COMODO
Creating Trust Online®

Comodo
Internet Security
Software Version 12.2

Quick Start Guide
Guide Version 12.2.050520

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**
- **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**
- **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 'Options' if you wish to configure advanced options.
  - After finishing the wizard, CIS runs an initial scan
  - You will be asked to choose your type of internet connection
  - On completion of scanning, the scan results are shown. You can choose the action to be taken on the threats found, if any.
  - You need to reboot your computer to complete installation.

A more detailed description of the options available during installation can be found in the installation guide at **https://help.comodo.com/topic-72-1-772-9552-CIS-Installation.html**

The Main Interface

The CIS interface is designed to be as clean and informative as possible while letting you carry out tasks with the minimum of fuss. Each tile on the home screen contains important security and update information and lets you quickly delve further into areas of interest.
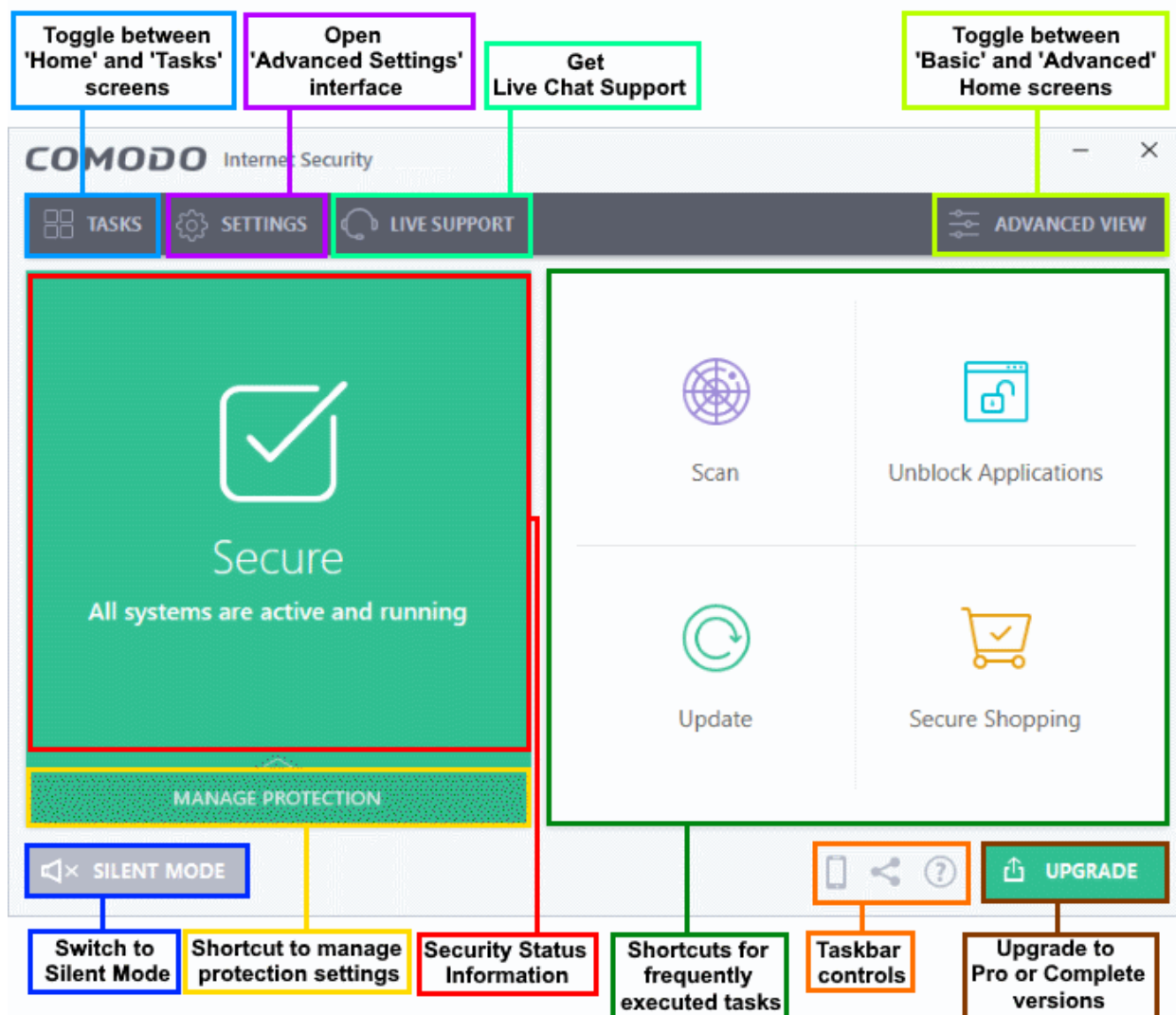
- Overall security status is shown in the large box on the left. If problems are found, this box will show a large red 'X" and a 'Fix It!' button which will allow you to remediate the issue

