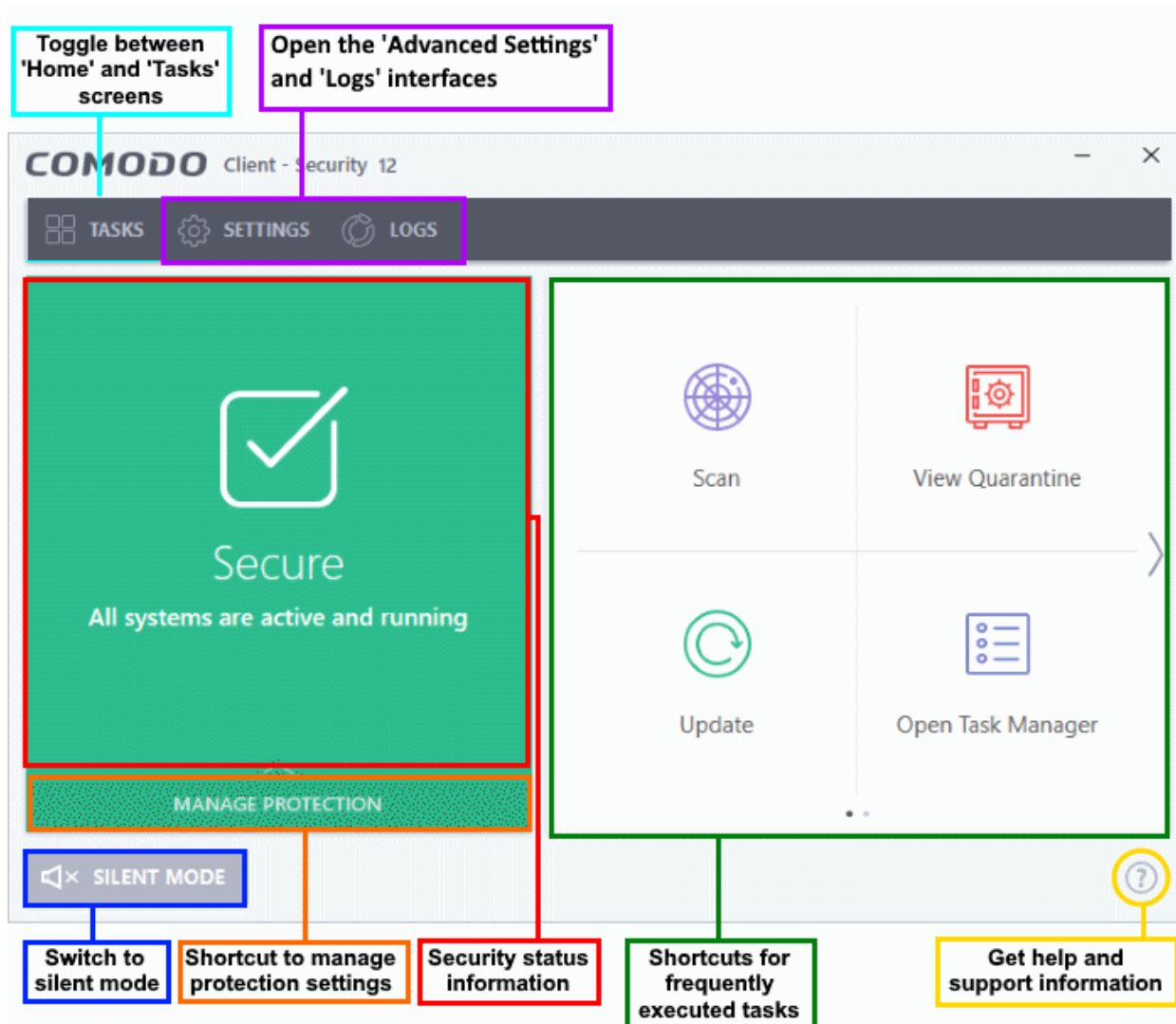



- **Run Virtual Desktop** - Opens the virtual desktop. See [The Virtual Desktop](#) for more help on this.
- **Open Virtual Desktop Settings** - Opens the virtual desktop settings area in CCS. See [Virtual Desktop Settings](#) for help with these settings.

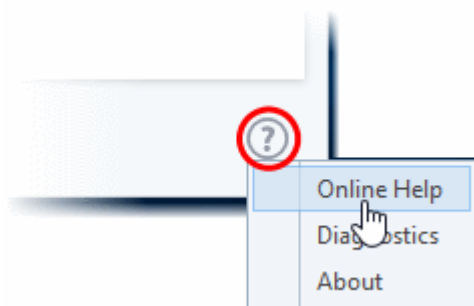
End-users cannot access any other area of CCS.

The Main Interface

The CCS interface is designed to be as clean and informative as possible while letting you carry out tasks with the minimum of fuss.



- Overall security status is shown in the large box on the left. This box will show a large red 'X' if there are security issues. The 'Fix It!' button in the same box allows you to remediate the issue.
- Click the 'Home'/'Tasks' button at the upper-left to switch between the home screen and the tasks interface.
- The tiles on the right give you one-click access to important features, including the antivirus scanner, updates, task manager and more.
 - Add tasks to this area - click the 'Tasks' button at top-left then click the 'pin' icon  next to your desired task .
- Click 'Scan' to run an instant antivirus scan
- The 'Manage Protection' button lets you turn security components on or off.
- Switch on 'Silent Mode' to suppress alerts. Make sure nothing interrupts you during presentations or gaming sessions. All protection technologies remain fully active while in silent mode.
- The help icon at the bottom-right corner contains the following options:



- **Online Help** - Opens Comodo Client Security's online help guide at <https://help.comodo.com>.
- **Diagnostics** - Helps to identify any problems with your installation.
- **About** - Contains version details and legal information.

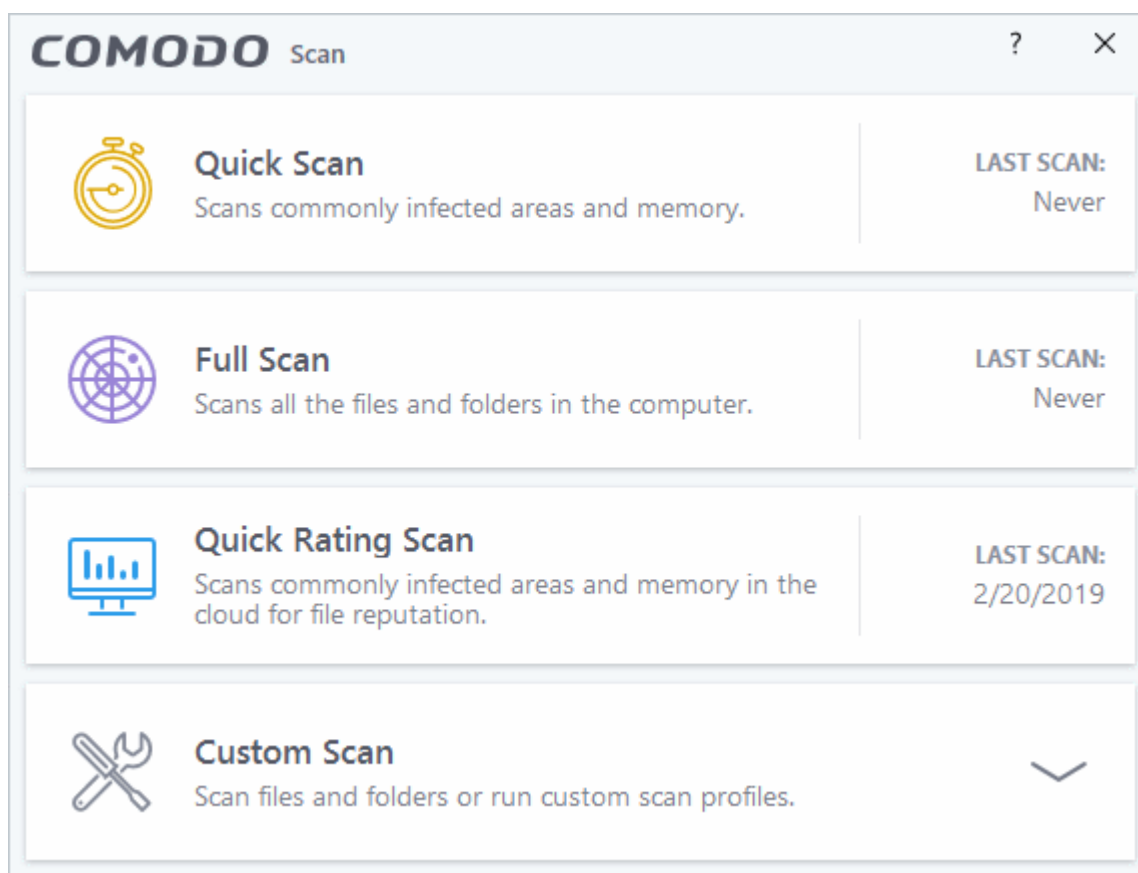
Scan and Clean your Computer

- Click 'Tasks' > 'General Tasks' > 'Scan'
- CCS leverages multiple technologies to keep endpoints free of malware, including real-time threat monitoring and on-demand scans.
- You can schedule a scan to run at a certain time and create custom scan profiles to check specific items.

