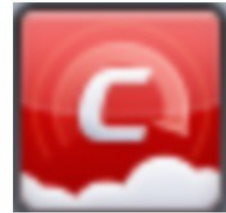


COMODO
Creating Trust Online®



Comodo Cloud Antivirus

Software Version 1.20

Quick Start Guide

Guide Version 1.20.120418

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

Comodo Cloud Antivirus – Quick Start Guide

This tutorial explains how to use Comodo Cloud Antivirus (CCAV). Please use the following links to go straight to the section that you need help with:

- [Installation](#)
- [The Main Interface](#)
- [Scan and Clean your Computer](#)
- [Run an Instant Antivirus Scan on Selected Items](#)
- [Configure Sandbox Settings for Maximum Security and Usability](#)
- [Configure File Rating Settings for Maximum Security and Usability](#)
- [Submit Unknown Files for Analysis](#)
- [Browse the Internet and run Untrusted Programs inside the Sandbox](#)

Installation

- If you haven't done so already, please download the CCAV setup file from <https://antivirus.comodo.com/cloud-antivirus.php>
- Before beginning installation, please ensure you have uninstalled any other antivirus products. This includes other Comodo antivirus products like CIS, CAV or CES.

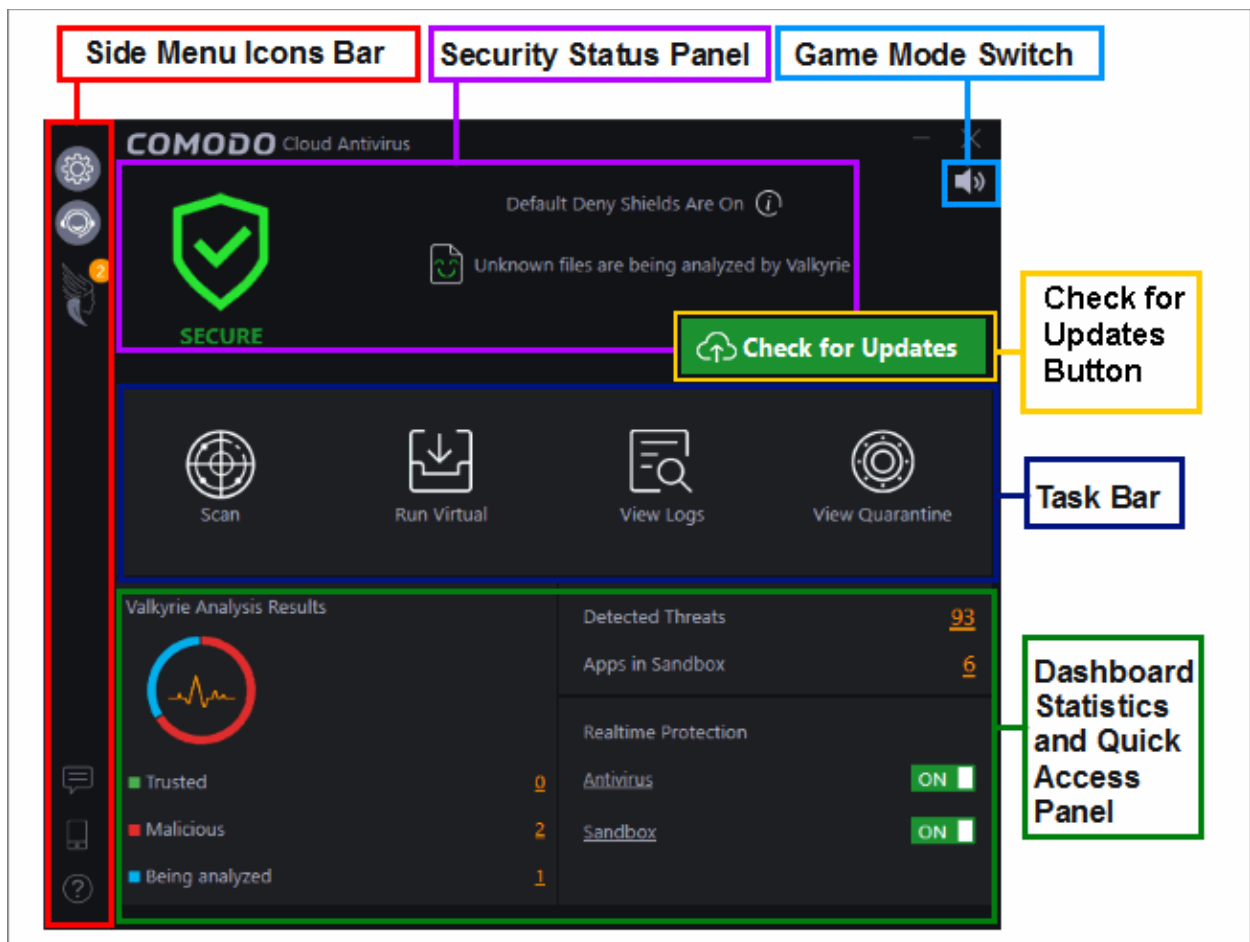
To install:

- Double-click the CCAV setup file to start the installation wizard.
- Use the drop-down menu to select the language that you want to see in the CCAV interface
- After finishing the wizard, CCAV will automatically launch a quick scan of important areas. Areas scanned include system memory, auto-run entries, start-up items, hidden services, boot sectors and other critical areas.
- Click 'Close' after the scan is completed.
- You will be prompted to restart your computer after the scan. The application will only work to its full potential after the restart.

A more detailed description of the options available during installation can be found in the installation guide at <https://help.comodo.com/topic-394-1-767-9216-Installation.html>

The Main Interface

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



- Overall security status is shown in the upper pane, 'Security Status Panel'. If problems are found, this box will show a large red 'X' and a 'Fix It!' button which allows you to remediate the issue.
- The side-menu lets you open the settings area, chat with support, and manage Valkyrie.
- The middle pane lets you run a virus scan, run an application in the sandbox, view logs, and view quarantined items.
- You can enable / disable realtime protection in the lower-right pane, and view Valkyrie results on the left.

See <https://help.comodo.com/topic-394-1-767-9218-The-Main-Interface.html> if you need more help with the home screen.

Scan and Clean your Computer

CCAV allows you to run on-demand virus scans at any time. An alert is shown if any threats are found.

Click the following links to read more about each type of scan:

- [Run a Quick Scan](#)
- [Run a Full Scan](#)
- [Run a Certificate Scan](#)
- [Run a Folder Scan](#)
- [Run a File scan](#)

Run a Quick Scan

- A 'Quick Scan' is a focused scan of very important areas of your computer. These areas are the ones most often targeted by malware and so are more prone to infection.
- Areas scanned include system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files.
- These areas are of great importance to the health of your computer so it is essential to keep them free of infection.

To run a Quick Scan

- Click 'Scan' on the home screen, or click the 'Start a scan' button on the widget
- Click 'Quick Scan' to start the scan
- To pause, continue or stop the scan, click the appropriate button at the bottom of the interface
- Scan results are shown at the end of the scan. Results include the number of objects scanned and any identified threats.
- The drop-down menu on the right contains actions you can take on detected threats. You have the following options:
 - Clean – delete the threat
 - Move to quarantine
 - Ignore the threat
 - Add to trusted applications
 - Submit as false positive
 - Add to exclusions

Run a Full Scan

A full scan covers every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras are also scanned.

To run a Full Computer Scan

- Click 'Scan' on the home screen, or click the 'Start a scan' button on the widget
- Click 'Full Scan' to start the scan
- To pause, continue or stop the scan, click the appropriate button at the bottom of the interface
- Scan results are shown at the end of the scan. Results include the number of objects scanned and any identified threats.
- The drop-down menu on the right contains actions you can take on detected threats. You have the following options:
 - Clean – delete the threat
 - Move to quarantine
 - Ignore the threat
 - Add to trusted applications
 - Submit as false positive
 - Add to exclusions

Run a Certificate Scan

- A root certificate scan checks that all roots on your computer were issued by a trusted certificate authority.
 - Website certificates are used for security on websites. They provide the lock symbol you see on the right of your browser address bar.
 - Root certificates are stored on your computer. They are used to verify the website certificates just mentioned are legitimate and should be trusted.
- A fraudulent root certificate can trick you into thinking a fake/phishing/malware website is trustworthy.

To run a Certificate scan

- Click 'Scan' on the home screen, or click the 'Start a scan' button on the widget
- Click 'Certificate Scan'
- To pause, continue or stop the scan, click the appropriate button at the bottom of the interface
- Scan results are shown at the end of the scan. Results show the number of certs scanned and any untrusted roots.
- Use the drop-down menu on the right to choose whether to ignore untrusted certificate or delete the certificate.

Run a Folder Scan

The 'Folder Scan' option allows you to scan a specific folder on your hard drive, CD/DVD or external device.

- Click 'Scan' on the home screen, or click the 'Start a scan' button on the widget
- Click 'Folder Scan'
- Browse to the folder you want to scan and click 'OK'
 - Alternatively, right-click on a folder and select 'Scan with Comodo Cloud Antivirus'.
- To pause, continue or stop the scan, click the appropriate button at the bottom of the interface
- Scan results are shown at the end of the scan. Results include the number of objects scanned and any identified threats.
- The drop-down menu on the right contains actions you can take on detected threats. You have the following options:
 - Clean – delete the threat
 - Move to quarantine
 - Ignore the threat
 - Add to trusted applications
 - Submit as false positive
 - Add to exclusions

Run a File Scan

The 'File Scan' option allows you to scan a specific file on your hard drive, CD/DVD or external device.