- Click 'Home'/'Tasks' button at the upper left to switch between the home screen and the tasks interface

- The four smaller boxes on the right of the home screen show frequently executed tasks.

- Click the 'Tasks' button at top-left then click the 'pin' icon ✎ next to your desired task to add or remove tasks in this area

- Click 'Scan' to run an instant antivirus scan

- Scan individual files or folders by right-clicking on them and selecting 'Scan with Comodo antivirus'

- Flip between 'Advanced View' and 'Basic View' by clicking the toggle button ⚏ at the upper-right

- Advanced view shows 'Antivirus', 'Containment' and 'Firewall' activities 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 lets you quickly change security settings for each component.

- The 'Manage Protection' button in the 'security information' tile lets you to turn security components on or off.

- Switch on 'Silent Mode' to make sure nothing interrupts you while you play a full screen game

- The 'Upgrade' button allows Premium users to upgrade to CIS Pro or Complete

- The tiles on the home screen provide one-click access to the antivirus scanner, updates, Secure Shopping, and more

- The 'Upgrade' button lets you upgrade to CIS Pro or Complete.

Scan and clean your computer

CIS allows you to run on-demand virus scans at any time. If any threats are found then an alert screen is shown 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

- 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.

Run a Quick Scan

- Click the 'Scan' tile on the CIS home screen

  OR
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Quick Scan' from the 'Scan' interface.
- The scanner will start and first check whether your virus signature database is up-to-date
- To pause, resume or stop the scan, click the appropriate button at the bottom of the interface
- If you want to run the scan in the background, click 'Send to Background'.
- On completion, the scan results screen is displayed. The results screen shows the number of objects scanned and the list of identified threats (Viruses, Rootkits, Malware).
- Use the drop-down menu on the right to choose whether to clean, move to quarantine or ignore each threat.

Run a Full Computer 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.

**Run a Full Computer Scan**

- Click the 'Scan' tile on the CIS home screen

  OR
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Full Scan' from the 'Scan' interface.
- The scanner will check whether your virus signature database is up-to-date 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'
- On completion, the scan results screen is displayed. The results screen shows the number of objects scanned and the list of identified threats (Viruses, Rootkits, Malware).
- Use the drop-down menu on the right to choose whether to clean, move to quarantine or ignore each threat.

Run a Rating Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Rating Scan'
- A rating scan checks the trust-rating of files and root certificates on your computer. Root certificates are used by your internet browser to validate the SSL certificates on sites you visit.
- Trust ratings are as follows:
  - **Trusted** - The file is safe to run. The root certificate was issued by a trusted certificate authority (CA).
  - **Untrusted** - The root certificate is not safe. It was not issued by a trusted CA and could be linked to fraud/phishing websites.
  - **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.
  - **Malicious** - The file is malware. Depending on your settings, CIS will either quarantine the file immediately or present you with disinfection options.

