

COMODO
Creating Trust Online®



Comodo Internet Security

Software Version 8.2

Quick Start User Guide

Guide Version 8.2.092818

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

Comodo Internet Security - Quick Start Guide

This tutorial explains how to use Comodo Internet Security (CIS). Please use the following links to go straight to the section that you need help with.

Installation

The main interface

Scanning and cleaning your computer

Run an instant antivirus scan on selected items

Setting up the Firewall for maximum security and usability

Setting up HIPS for maximum security and usability

Running untrusted programs in the sandbox

Browse the internet and run untrusted programs inside the Virtual Desktop

Renew or upgrade licenses

More Help

Installation

If you haven't done so already, please download the CIS setup file from <https://www.comodo.com/home/internet-security/security-software.php>

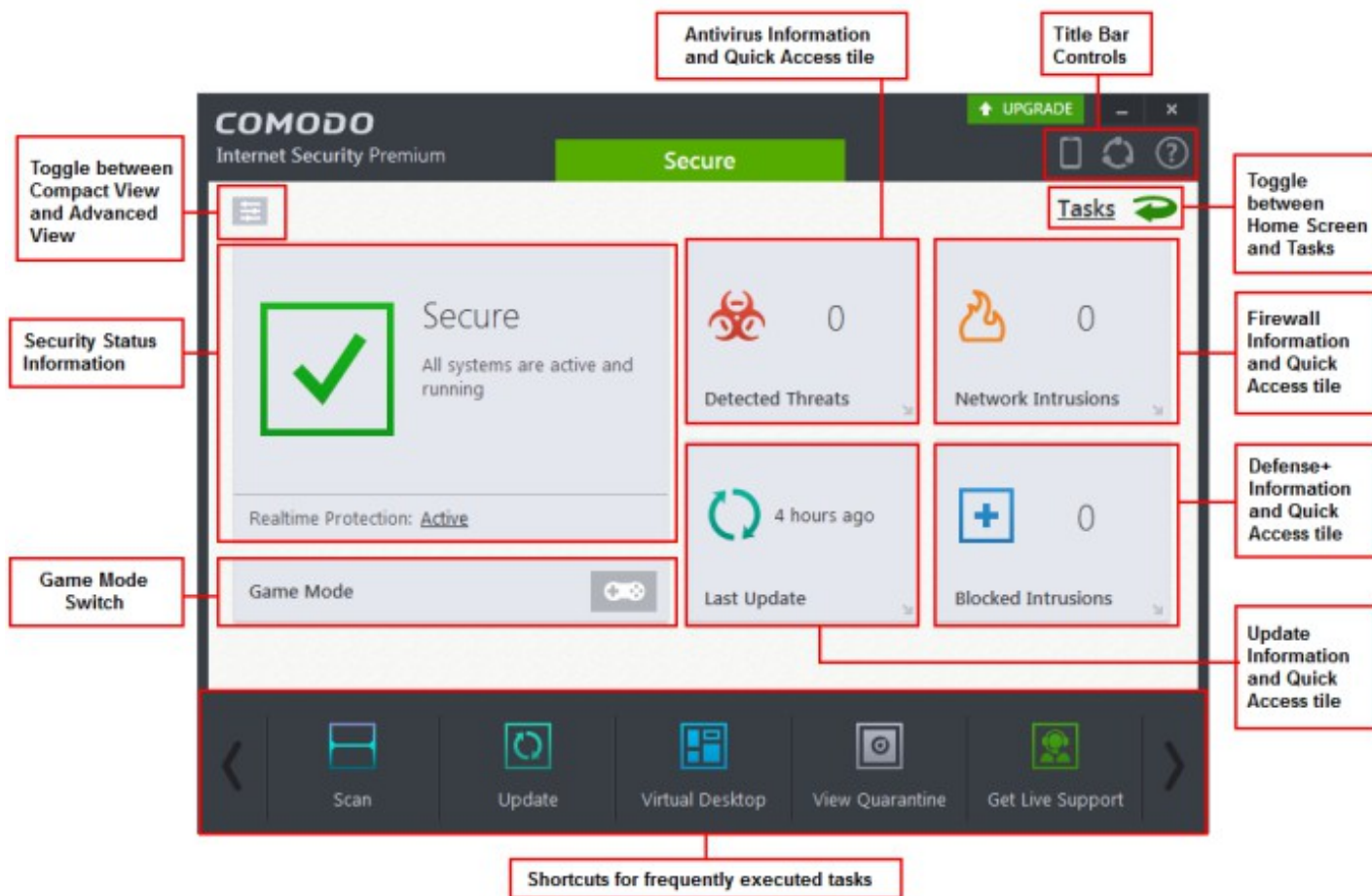
Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. More specifically, remove any other products of the *same type* as those Comodo products you plan to install.