- Click 'Scan' on the home screen, or click the 'Start a scan' button on the widget
- Click 'File Scan'
- Browse to the file that you want to scan and click 'OK'

- Alternatively, right-click on a file and select 'Scan with Comodo Cloud Antivirus' from the context-sensitive menu.
- To pause, continue or stop the scan, click the appropriate button at the bottom of the interface
- Scan results are shown at the end of the scan. Results include the number of objects scanned and any identified threats.
- The drop-down menu on the right contains actions you can take on detected threats. You have the following options:
 - Clean – delete the threat
 - Move to quarantine
 - Ignore the threat
 - Add to trusted applications
 - Submit as false positive
 - Add to exclusions

Run an Instant Antivirus Scan on Selected Items

- Right-click on any file, folder or drive
- Select 'Scan with Comodo Cloud Antivirus' from the right-click menu
- CAV will scan the selected item
- Results are shown at the end of the scan. Results include the number of objects scanned and any identified threats.
- The drop-down menu on the right contains actions you can take on detected threats. You have the following options:
 - Clean – delete the threat
 - Move to quarantine
 - Ignore the threat
 - Add to trusted applications
 - Submit as false positive
 - Add to exclusions.

Configure Sandbox Settings for Maximum Security and Usability

The sandbox settings area allows you to configure your overall sandbox policy.

To open sandbox settings

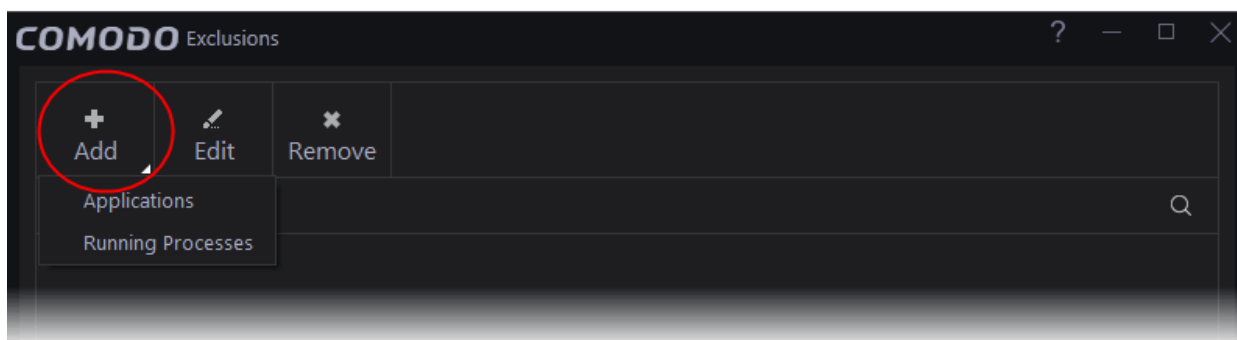
- Click the 'Settings' icon on the left then 'Sandbox' > 'Sandbox Settings'
OR
- Click the 'Sandbox' link under 'Realtime Protection' on the home screen
OR
- Right-click on the CCAV system tray icon (or the widget) and choose 'Sandbox Settings' from the options.