Run an on-demand virus scan

- Click the 'Scan' tile on the CCS home screen
- Or
- Click 'Tasks' > 'General Tasks' > 'Scan'

Any of these methods will open the scan selection screen:



- **Quick Scan** - Checks important and commonly infected areas
- **Full Scan** - Checks your entire computer

- **Rating Scan** - Searches for unknown files on your computer. Assigns a trust rating to your files where possible.
- **Custom Scan** - You choose specific areas to scan

Run a Quick Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Quick Scan'
- The quick scan profile scans important areas of your computer which are most prone to attack.
- This includes system files, auto-run entries, hidden services, boot sectors, and important registry keys.
- These areas are of great importance to the health of your computer, so it is essential to keep them free of infection.
 - Note - You can change the settings of a quick scan in 'Settings' > 'Antivirus' > 'Scans'.
 - See <https://help.comodo.com/topic-463-1-1033-15923-Scan-Profiles.html> for help with this.

Run a quick scan

- Click the 'Scan' button on the CCS home screen
- OR
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Quick Scan'
- CCS will download the latest database updates then start the scan.
- To pause, resume or stop the scan, click the appropriate button at the bottom of the interface

Note - CCS skips files which are larger than the max. size, and those that take longer to scan than is allowed. These thresholds are set in the 'Quick Scan' profile, which can be viewed in CCS at 'Settings' > 'Antivirus' > 'Scans'.

- Results are shown at the end of the scan. The results show the number of items scanned, a list of all discovered threats, and the files that were skipped.
- You have the following options if threats are found:
 - Clean - Will delete the file
 - Quarantine - Moves the file into a secure, encrypted holding area. Quarantining a file renders it harmless
 - Ignore - Allow the file. You can choose to ignore one-time-only, or ignore and create an exclusion (permanently ignore)

Run a Full Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Full Scan'
- A full scan checks every file, folder and drive on your computer. USB and other external drives are also scanned.
 - Note - You can change the settings of the full scan profile in 'Settings' > 'Antivirus' > 'Scans'.
 - See <https://help.comodo.com/topic-463-1-1033-15923-Scan-Profiles.html> for help with this.

Run a full computer scan

- Click the 'Scan' button on the CCS home screen
- OR
- Click 'Tasks' > 'General Tasks' > 'Scan'

- Select 'Full Scan'
- CCS will download the latest database updates then start the scan.
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'

Note: CCS skips files which are larger than the max. size, and those that take longer to scan than is allowed. These thresholds are set in the 'Full Scan' profile, which can be viewed in CCS at 'Settings' > 'Antivirus' > 'Scans'.

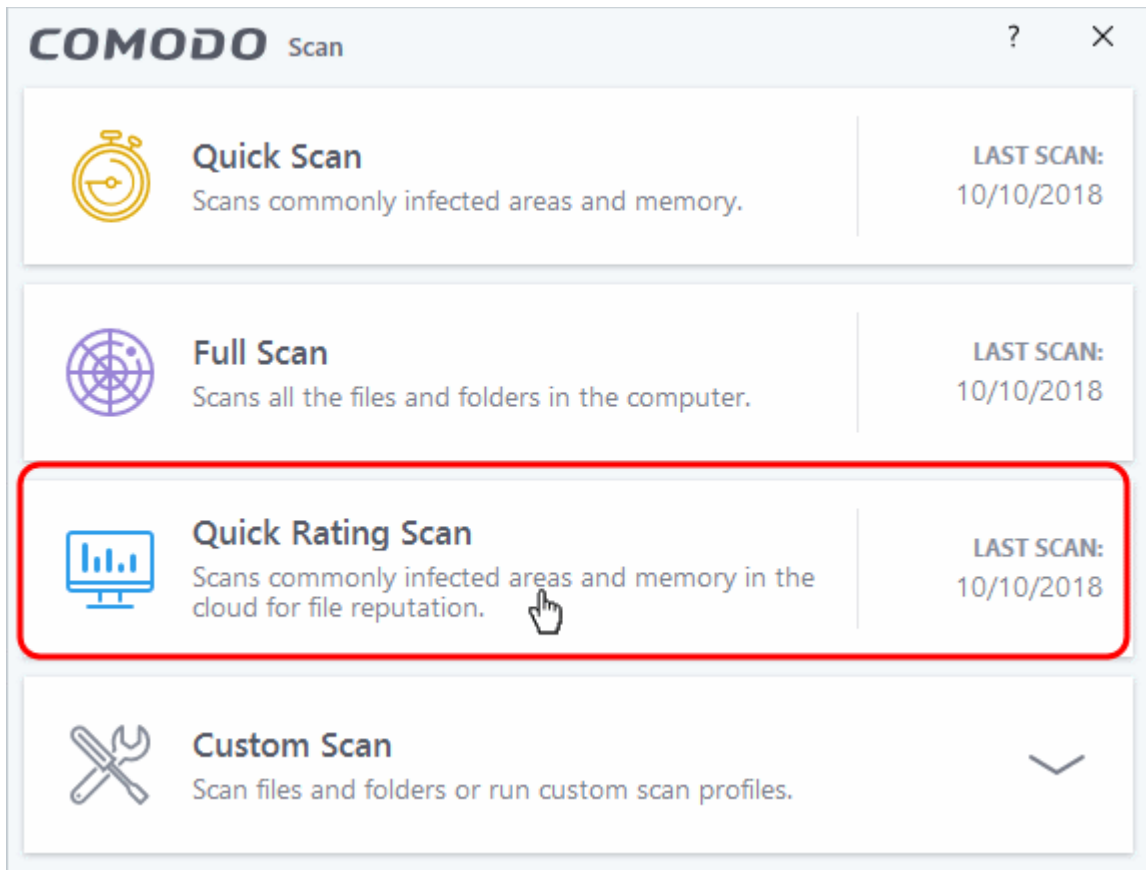
- Results are shown at the end of the scan. The results show the number of items scanned, a list of all discovered threats, and the files that were skipped.
- You have the following options if threats are found:
 - Clean - Will delete the file
 - Quarantine - Moves the file into a secure, encrypted holding area. Quarantining a file renders it harmless
 - Ignore - Allow the file. You can choose to ignore one-time-only, or ignore and create an exclusion (permanently ignore)