- Double click the CIS setup file to start the installation wizard.
- Click 'Customize Installation' if you wish to configure advanced options.
- After finishing the wizard, you need to reboot your computer to complete installation.
- After rebooting you will be asked to choose your type of internet connection
- On first load, the CIS interface will display a security status of 'At Risk', meaning you need to run your first antivirus scan.
- Click 'Fix It' to run the scan. The virus database will be updated automatically prior to the scan.
- After the scan has completed, click 'Fix It' again to deal with any discovered threats.

A more detailed description of the options available during installation can be found in the main user guide at <https://help.comodo.com/topic-72-1-623-7676-CIS-Premium---Installation.html>

The Main Interface

The CIS interface is designed to be as clean and informative as possible and lets you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.



- Overall security status is shown in the large box on the left. If problems are found, this box will show a large red 'X' and a 'Fix It' button which will allow you to remediate the issue
- The four smaller boxes on the right of the home screen show frequently executed Tasks
- Click the curved green arrow at the upper right to switch between the home screen and the tasks interface
- Click 'Scan' at bottom left to run an antivirus scan
- Scan individual files or folders by right-clicking on them and selecting 'Scan with Comodo Antivirus'
- Switch on 'Game Mode' to make sure nothing interrupts you while you play a full screen game.
- To add or remove tasks in this area, open the 'Tasks' interface, right-click on any task and select 'Add to Task Bar'.
- The 'Upgrade' button allows Premium users to upgrade to CIS Pro or Complete.
- Flip between 'Compact View' and 'Advanced View' by using the toggle button at the  upper left. Advanced view shows antivirus, firewall and sandbox activity in greater detail.
- Advanced view shows antivirus, sandbox and firewall activity in greater detail. This includes the number of detected threats, last virus database update time, number of inbound and outbound connections and more. This view also allows you to quickly change security settings for each component.

Scanning and Cleaning your Computer

Comodo Internet Security allows you to run on-demand virus scans at any time. If any threats are found then an alert screen will be displayed along with cleaning options.

- **Run a Quick Scan**

- **Run a Full Computer Scan**
- **Run a Rating Scan**
- **Run a Custom Scan**

Run a Quick Scan

The 'Quick Scan' profile enables you to quickly scan those critical areas of your computer which are most often targeted by viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files.

To run a Quick Scan

- If the 'Tasks' interface is not open already, click the 'Tasks' button at top-left to open it
- Click 'General Tasks' then select 'Scan' then 'Quick Scan'
- The scanner will start and first check whether your virus signature database is up-to-date
- To pause, resume or stop the scanning, click the appropriate button at the bottom in the interface
- If you want to run the scan in the background, click 'Send to Background'
- An alert screen will be displayed at the end of the scan if issues were detected. It displays the number of threats/infections discovered and present you with cleaning options
- If you click 'Yes, I want an expert to clean it', you will be connected to a GeekBuddy technician who will offer to expertly clean your system
- If you wish to clean the infections yourself, select 'No, I will clean it myself'

Run a Full Computer Scan

A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

To run a Full Computer Scan

- If the 'Tasks' interface is not open already, click the 'Tasks' button at top-left to open it
- Click 'General Tasks' then select 'Scan' then 'Full Scan'
- The scanner will start and first check whether your virus signature database is up-to-date
- 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'
- Any detected threats will be displayed in full at the end of the scan. The alert will tell you how many threats were found; the name and location of the threats and will provide you with virus removal options
- If you click 'Yes, I want an expert to clean it', you will be connected to a GeekBuddy technician who will offer to expertly clean your system.
- If you wish to clean the infections yourself, select 'No, I will clean it myself'

Run a Rating Scan

The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed. By default, unknown files will be automatically run in the CIS sandbox

- **Bad** - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files

To run a Rating scan

- If the 'Tasks' interface is not open already, click the 'Tasks' button at top-left to open it
- Click 'General Tasks' then select 'Scan' then 'Rating Scan'

You can filter the results by rating using the 'Show' drop-down:

- **File Name:** The file which was scanned
- **Rating:** The rating of the file as per the cloud based analysis
- **Age:** The period of time that the file has been stored on your computer
- **Auto-run:** Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately
- **Action:** Displays a drop-down with actions to be executed on Unrecognized and Malicious files identified

Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis
- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing to neither 'Clean' nor 'Trust', this file will be detected by the next ratings scan that you run
- **Trusted** - The file assigned Trusted status in the 'File List' and will be given 'Trusted' rating from the next scan

For the same action to be applied to all 'Bad' files, make a selection from the drop-down menu at the top of the 'Action' column.

- Click 'Apply Selected Actions' to implement your choice
- Click 'Close' to exit

Run a Custom Scan

Comodo Antivirus allows you to create custom scan profiles to scan specific areas, drives, folders or files in your computer.