Run a Rating scan

- Click the 'Scan' tile on the CIS home screen

  OR

- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Rating Scan' from the 'Scan' interface.
- CIS will analyze all files on your computer and assign them a trust rating. File ratings are shown as follows when the scan finishes.
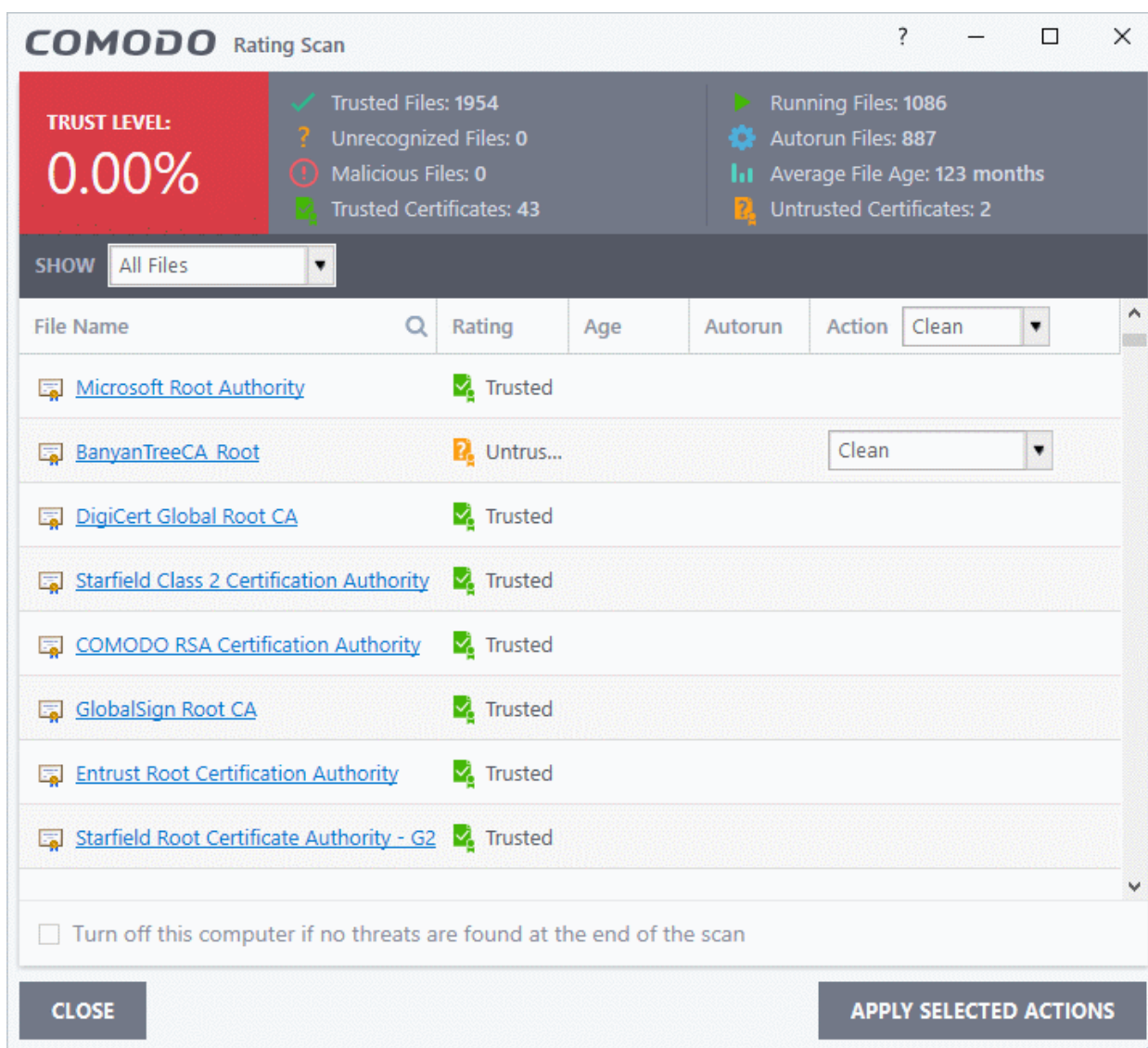
- **File Name**: The label of the scanned item

- **Rating**: The trust level of the file / SSL certificate as per the cloud based analysis

- **Age**: The length of time the item has been on your computer

- **Auto-run**: Whether or not the file automatically runs without user intervention.