Run a Rating Scan

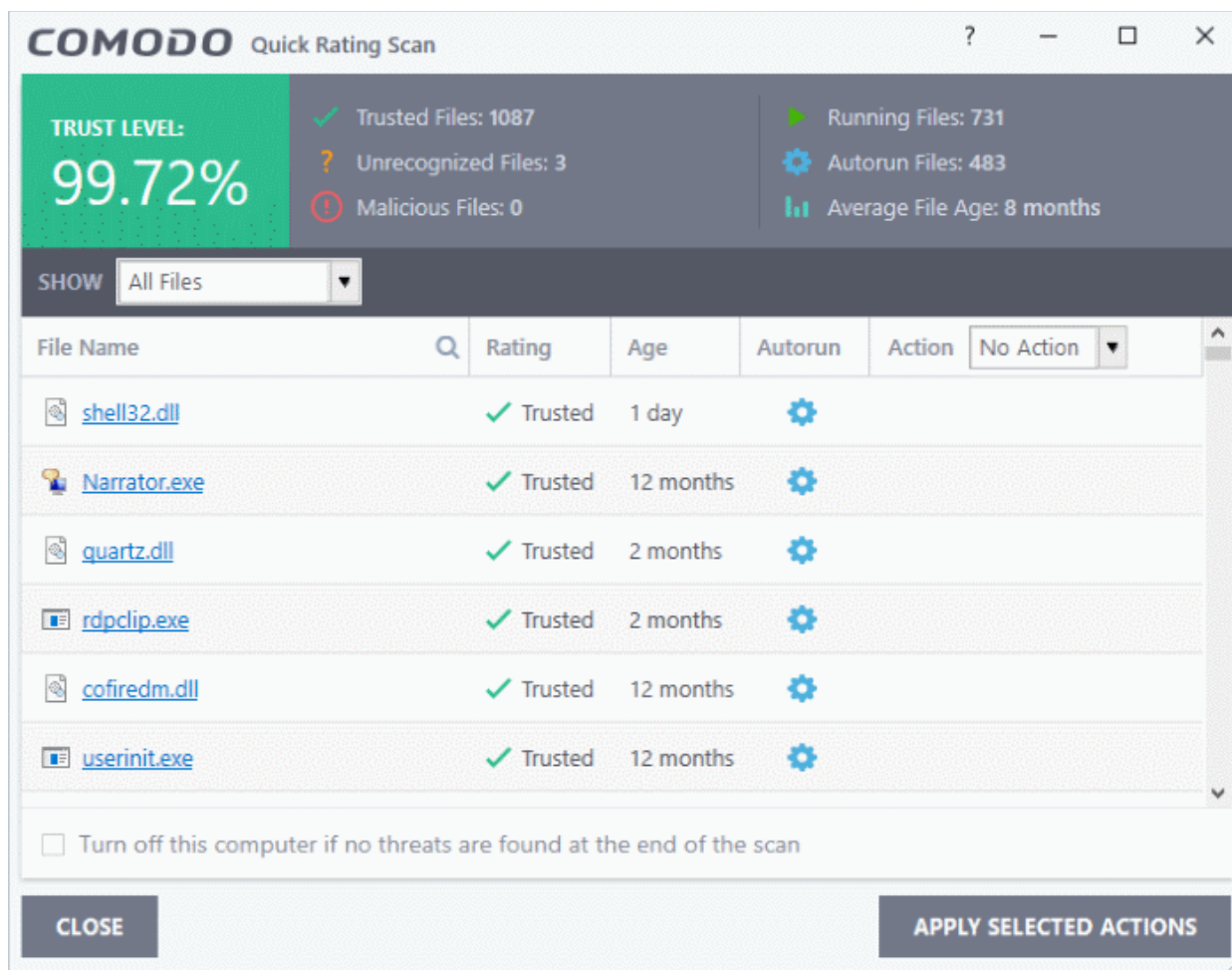
- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Rating Scan'
- A rating scan checks the trust-rating of all executable files on your computer.
- Trust ratings are as follows:
 - **Trusted** - The file is safe to run.
 - **Malicious** - The file is malware. Depending on your settings, CCS will either quarantine the file or present you with disinfection options.
 - **Unrecognized** - Comodo does not currently have a trust rating for the file. Unrecognized files should be run in the container to prevent them potentially attacking your computer. You can simultaneously submit them to Comodo for a trust-rating analysis.

Run a quick rating scan

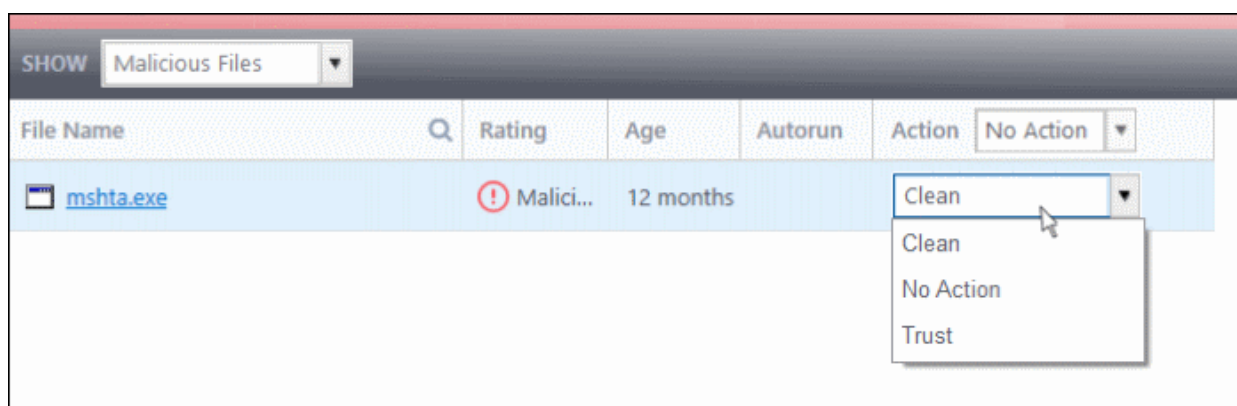
- Click the 'Scan' button on the CCS home screen
OR
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Quick Ratings Scan':



- Results are shown at the end of the scan. The results show the number of items scanned and a list of all discovered threats.



Each file is rated as 'Trusted', 'Unrecognized' or Malicious. The drop-down menus next to unrecognized and malicious files give you the following options:



- **Clean** - Available only for malicious items. The threat is placed in quarantine for your review. Click 'Tasks' > 'General Tasks' > 'View Quarantine' to open this area. You can restore or permanently delete files from quarantine as required
- **No Action** - Ignores the warning this time only. The file not placed in quarantine. Use this option with caution. The file will be caught again by the next rating scan you run.
- **Trust** - The file is awarded trusted status in the local 'File List' ('Settings' > 'File Rating' > 'File List'). The file will be excluded from any future rating scans. Only select this option if you are sure the item is trustworthy.

You can apply an action to multiple files as follows:

- Select your preferred action from the drop-down menu at top-left

- Select all files to which you want to apply the action
- Click 'Apply Selected Actions'

Run a Custom Scan

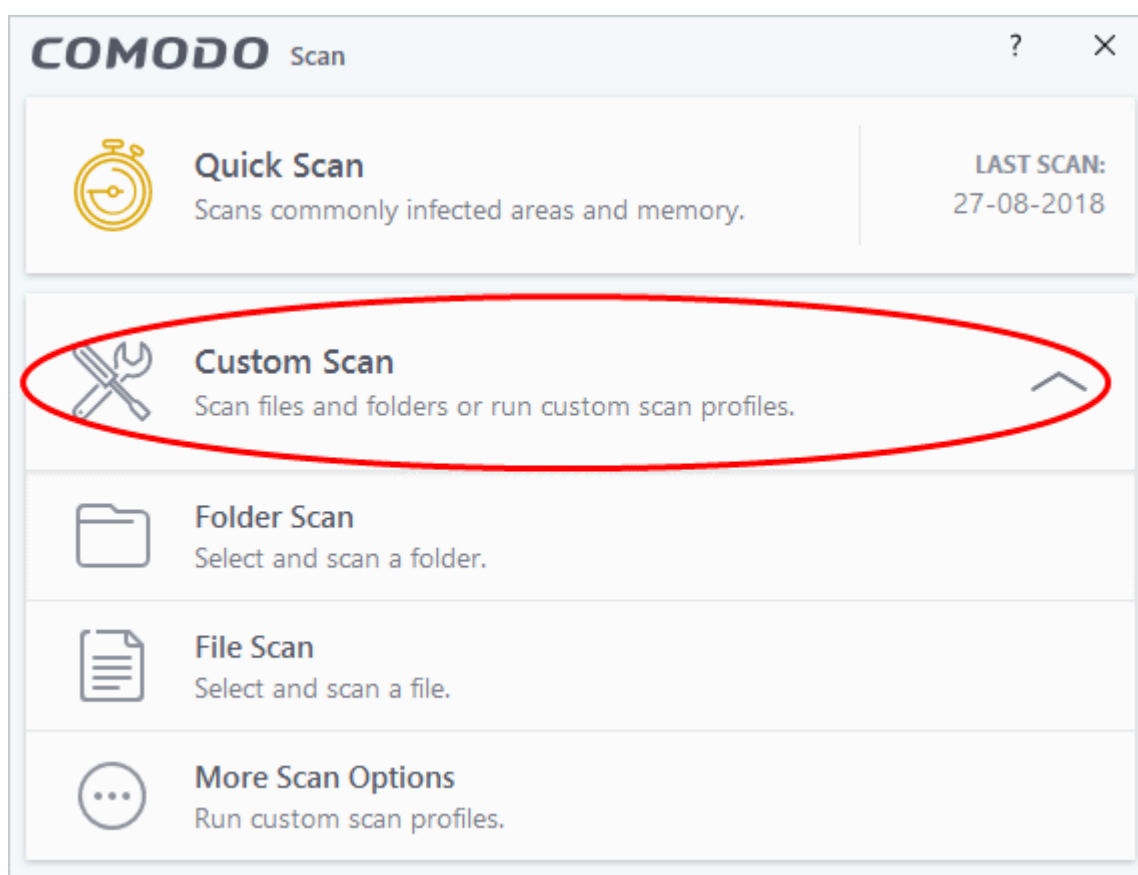
- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan'
- A custom scan lets you check specific files, folders, drives and areas on your computer.