To run a custom scan

- If the 'Tasks' interface is not open already, click the 'Tasks' button at top-left to open it
- Click 'General Tasks' then select 'Scan' then 'Custom Scan'

The 'Custom Scan' panel will open and contains the following scan options:

Scan a folder – Scan the contents of a folders and sub-folders. Chose the target folder in the 'Browse for Folder' window and click 'OK'.

Scan a file - Scan a specific file stored on your hard drives or external devices. Click 'File Scan' from the 'Custom Scan' pane to chose your target file.

More Scan options - Create a custom scan profile which allows you to schedule exactly which files and folders are scanned, when they are scanned and how they are scanned.

To create a custom scan profile

- In 'General Tasks', click 'Scan' > 'Custom Scan' > 'More Scan Options'
- In the 'Advanced Settings' interface, the 'Scans' pane opens with a list of pre-defined and user created scan profiles
- Click 'Add' from the options at the top create a new custom scan profile

- Type a name for the profile in the 'Scan Name' text box
- The buttons at the top allow you to add the items to be scanned in three ways:
 - **Add File** - Allows you to add individual files to the profile.
 - **Add Folder** - Allows you to select entire folders to be included in the profile
 - **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory')
- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice.
- Click 'Options' to further customize the scan
- To run your custom scan, simply click 'Scan' beside the profile name

Run an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders, files and removable storage

To instantly scan an item

- Right click on a file, folder or drive and select 'Scan with COMODO Antivirus' from the context sensitive menu
- OR
- Click the 'Advanced View' button (top-right)
 - Drag and drop the item you wish to scan into the 'Drop Files to Scan' box

Setting up the Firewall For Maximum Security and Usability

Note – the firewall is configured by default to provide total security. This section is for advanced users who wish to tweak 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.

1. Open 'Firewall Tasks' from the Tasks interface
2. Open 'Stealth Ports' interface by clicking the 'Stealth Ports' icon from the 'Firewall Tasks' panel
3. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

Network Zones Settings

The 'Network Zones' settings allow you to configure connections for a router/home network. (This is usually done **automatically** for you)

To view the configurations

4. Open 'Firewall Tasks' from the Tasks interface > 'Open Advanced Settings'
5. Click 'Network Zones' under Firewall from the left hand side pane
6. Click 'Network Zones' tab from the 'Network Zones' interface

Check the Loopback zone and Local Area Network #1. **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 *192.168.1.100/255.255.255.0*

Firewall Settings

The Firewall Settings option allows you to configure the protection level for your internet connection and the frequency of alerts generated.

To open Firewall Settings panel

- Open 'Firewall Tasks' from the Tasks interface > 'Open Advanced Settings'.
- Click 'Firewall Settings' under Firewall from the left hand side pane
- Ensure that 'Enable Traffic Filtering (Recommended)' is selected and choose **Safe mode** from the drop-down beside it.

Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of 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

Under 'Alert Settings' in the Advanced Settings interface:

- Deselect 'Do NOT show pop-up alerts'
- Select 'Set alert frequency level' option 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:

- Select **Filter loopback traffic**
- Ensure that the **Block fragmented IP traffic** is selected
 - **Block fragmented IP 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 i.e 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, these fragmentations can double the amount of time it takes to send a single packet and slow your download time
- Select the '**Do Protocol Analysis**' checkbox to detect fake packets used in denial of service attacks
- Select '**Enable anti-ARP spoofing**'

Click 'OK' for your settings to take effect.

Setting-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.

To view Application Rules

- Open 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.

- Click 'Application Rules' under Firewall from the left hand side pane
- Use this interface to add, edit, enable/disable or remove internet connection rules for specific applications.

To view Global Rules

- Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
- Click 'Global Rules' under Firewall from the left hand side pane
- Use this interface to add, edit, enable/disable or remove global rules which apply to all traffic

To view Predefined Firewall rulesets

- Open 'Firewall Tasks' then 'Open Advanced Settings' (bottom right)
- In the left hand menu, click 'Rulesets' under 'Firewall Settings'
- Use this interface to add, edit, enable/disable or remove rulesets

Setting up HIPS for Maximum Security and Usability

The Host Intrusion Prevention System (HIPS) component provides maximum security from malicious programs that try to execute on your system and so protects you from data theft, computer crashes and system damage. It prevents buffer overflow attacks, root-kits, inter-process memory injections, key-loggers and more.

To configure HIPS

- Open 'Advanced Tasks' and click 'Open Advanced Settings'.
- Click 'Security Settings' > 'Defense+' > 'HIPS' > 'HIPS Settings' from the left hand side pane
- Select 'Enable HIPS' and choose 'Safe Mode' from the drop-down below it.