- **Action:** Displays a drop-down with actions to be executed on Unrecognized and Malicious files identified.

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

  - **Clean** - Available only for untrusted/malicious items. The threat is placed in quarantine for your review. Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine' to open this area. You can restore or permanently delete files from quarantine as required. See **Manage Quarantined Items** for more details.

  - **No Action** - Ignores the warning this time only. The file or certificate is not placed in quarantine. Use this option with caution. The file/certificate will be caught again by the next rating scan you run.

  - **Trust** - Assigns a trusted rating to the item. Only select this option if you are sure the item is trustworthy.

    - **Files** - The file is awarded trusted status in the **File List** ('Settings' > 'File Rating' > 'File List'). The file will be excluded from any future rating scans.

    - **SSL Certificates** - The certificate authority (CA) who signed the certificate is awarded 'Trusted' status. CIS will allow you to connect to sites whose certificates chain to this root.

- Click the 'Apply Selected Actions' button to implement your choice.

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.
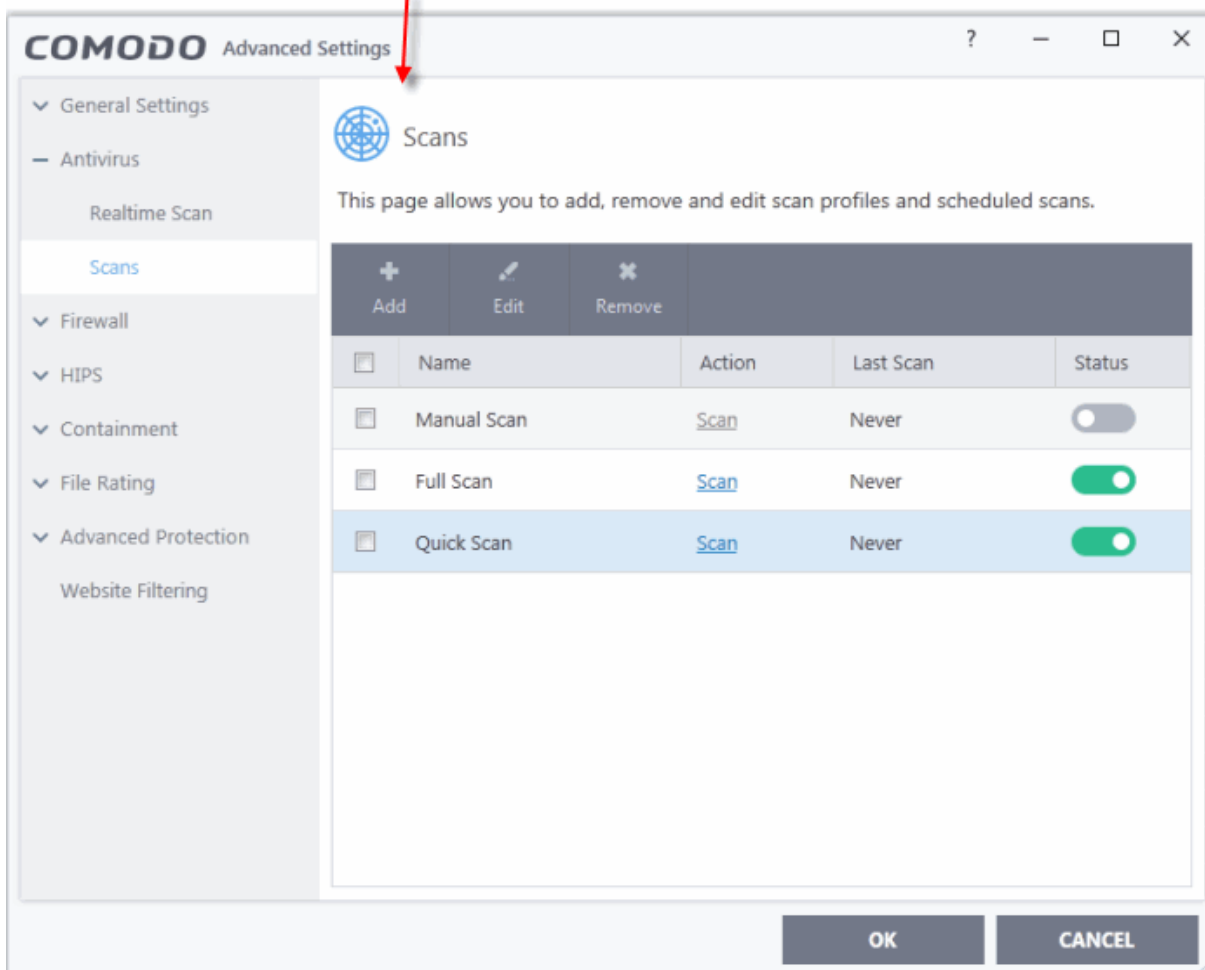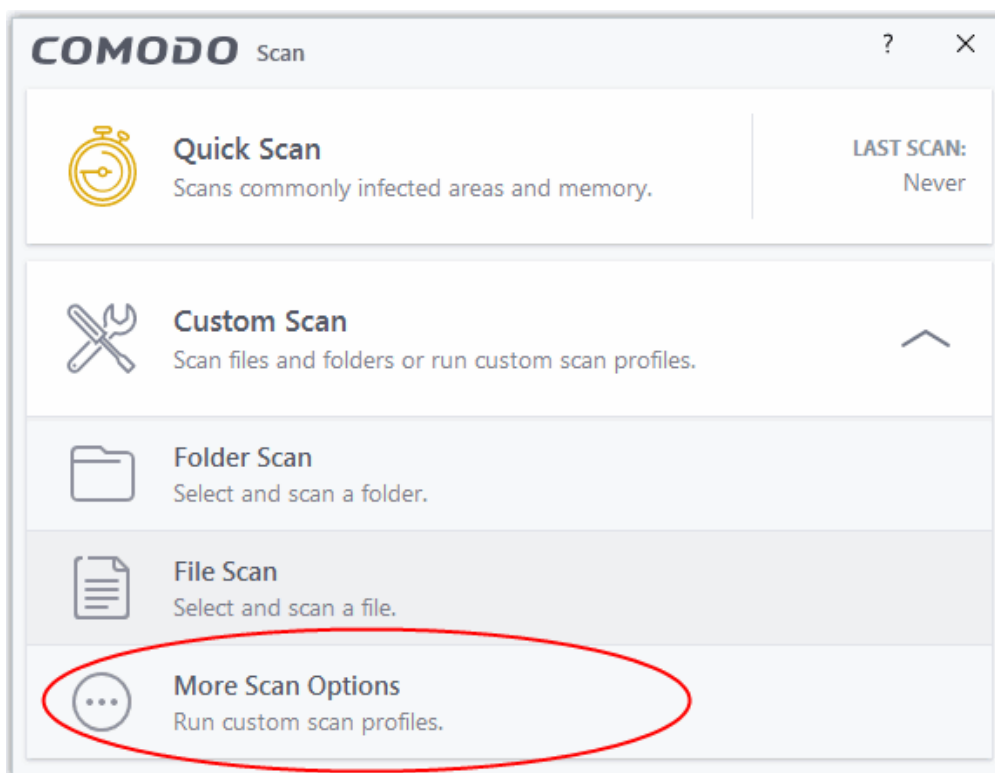
Run a custom scan

- Click the 'Scan' tile on the CIS home screen

  OR

- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Custom Scan' from the 'Scan' interface.