Sandbox Settings

- **Enable Auto-Sandbox** - Switch automatic sandboxing on or off. Default = On.
 - If you disable the sandbox then any sandbox rules you have created will be disregarded.
 - If you enable the sandbox, you have the following options:
 - **Sandbox all untrusted applications** - CCAV will automatically run 'unknown' files and applications in the sandbox. A file can have one of three trust statuses - 'Trusted', 'Untrusted' or 'Unknown'. 'Trusted' files are those that are either on the Comodo white-list of known-good applications or have been manually trusted by the user. Trusted files are allowed to run outside the sandbox. 'Untrusted' files are malware and will be quarantined by the antivirus scanner. 'Unknown' files are those which are neither 'Trusted' nor 'Untrusted'. As their precise intentions are not yet known, we run these applications in a secure virtual environment known as the 'sandbox'. If they later transpire to be malicious, they will not have been able to cause damage to your computer or data because they were isolated.
 - **Run only safe applications** - Only applications from trusted vendors or those in your list of trusted applications will be allowed to run. All other applications will be blocked.
 - **Ask for untrusted files** - Instead of automatically sandboxing unknown files, CCAV will show you an alert and offer you the choice of sandboxing the application or running it normally.
- **Save file with trusted rating outside sandbox automatically** – If enabled, files saved in the sandbox which are subsequently found to be safe will be moved to your local hard drive. Default= Disabled.
- **Enable Sandbox indicator** - CCAV will display a green border around an application if it is running in the sandbox. Disable this setting if you do not want to see this border.
- **Do not virtualize access to the specified folders** – By default, sandboxed applications can access folders and files on your computer but cannot save any changes to them. You can define exceptions to this rule by using the 'Do not virtualize access to...' links.
- **Enable Viruscope** - Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Viruscope alerts give you the opportunity to quarantine the process & reverse its changes or to let the process continue. Viruscope forms another layer of security on top of the core antivirus protection and helps CCAV to control and evaluate the behavior of sandboxed applications.
 - **Do NOT show Viruscope pop-up alerts** - Configure whether or not CCAV should show an alert if Viruscope detects suspicious activity. Choosing 'Do not show' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.
 - **Monitor only the applications running in the Sandbox** - Choose whether Viruscope should monitor the activities of all running processes, or only processes which are sandboxed.
- **I want to enable 'Cloud based Behavioral Analysis of unrecognized programs by submitting them to Comodo automatically in compliance with Comodo Privacy Policy'** - Any file that is identified as unknown is sent to the Cloud server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. If you disable this setting, an alert to submit unknown files will be displayed.
- **Copy any shortcuts created by sandboxed applications to my desktop** - Will place a duplicate of any shortcuts created by sandboxed applications onto the desktop of your local machine. This allows you to open the application faster and also alerts you to the fact that the application created a shortcut. Clicking the local shortcut will run the application in the sandbox.
- **Allow sandboxed applications to access the clipboard** - If enabled, you will be able to copy and paste content between sandboxed applications and non-sandboxed applications. This option is disabled by default.
- **Net Traffic Control Over Sandbox Apps**
 - **Block incoming connections to sandboxed applications (so they can't act like a server or listen for connections)** - Will prevent sandboxed applications from accepting TCP internet connections from

external sources. This stops potentially malicious applications from receiving instructions from their control server.

- **Block outgoing connections from sandboxed applications (so they can't send data out of your system)** - Will prevent sandboxed applications from making TCP internet connections to external sources. This stops potentially malicious applications from broadcasting your confidential data without your knowledge.
- **Add these applications to Exclusions and allow them to connect to the internet by overriding the above settings** - Specify applications which are allowed internet connectivity, even if sandboxed.
 - To specify exceptions, select the option then click the 'Exclusions' link. Click 'Add' at top-left. Choose applications or running processes:



- **Applications** – Choose an installed programs that should be allowed to connect to the internet.
- **Running Processes** - Select an application from the list of currently running processes. The parent application of the chosen process will also be excluded.
- Click 'Apply' for your settings to take effect.

Configure File Rating Settings for Maximum Security and Usability

- A file rating determines how CCAV interacts with a file.
- 'Trusted' files are safe to run. 'Untrusted' files are malware so they get quarantined or deleted. 'Unknown' files are run in the sandbox until they are classified as trusted or untrusted.
- Especially in the case of 'unknown' files, the rating of a file can change over time. For example, an 'unknown' file might be re-classified as 'trusted' or 'untrusted' after it has been tested.
- 'File Ratings Settings' lets you configure how long a rating downloaded from our servers should be considered valid.
- You can also configure whether CCAV should check cloud vendor lists to obtain file ratings.

To open the 'File Rating Settings' interface

- Click the 'Settings' icon at the top left of the CCAV home screen
- Click 'File Rating' > 'File Rating Settings' on the left

File Rating Settings

- **Cloud file rating expires after NN days** - In order to determine its run-time privileges, CCAV consults a file's rating whenever you access the file. This rating is obtained from Comodo's cloud-based file ratings server and is then cached locally to speed-up subsequent executions. This settings allows you to specify the number of days for which a cached rating should be considered valid (**Default = 10**)

days). When this period has elapsed, CCAV obtains updated ratings from the cloud server.

- **Detect potentially unwanted applications** - When this check box is selected, CCAV also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. **(Default = Enabled)**
- **Do cloud lookup for trusted vendors** – CCAV checks the trusted vendor list in Comodo cloud during scans. If this option is disabled, the trusted verdicts returned during vendor cloud lookup will be ignored. **(Default = Enabled)**
- **Do cloud lookup for malicious vendors** - CCAV checks the malicious vendor list in Comodo cloud during scans. If this option is disabled, the malicious verdicts returned during vendor cloud lookup will be ignored. **(Default = Enabled)**
- **Do not update local list upon program updates** - CCAV downloads the latest trusted vendor list (TVL) when the program receives updates. If you disable this option then the TVL is not refreshed when you update the program. **(Default = Disabled)**
- Click 'Apply' for your settings to take effect.