Monitoring Settings

- Click 'Monitoring Settings' from the HIPS Settings interface
- Make sure that all the check boxes are selected and click 'OK'

Advanced Settings

- Make the following settings under Advanced in the HIPS Settings interface
 - Optional - Enable 'Block all unknown requests if the application is not running'. Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This 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
 - If you are using a 64-bit system, in order to maximize the security, it is important to select 'Enable enhanced protection mode (Requires a system restart)' - Enabling this mode will activate additional host intrusion prevention techniques in Defense+ to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures
Because of limitations in Windows 7 x64, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS in Defense+
 - In order to improve online security leave 'Show alert in case any other software attempts to modify current settings of installed browsers' is enabled. Each time a program attempts to modify your browser's settings you will see an alert

Running Untrusted Programs in the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded and/or you are not sure that you trust. There are a couple of ways of doing this:

Run a program inside the sandbox by right-clicking

1. Browse to the installation folder of the .exe file through Windows Explorer
2. Right click on the program that you want to run inside the sandbox
3. Choose 'Run in COMODO Sandbox' from the context sensitive menu

Run a program in the sandbox via the Sandbox Tasks interface

1. Click 'Sandbox Tasks' > 'Run Virtual' from the 'Sandbox Tasks' interface
2. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Note. By default, all unknown programs are automatically run in the sandbox. You can disable this behavior and/or modify sandboxing rules in the 'Auto-Sandbox' interface. To access this interface – open 'Tasks' > 'Sandbox Tasks' > Open Advanced Settings

Browse the Internet and Run Untrusted Programs Inside the Virtual Desktop

The Virtual Desktop 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 desktop, then that malware will not be able to damage your computer or access your private data.

Start the Virtual Desktop

- Click 'Tasks' > 'Sandbox Tasks' > Run 'Virtual Desktop'

Or

- Click 'Virtual Desktop' from the basic view of CIS home screen

Or

- Click the 'Virtual Desktop' shortcut button on the CIS widget

Please ensure Chromodo and Microsoft Silverlight are installed to utilize the 'Virtual Desktop' to its full potential.

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left of the Virtual Desktop
2. Select the browser you want to run

Desktop Shortcuts

Files and shortcuts on your real desktop are available to you when you open the Virtual Desktop. Simply open the Virtual Desktop, double-click on one of your desktops files or shortcut, and that item will open the virtual environment.

Shared Space

The Virtual Desktop creates a folder Shared Space in the location "C:\ProgramData\Shared Space". This space is shared by your host operating system and the Virtual Desktop and allows you to move items between the two environments. It also provides another way for you to open programs in the virtual environment.

The shared space folder can be accessed in the following ways:

- Click 'Open Shared Space' under 'Sandbox Tasks' in the 'Tasks' Interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS
- Click the 'Shared Space' shortcut icon from the CIS widget
- Click the 'Shared Space' desktop shortcut icon

To open an application or file from your host system in the Virtual Desktop

1. Open 'Shared Space' as mentioned above
2. Copy/Move your application or file into the Shared Space
3. Start the Virtual Desktop
4. Open shared space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.
5. Double click on the application/file in the shared space to open it inside the virtual Desktop.

Renew or Upgrade Licenses

You will get alerts to activate your license if you have not already done so.

Activating CIS

- Click 'Activate Now' beside 'Subscription' in the home screen to activate your License. You should have received your License key through email if you have purchased CIS Pro/Complete

For CIS Complete activation,

- Complete the registration form with the login details and password for your Comodo Accounts Manager (CAM) account.
 - If you already have an account with Comodo Accounts Manager (CAM), select 'I already have a COMODO Account'
 - Enter your username and password for the account and click 'Next'.
 - If you do not have a CAM account, select I do not have a COMODO account and click 'Next'.
- On successful validation, your license will be activated.
- Click 'Continue' to exit the wizard. The main interface will display the number of days left for the license before it should be renewed.

Renew / upgrade your license

To renew or upgrade your license,

- Click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left').
- The Product Activation Wizard will start.
- Click the '[click here](https://secure.comodo.com/home/purchase.php?aff=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUlZRkY&lid=&)' link. You will be taken to <https://secure.comodo.com/home/purchase.php?aff=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUlZRkY&lid=&>
- Select your CIS Package.
- Select 'returning user' in the 'Sign-up Information' area, enter your login and password and complete the payment procedures.

- The License key will be sent to you by email. Activate your license using the new key.

More Help

User Guide - <https://help.comodo.com/topic-72-1-623-7587-Introduction-to-Comodo-Internet-Security.html>

Community Forums - <https://forums.comodo.com/comodo-internet-security-cis-b125.0/>

Product Support (Pro and Complete customers only)

- General questions and advice – please use the Geek Buddy client to instantly chat with a Comodo technician
- Submit support tickets at <https://support.comodo.com/>

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>