The 'Custom Scan' panel will open with the following options:

- **Scan a folder** - Lets you check specific folders on your hard drive, CD/DVD, or external device.
  - Browse to the target folder and click 'OK'.
- **Scan a file** - Lets you check specific files on your hard drive, CD/DVD, or external device.
  - Browse to the file you want to scan and click 'Open'.
- **More Scan options** - Create and run custom scan profiles
  - A custom scan profile lets you configure your own scan with your own scan settings.
  - You can define exactly which files and folders to scan, what time they should be scanned, and configure scan settings.
  - Once saved, you can select and run your custom scan at any time in the scans interface.

Create a custom scan profile

- Click 'Tasks' > 'General Tasks' > 'Scan' >
- Select 'Custom Scan' then 'More Scan Options'
- The 'Scans' page shows pre-defined and user created scan profiles. You can create and manage new profiles in this page:

- Click 'Add' from the options at the top create a new custom scan profile
- Type a name for the profile
- Click the 'Items' button at the top of the scan interface.

You can add items as follows:

- **Add File** - Add individual files to the profile. Click the 'Add Files' button and browse to the file you want to include.
- **Add Folder** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder you want to include. All files in the folder are covered by the scan.
- **Add Area** - Scan a specific region. The choices are 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store'.
- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice
- Click 'Options' to further customize the scan
- Click 'Scan' beside the profile name to launch your scan

Run an Instant Antivirus Scan on Selected Items

- You can scan individual files or folders instantly to check whether they contain any threats.
- This is useful if you are wary about an item you have copied from an external source or downloaded from the internet.

Instantly scan an item

- Right click on a file, folder or drive and select 'Scan with COMODO antivirus' from the context sensitive menu

  OR

- Use the toggle button at the upper-right to switch to the 'Advanced View' button
- Drag and drop the item you wish to scan into the 'Drop Files to Scan' box

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

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. Click 'Tasks' > 'Firewall Tasks'
2. Click 'Stealth Ports'
3. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

Network Zones Settings

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

View the configurations

1. Click 'Settings' on the CIS home screen
2. Click 'Firewall' > 'Network Zones'
3. Click the 'Network Zones' tab
4. 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 127.0.01/255.0.0.0
   - In most cases, the IP address of the auto detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0

---

5. Click 'OK'.

Firewall Settings

The firewall settings option lets you configure the protection level for your internet connection, and the frequency of alerts generated.

Open firewall settings panel

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Firewall' > 'Firewall Settings'
3. Select 'Enable Firewall' and choose 'Safe Mode' from the drop-down

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 same 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 ensure that the following settings are enabled 'Advanced' in the 'Firewall Settings' interface:

- 'Filter loopback traffic'
- 'Block fragmented IP traffic'
- 'Do Protocol Analysis'
- 'Enable anti-ARP'

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 and policies on an application-specific and global basis.

View application rules

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Application Rules'
- Use this interface to add, edit, enable/disable or remove internet connection rules for specific applications.
- See **Application Rules** if you need guidance on this

View global rules

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Global Rules'
- Use this interface to add, edit, enable/disable or remove global rules which apply to all traffic
- See **Global Rules** if you need guidance on this

View predefined firewall rulesets

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Rulesets'
- Use this interface to add, edit, enable/disable or remove rulesets
- See **Firewall Rule Sets** if you need guidance on this

Set up HIPS for Maximum Security and Usability

The host intrusion prevention system (HIPS) provides maximum security from malicious programs that try to execute on your system, protecting you from data theft, computer crashes and system damage. It prevents buffer overflow attacks, root-kits, inter-process memory injections, key-loggers and more.