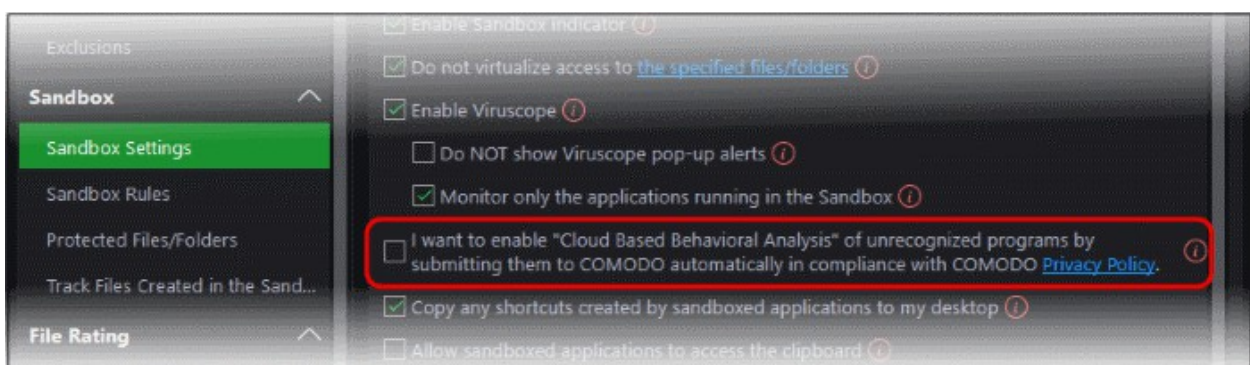
Submit Unknown Files for Analysis

CCAV awards a trust verdict of 'unknown' to a file after the following processes:

- Files are checked against the local and cloud trusted vendor lists. If the file was published by a trusted vendor then it is considered safe.
- CCAV consults Comodo's file lookup service (FLS) to see if the file is on the whitelist or blacklist.
- If no trust verdict is provided by the above processes, CCAV declares the file is 'unknown'.

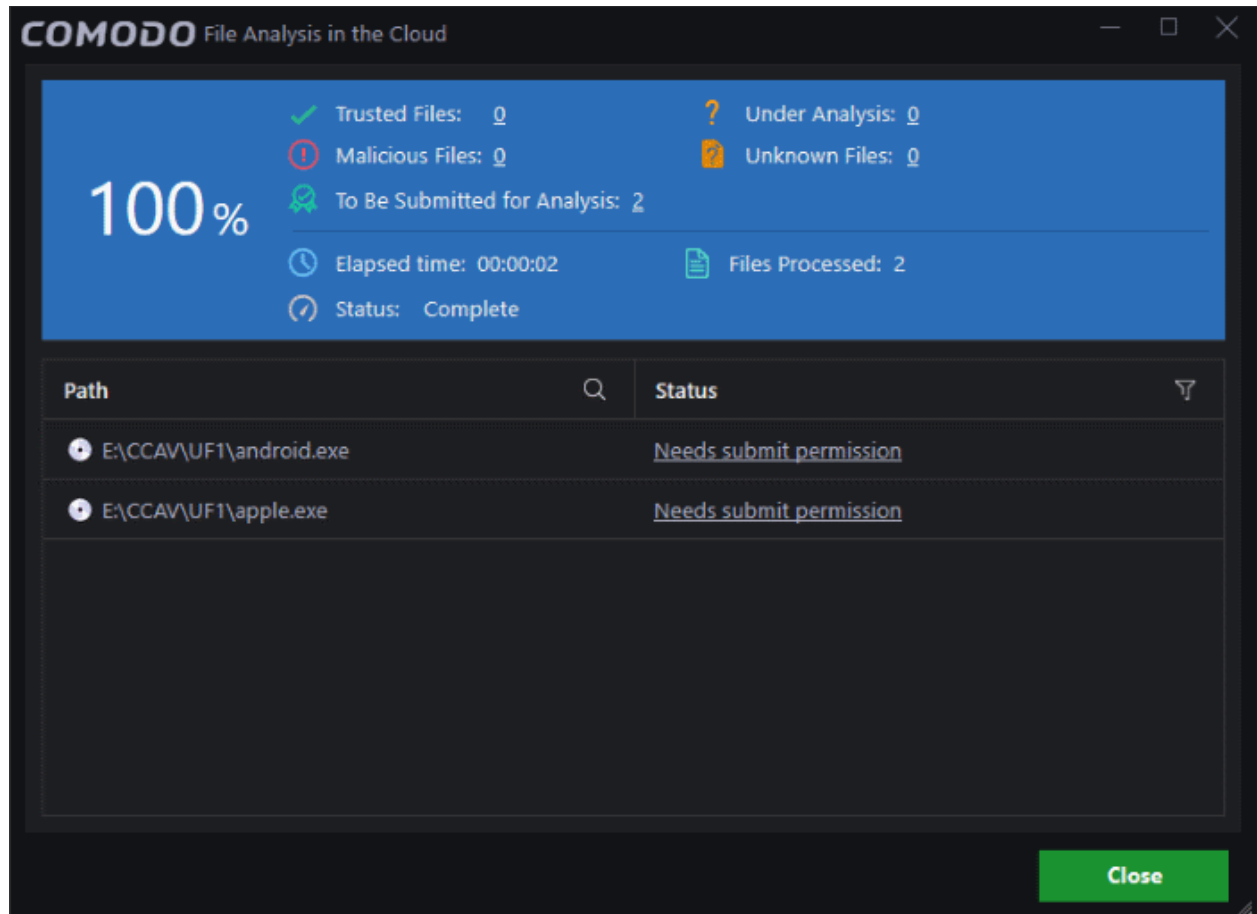
Unknown files are submitted to Comodo cloud for analysis. Depending on the settings, unknown files are submitted automatically or manually.