Run a custom scan

- Click the 'Scan' button on the CCS home screen

OR

- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Custom Scan':



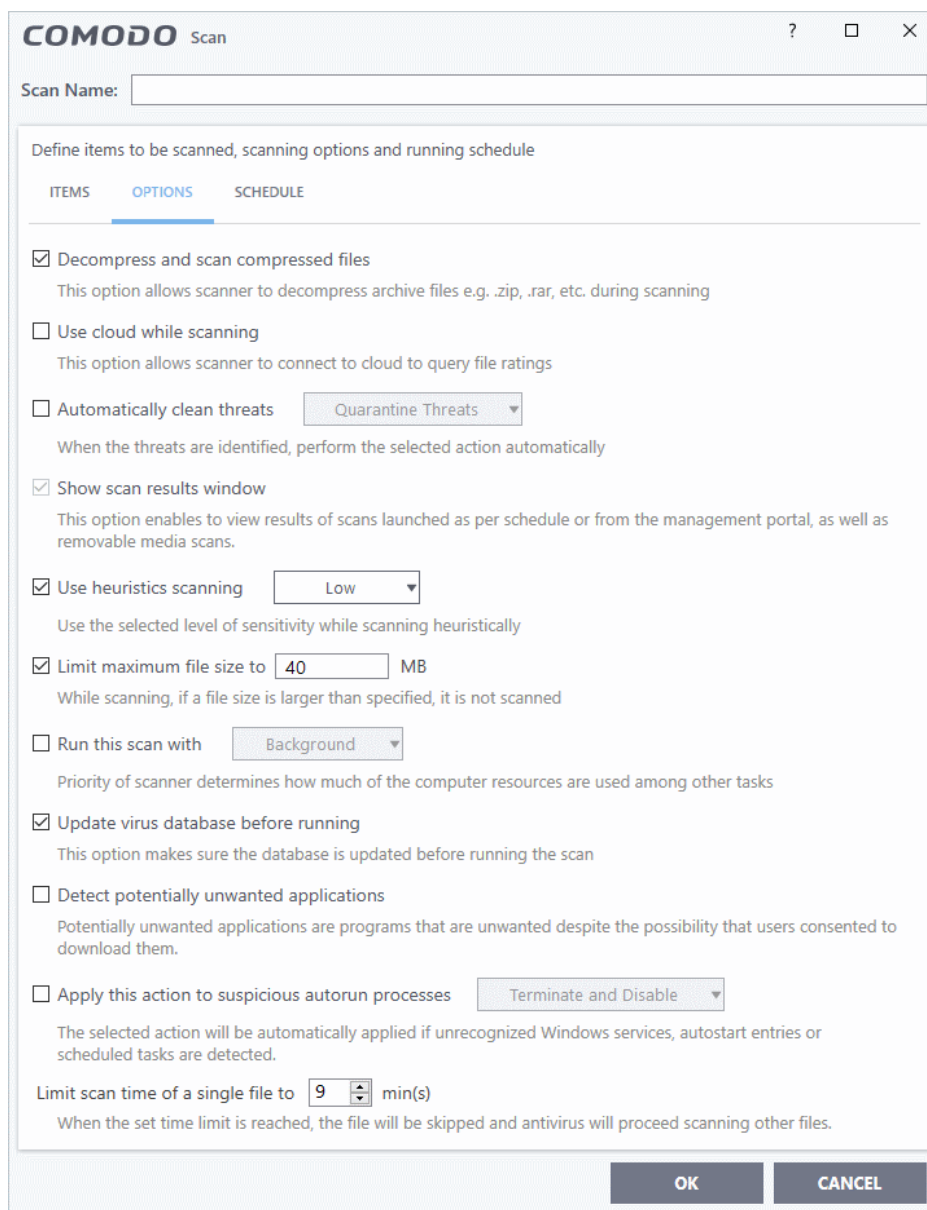
You have the following options:

- **Scan a folder** - Scan the contents of folders and sub-folders.
- **Scan a file** - Scan a specific file stored on your hard drives or external devices.
- **More Scan options** - Create a custom profile to scan specific files and folders.

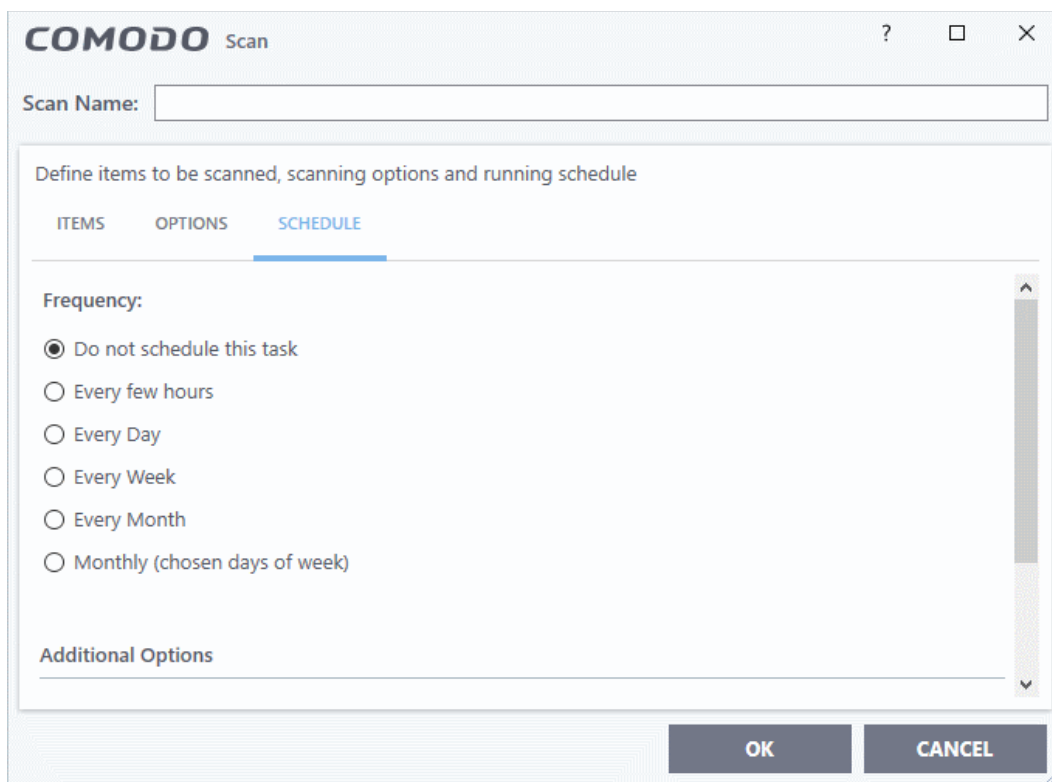
Create a custom scan profile

- Click 'Scan' on the CCS home screen
- Click 'Custom Scan' > 'More Scan Options'
- You will see a list of all existing scan profiles.