Configure HIPS

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'HIPS Settings'
- Select 'Enable HIPS'

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
    - **Enable adaptive mode under low system resources**. Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. Enable this option to instruct CIS 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)
    - **Block all unknown requests if the application is not running**. Prohibits execution of unrecognized applications, even if CIS 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.

Run Untrusted Programs in the Container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'
    - Choose the program you want to run
    - Click 'Open'
- CIS lets you run programs inside the container on a 'one-off' basis.
- This is helpful to test new/beta programs you have downloaded but are not yet sure you trust.
- You can also create a desktop shortcut to run the application inside the container on future occasions.

Use any of the following methods to run a program in the container:
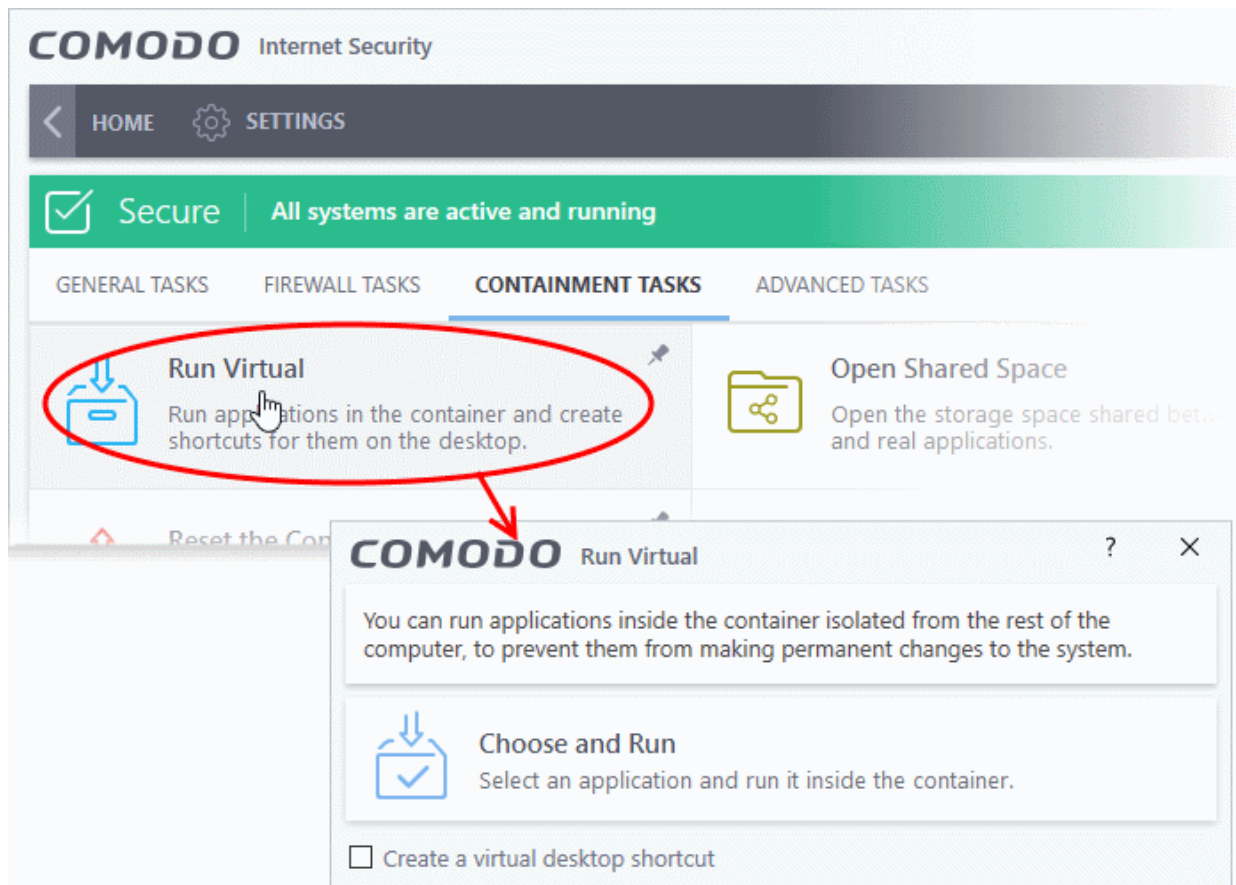
- **Right-click menu**
- **From the 'Containment Tasks' area**
- **From the widget (browsers only)**