- To configure the unknown file submission settings, click the 'Settings' icon on the top-left then 'Sandbox' > 'Sandbox Settings'

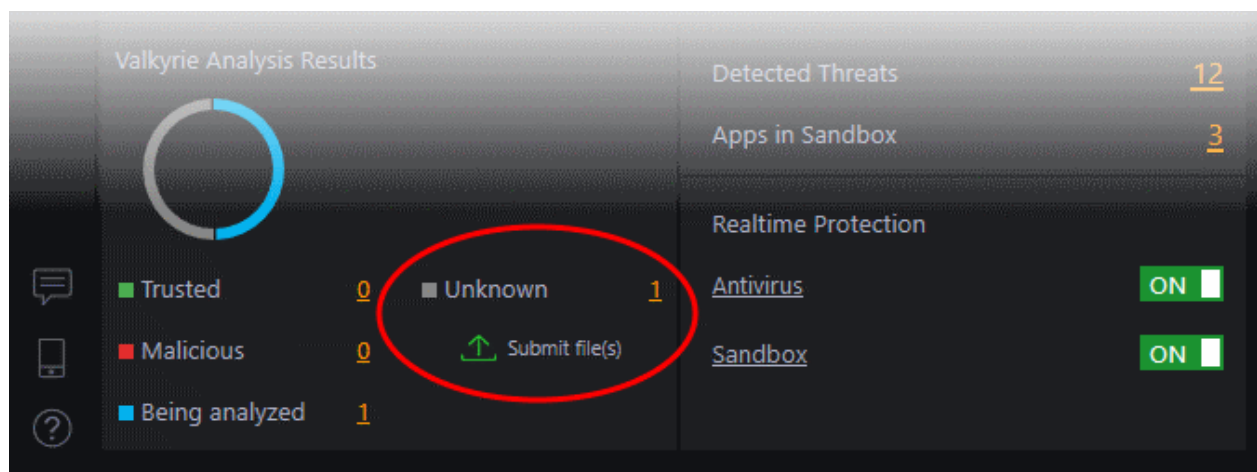


- Enable / disable the option 'I want to enable 'Cloud Based Behavioral Analysis' of unrecognized....' as shown above.
- If the above is enabled, unknown files will be automatically uploaded to cloud for analysis during the following actions:
 - Quick scan, full scan, certificate scan, folder scan and file scan (Click 'Scan' in the home screen and select the scan type)

- Right-click a folder and select 'Analyze Content of this Folder in the Cloud'
- When an unknown application is executed on your computer
- Right-click folder / file and select option of 'Scan with Comodo Cloud Antivirus',
- If the above is disabled, you have to submit unknown files manually to Comodo cloud for analysis during the following actions:
 - Right-click a folder and select 'Analyze Content of this Folder in the Cloud'



- Click 'Needs submit permission' to upload for analysis
- When an unknown application is executed on your computer



- Click 'Submit file(s)' in the home screen under 'Valkyrie Analysis Results' to upload for analysis

Note - For quick scan, full scan, folder scan, file scan, scheduled scan and scan with Comodo cloud antivirus from

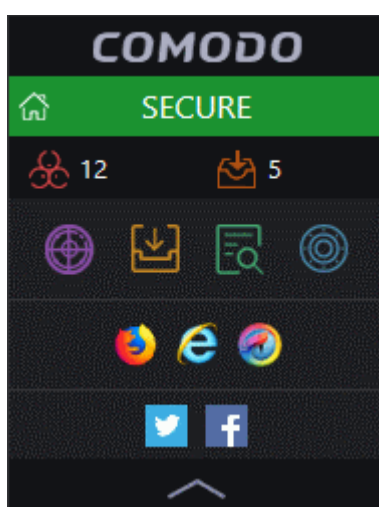
right-click context sensitive menu, there is no option to submit unknown files manually for analysis. So make sure that the option is enabled.