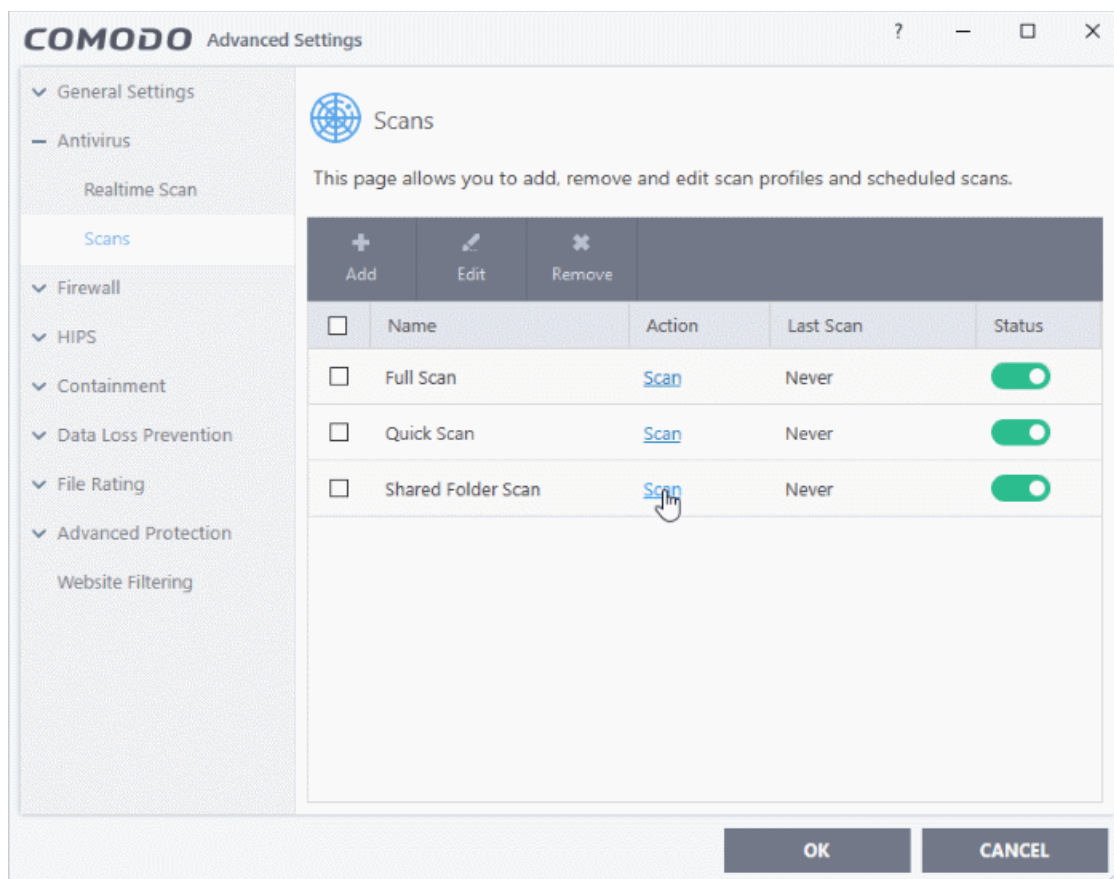
- Click 'Add' to create a new profile
- Type a name for your profile
- Use the buttons at the top to add items to your profile:
 - **Add File** - Pick individual files that you want to scan.
 - **Add Folder** - Add entire folders to the profile. All files in the folder are covered by the scan.
 - **Add Area** - Scan a computer region. The choices are 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.
- Repeat the process to add more items to the profile.
- Click 'Options' to further customize the scan



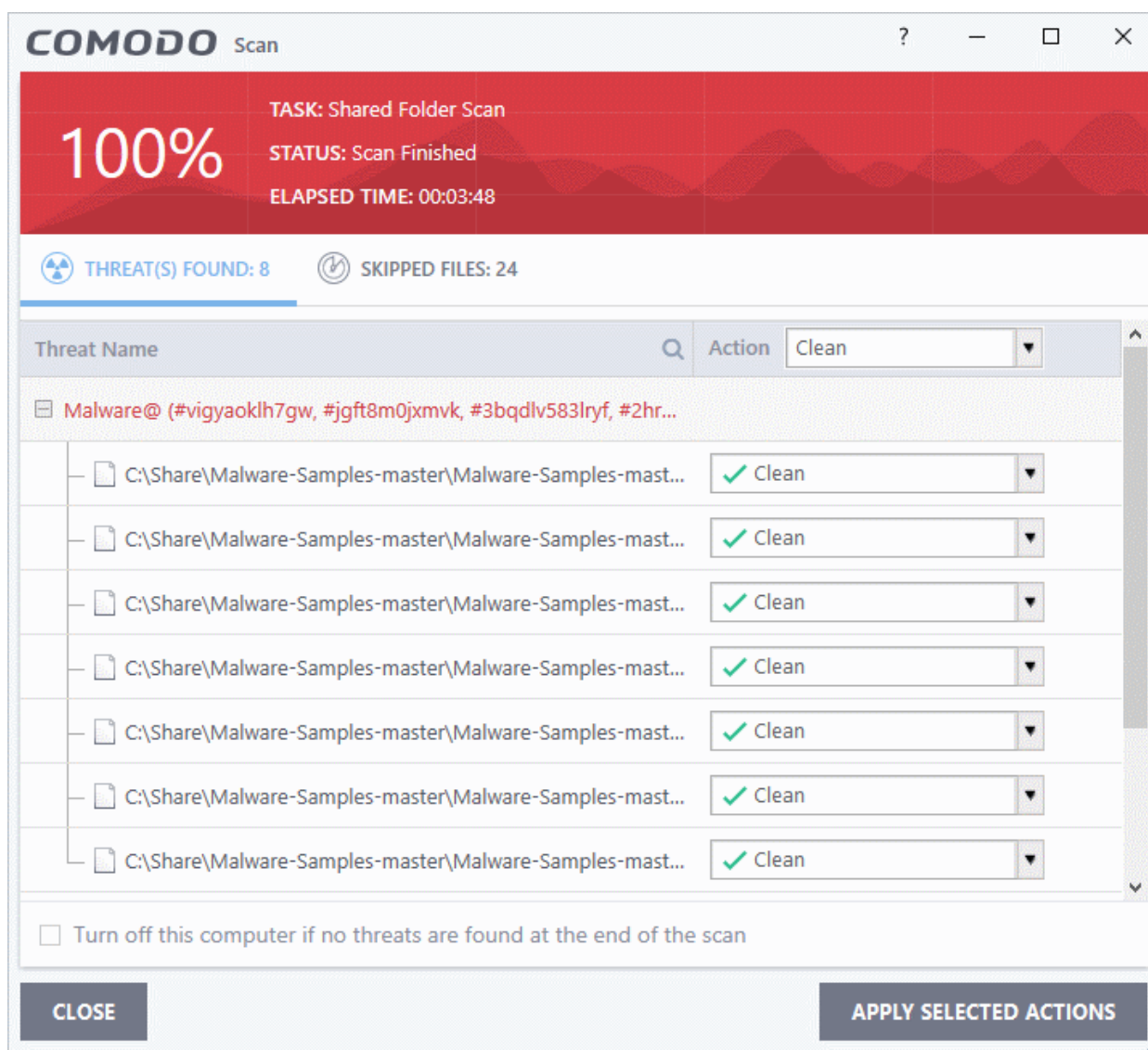
- Click 'Schedule' if you want the scan to be run automatically at set intervals (Optional)



- Click 'OK' to save your custom profile
- Click 'Scan' beside the profile name to launch your scan



- Results are shown at the end of the scan. The results show the number of items scanned, a list of all discovered threats, and the files that were skipped.