Right-click menu

1. Navigate to the program you want to run in the container
2. Right-click on the program
3. Choose 'Run in COMODO container' from the context sensitive menu:

**The 'Containment Tasks' interface**

- Click 'Tasks' > 'Containment Tasks'
- Click the 'Run Virtual' tile

- Click 'Choose and Run', browse to your application then click 'Open'.
- The contained application will have a green border around it. Enable 'Create a virtual desktop shortcut' if you plan to run the application in the container in future.

Run browsers in the container

The CIS widget contains shortcuts to run your browsers in the container:
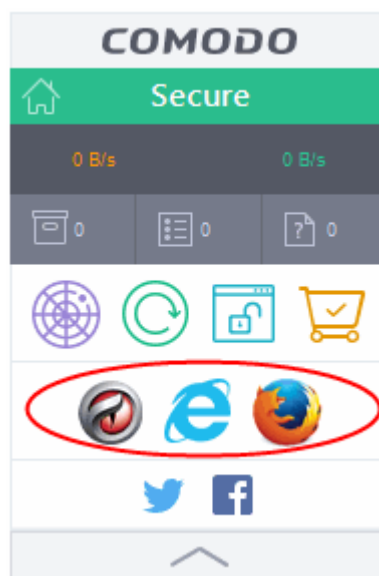
- The the browser will open with a green border.

Note. By default, all 'unknown' programs are automatically run in the container. You can disable this behavior and/or modify containment rules in the 'Auto-Containment' settings area.

- Click 'Settings' > 'Containment' > 'Auto-Containment' to access this interface

- See **Auto-Containment Rules** if you want guidance on this.

Browse the Internet and Run Untrusted Programs inside the Virtual Desktop

- The 'Virtual Desktop' provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.

- Just by visiting them, malicious websites can install malware onto your computer that can allow hackers to steal confidential information.

- Surfing the internet from inside the virtual desktop removes this threat by preventing websites from installing applications on your real computer.

- Furthermore, the virtual keyboard lets you securely enter usernames/passwords without fear of key-loggers recording what you type.

Start the Virtual Desktop

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

  Or

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

Note: Please ensure Comodo Dragon and Microsoft Silverlight are installed to utilize the 'Virtual Desktop' to its full potential.

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.

- Click 'Open Shared Space' under 'Containment Tasks' in the 'Tasks' Interface

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 the 'Shared Space' folder 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

CIS will notify you when it is time to activate or renew your license:

Activate 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 / Pro activation:

- Complete the registration form to activate your license.
    - If you already have a Comodo account, select 'I already have a COMODO Account. Enter your username and password and click 'Next'.
    - If you haven't yet created an account, select 'I do not have a COMODO account' and click 'Next'.
    - Create a new account by specifying a username and password
- Comodo servers will validate your purchase and activate your license.
- Click 'Continue' to exit the wizard. The main interface will show the number of days remaining on your license.

Renew / 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 'Get License Key' link. You will be taken to **https://secure.comodo.com/home/purchase.php** page
- Select your CIS Package.
- Select 'Existing Comodo User' in the 'Enter Customer Details' area. Type your username and password and complete the payment form.
- Your license key will be sent to you by email.
- Activate your license with the new key.

More Help

User Guide - **https://help.comodo.com/topic-72-1-766-9024-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 GeekBuddy client to instantly chat with a Comodo technician
- Submit support tickets at **https://support.comodo.com/**

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**