Browse the Internet and run Untrusted Programs inside the Sandbox

CCAV allows you to browse the internet and run untrusted programs inside a 100% virtual environment. Programs running inside this virtual environment are isolated from the rest of your computer and so cannot infect it. For example, if you inadvertently download malware from the internet while browsing in the virtual environment, then that malware will not be able to damage your computer or access your private data.

You can run an application / browser inside the sandbox by the following methods:

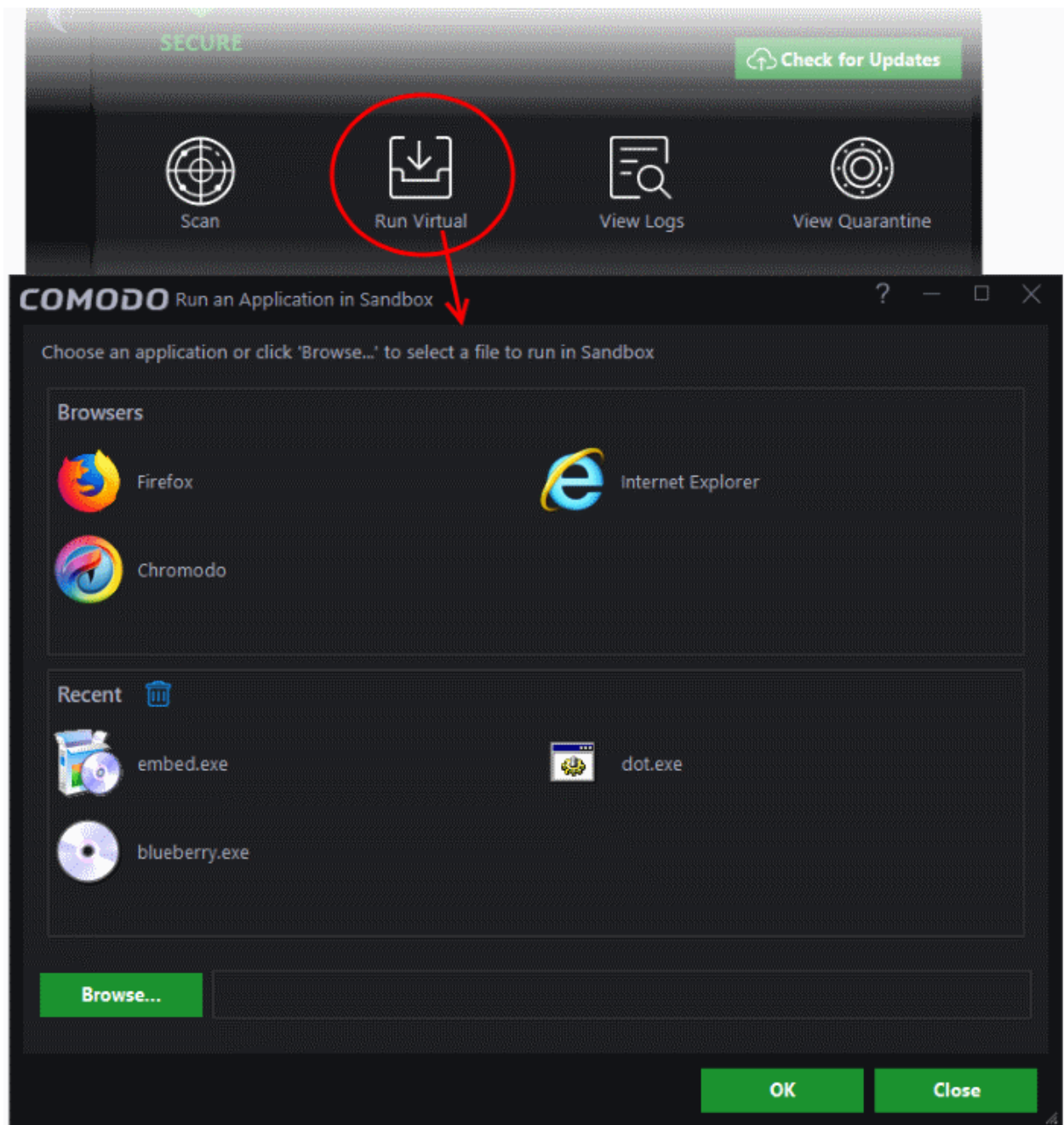
Widget



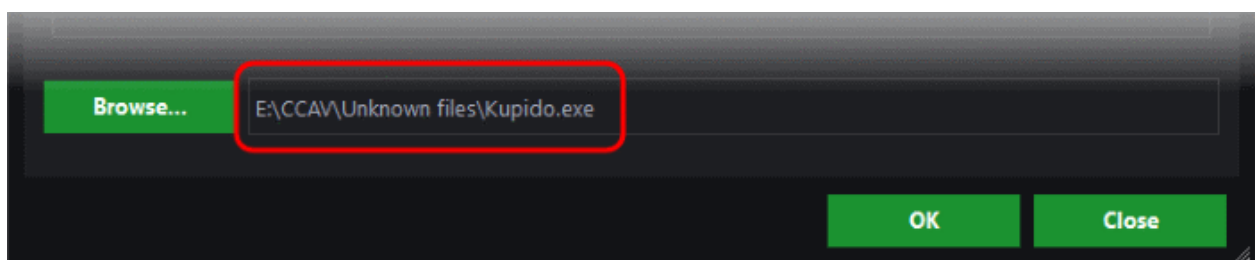
- Browsers in your system will be automatically be added to the widget. Click a browser icon in the widget in the third row to open it in the virtual environment.
- To run an application inside the sandbox, click the 'Run Virtual' icon  in the widget.
 - The 'Run an Application in Sandbox' dialog will open. You can open this dialog from the home screen also. See below.