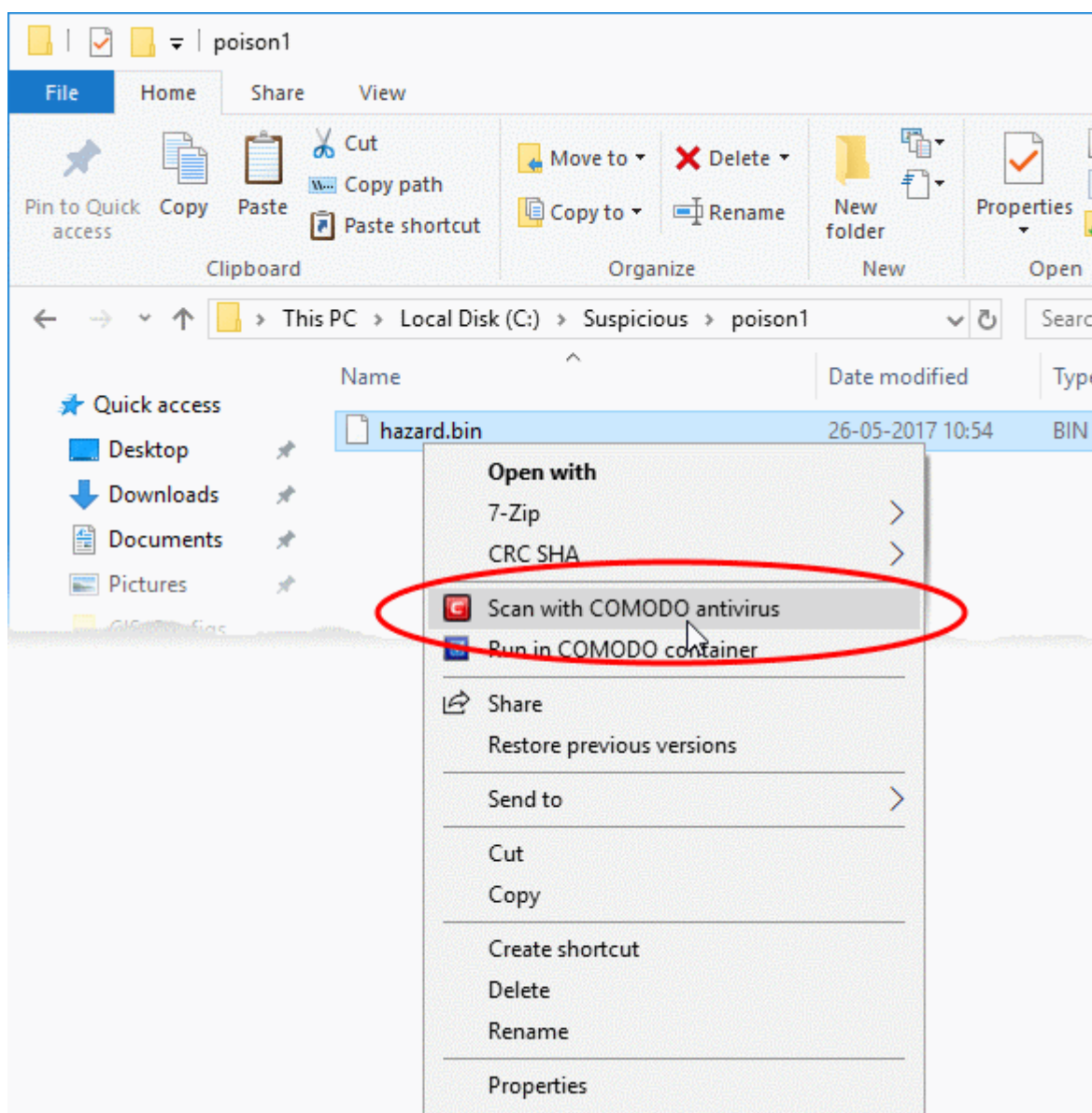
- You have the following options if threats are found:
 - Clean - Will delete the file
 - Quarantine - Moves the file into a secure, encrypted holding area. Quarantining a file renders it harmless
 - Ignore - Allow the file. You can choose to ignore one-time-only, or ignore and create an exclusion (permanently ignore)

Run an Instant Antivirus Scan on Selected Items

- You can scan individual files, folders or drives to instantly to check whether they contain threats.
- This is useful, for example, if you are unsure about a file you have downloaded from the internet.

Instantly scan an item

- Right-click on the item and select 'Scan with Comodo Antivirus' from the menu:

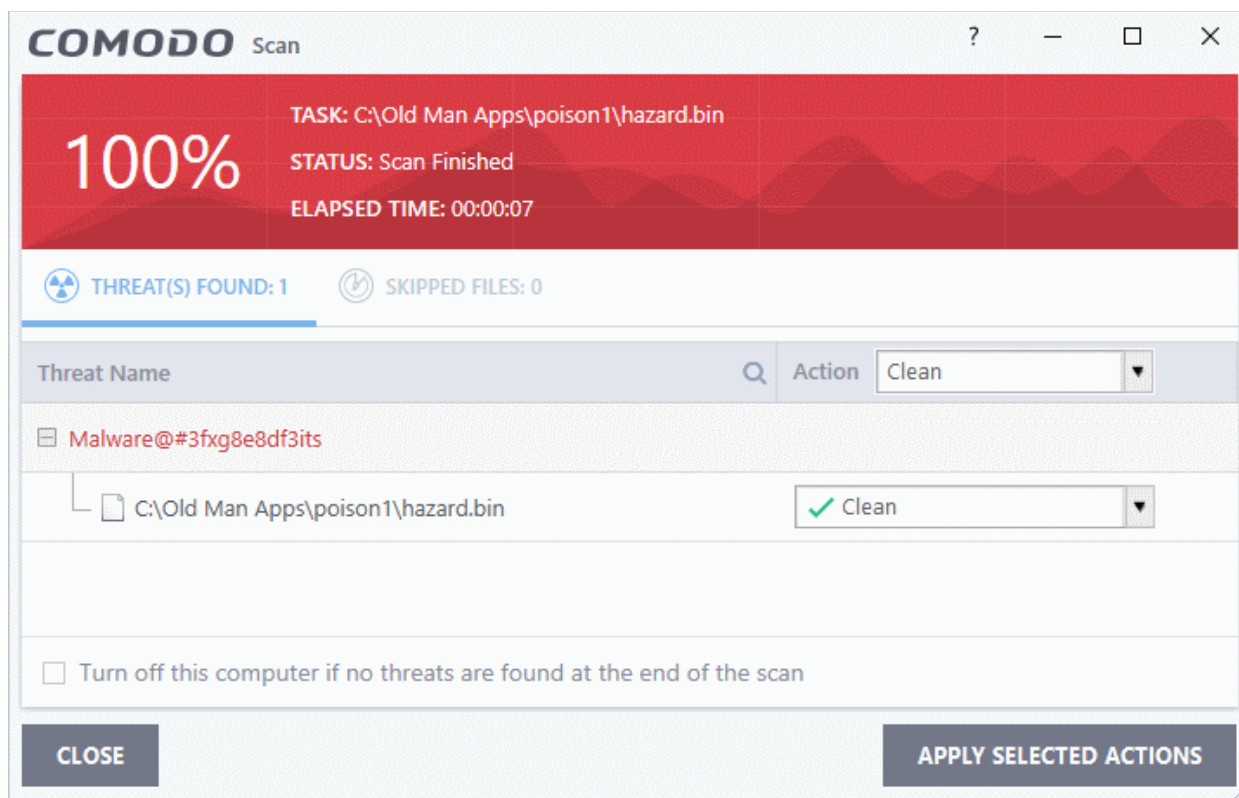


The item will be scanned immediately.

Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed.

These thresholds are set in the 'Full Scan' profile, which can be viewed in CCS at 'Settings' > 'Antivirus' > 'Scans'.

- Scan results are shown when the scan finishes:



- The results show the number of items scanned, a list of all discovered threats and the files that were skipped.
- You have the following options if threats are found:
 - Clean - Will delete the file
 - Quarantine - Moves the file into a secure, encrypted holding area. Quarantining a file renders it harmless
 - Ignore - Allow the file. You can choose to ignore one-time-only, ignore and create an exclusion (permanently ignore)

Set up the Firewall for Maximum Security and Usability

Note: The firewall is already configured to provide total security. This section is only for advanced users who wish to tweak the settings even further.

Stealth Ports Settings

Port stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, sending no response to opportunistic port scans.

- Click the 'Tasks' button on the CCS home screen
- Click 'Firewall Tasks' > 'Stealth Ports'
- Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

Network Zones Settings

'Network Zones' settings let you configure connections for a router/home network. Note - this is usually done automatically for you.

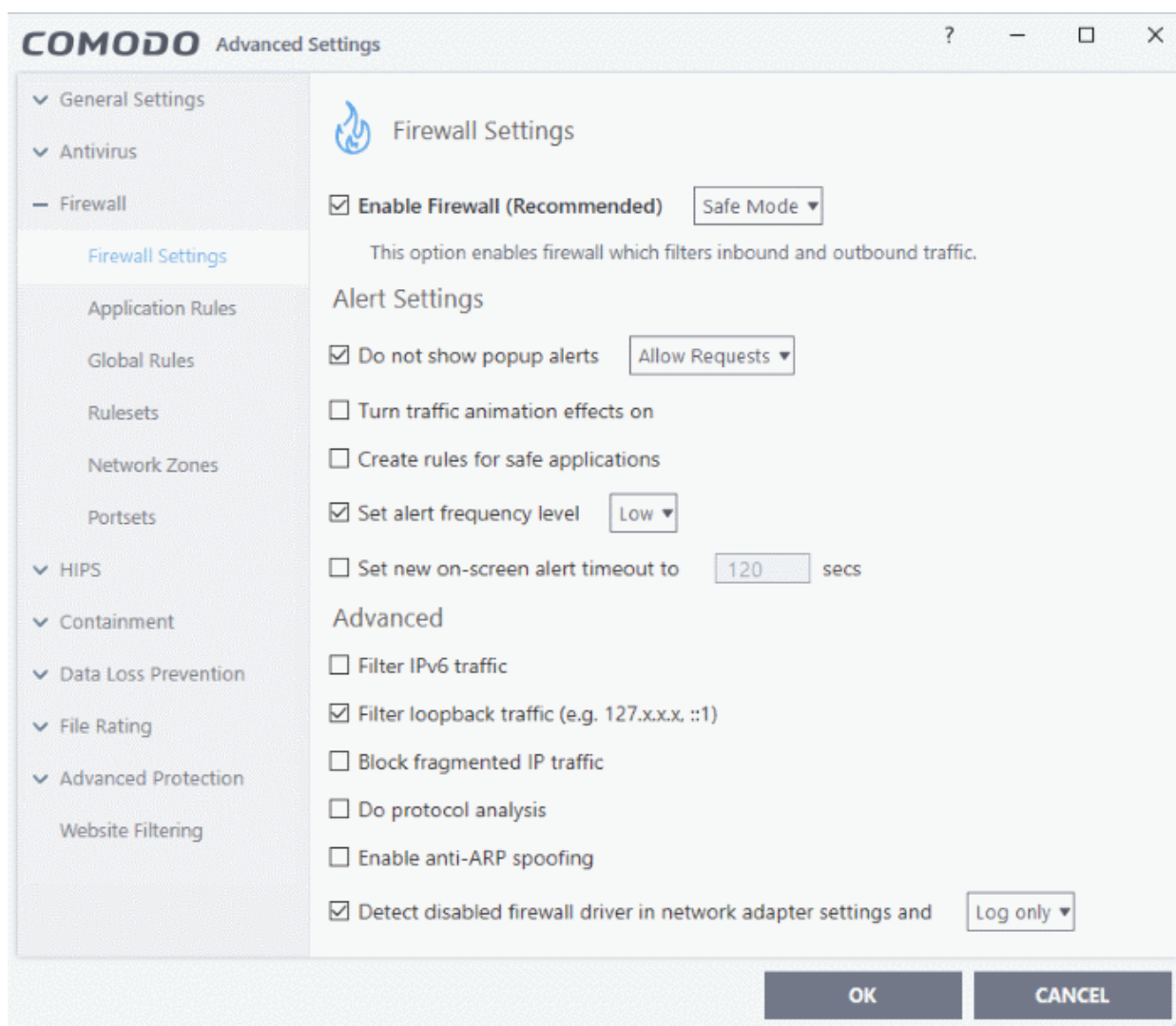
- Click 'Settings' on the top left to open the 'Advanced Settings' pane
- Click 'Firewall' > 'Network Zones'

- Click the 'Network Zones' tab from the 'Network Zones' interface
- Inspect the Loopback zone and Local Area Network #1 by clicking the '+' button beside the zone name.
 - In most cases, the loopback zone IP address should be 127.0.0.1/255.0.0.0
 - In most cases, the IP address of the auto detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0
- Click 'OK'.

Firewall Settings

Firewall settings let you configure the protection level for your internet connection and the frequency of alerts.

- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Firewall Settings'



- **Enable Firewall** - Leave this option enabled to activate firewall and choose 'Safe mode' from the drop-down beside it.

Safe Mode: The firewall will automatically create rules that allow all traffic for applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

- **Do not show popup alerts** - Deselect the option to get notified when the firewall encounters a request for network access.
- **Set alert frequency level** - Enable and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.

Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- **Filter loopback traffic:**

Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to by its domain name of 'http://localhost'. This is the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer.

- Leave this option enabled for the firewall to filter traffic sent through this channel.

- **Block fragmented traffic:**

When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using. When a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, fragmentation can double the amount of time it takes to send a single packet and slow down your download time.

- Enable this option for the firewall to bar fragmented IP traffic

- **Do Protocol Analysis:**

Protocol Analysis is key to the detection of fake packets used in denial of service attacks.

- Enable this option for the firewall to check that every packet conforms to that protocols standards. If not, then the packets are blocked.

- Click 'OK' for your settings to take effect.

Set-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules on an application-specific and a global basis. You can also create and deploy predefined firewall rule-sets.

Application Rules

- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Application Rules'
- Use this interface to add, edit, enable/disable or remove internet connection rules for specific applications.
- See <https://help.comodo.com/topic-463-1-1033-15925-Application-Rules.html> for more help on this.

Global Rules

- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Global Rules'
- Use this interface to add, edit, enable/disable or remove global rules which apply to all traffic.
- See <https://help.comodo.com/topic-463-1-1033-15926-Global-Rules.html> for more help on this.

Predefined Firewall rulesets

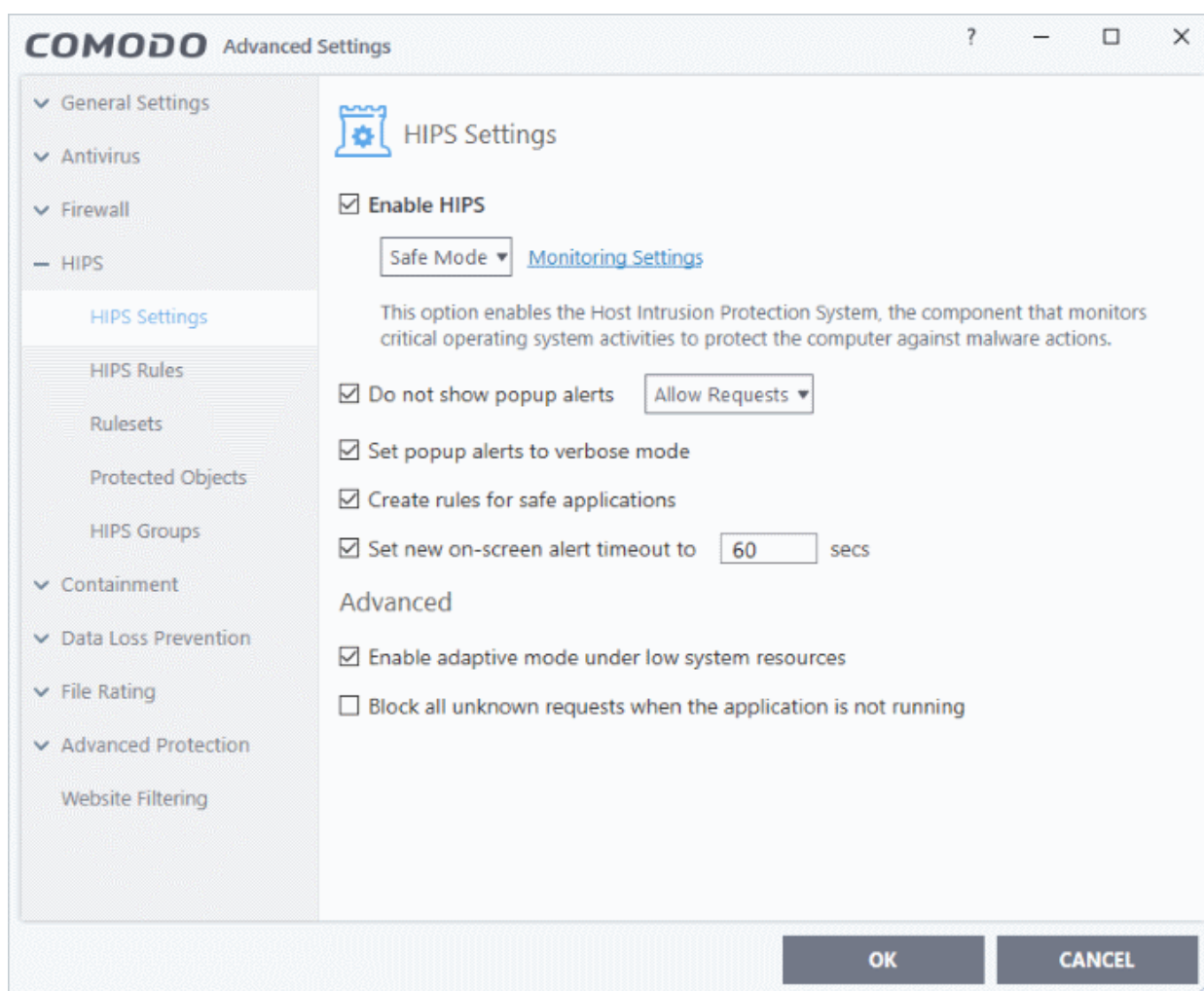
- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Rulesets'
- Use this interface to add, edit, enable/disable or remove firewall rulesets
- See <https://help.comodo.com/topic-463-1-1033-15927-Firewall-Rule-Sets.html> for more help on this.