 - Click 'Browse...', navigate, select the application and click 'Open'
 - Click 'OK'.

Home Screen

- Click 'Run Virtual' in the home screen
- The 'Run an Application in Sandbox' dialog will open.



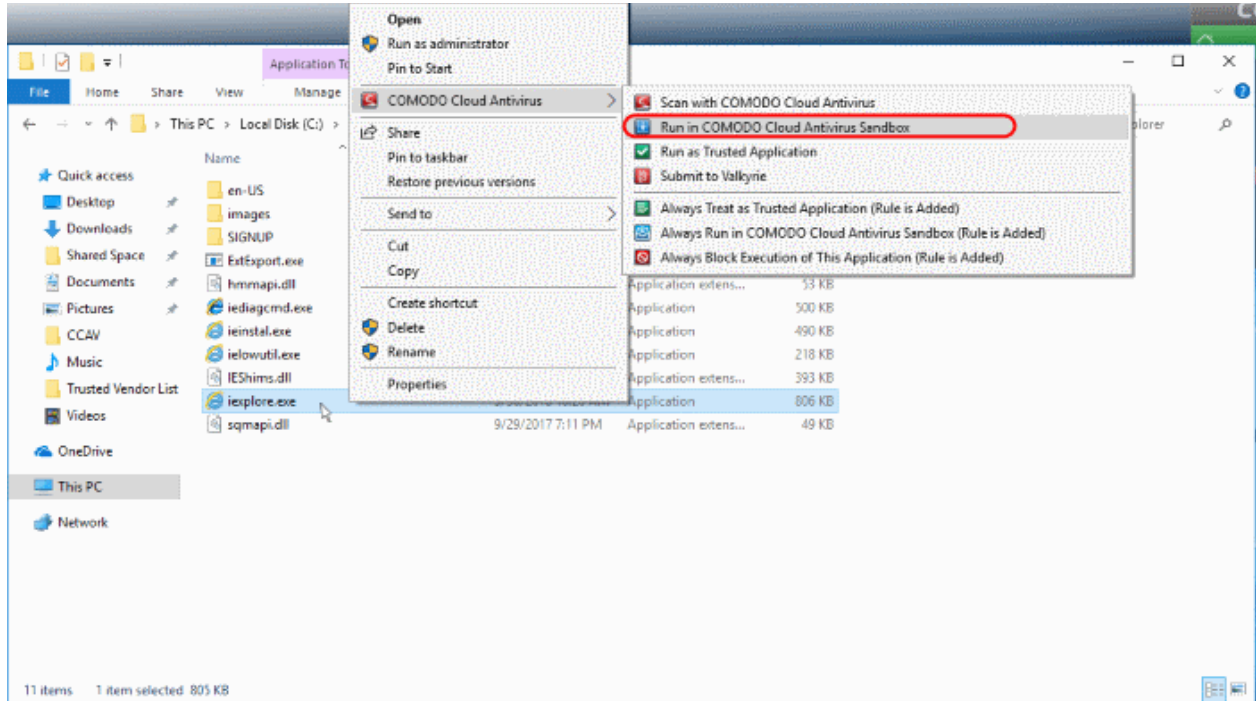
- Browsers in your system will be shown in the upper pane. Click on a browser to open it in the sandbox.
- To run an application inside the sandbox, click 'Browse...', navigate, select and click 'Open'
 - The full path of the file will be shown in the field beside 'Browse...'



- Click 'OK'
- The application will run inside the virtual environment. You can see recently run applications inside the sandbox in the lower pane. You can run it again by double-clicking it or select it and click 'OK'

Right-click option

- Navigate to the browser \ application in your system, right-click and select 'Run in Comodo Cloud Antivirus Sandbox' from the context-sensitive menu.



See the full guide at <https://help.comodo.com/topic-394-1-767-9214-Introduction-to-Comodo-Cloud-Antivirus.html> to know more.

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