Set up HIPS for Maximum Security and Usability

HIPS stands for 'Host Intrusion Prevention System'. The system prevents malicious programs from executing on your computer, protecting you from data theft, computer crashes and system damage. HIPS also blocks buffer overflow attacks, inter-process memory injections, key-loggers and more.

Configure HIPS

- Click 'Settings' at the top of the CCS home screen
- Click 'HIPS' > 'HIPS Settings'



- **Enable HIPS** - Select this option and choose 'Safe Mode' from the drop-down.
- **Monitoring Settings** - Click 'Monitoring Settings' and make sure that all the check boxes are selected and click 'OK'

Advanced

- Make the following settings under 'Advanced' in the 'HIPS Settings' interface
 - **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems. (*Optional*)
 - **Enable 'Block all unknown requests if the application is not running'** - Prohibits execution of unknown applications if CCS is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked. (*Optional*)

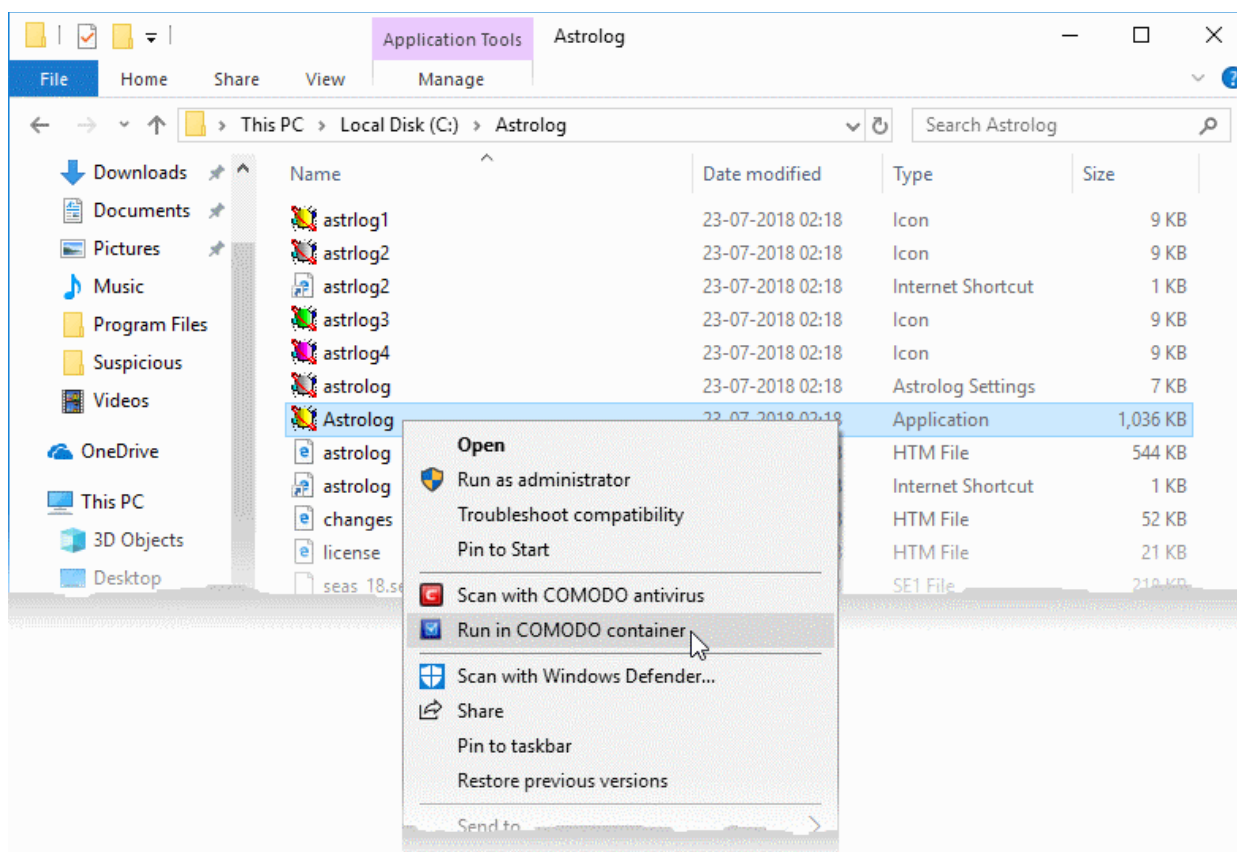
Run Programs in the Container

- The container is a secure, virtual environment in which you can run unknown, untrusted, and suspicious applications.
- Applications in the container are isolated from the rest of your computer. They are denied access to other processes, write to a virtual file system and registry, and cannot access your personal data.
- The container is useful for testing new programs and for programs you are not sure about.
- You can run applications in the container on an ad-hoc basis, and you can also create desktop shortcuts to always launch a program in the container.

This section explains how you can run programs in the container on a one-off basis. There are a couple of ways to do this:

Run a program inside the container from the right-click options

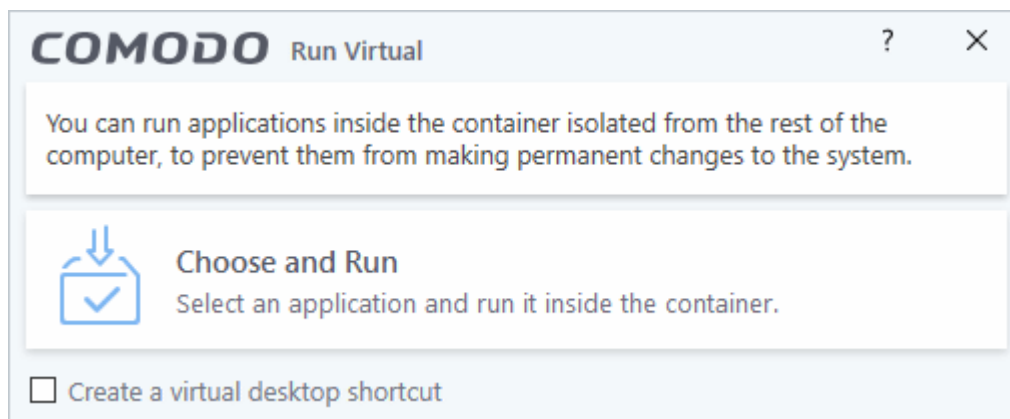
- Browse to the installation folder of the .exe file through Windows Explorer
- Right-click on the program that you want to run inside the container



- Choose 'Run in COMODO container' from the context sensitive menu

Run a program in the container from the 'Containment Tasks' interface

- Click the 'Tasks' on the CCS home screen
- Click 'Containment Tasks' > 'Run Virtual'

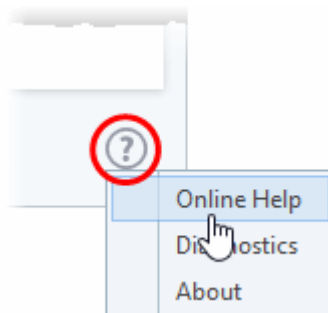


- Click 'Choose and Run' then browse to the application.
 - Select 'Create a virtual desktop shortcut' if you want to run the application in the container in future.
- The contained application will run with a green border around it.

More Help

Online Help

- Click the '?' icon at the bottom-right of the interface and choose 'Online Help' from the options.



- This will open the CCS user guide at <http://help.comodo.com>.

You can also print or download the guide as a pdf by clicking the print / pdf icons at top-right.

Support Forums

- You can access the Dragon / Comodo One community pages at <https://c1forum.comodo.com>, a forum for our users to discuss anything related to our products.
- Please register for a free account to post questions and join discussions.

Online Knowledge Base

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

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com