

# Comodo Client Security Software Version 11.4

### User Guide Guide Version 11.4.071319

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

#### COMODO Creating Trust Online\*

### **Table of Contents**

1.Introduction to Comodo Client Security	6
1.1.Special Features	9
1.2.System Requirements	11
1.3.Install Comodo Client Security	12
1.4.Start Comodo Client Security	21
1.5.The Main Interface	25
1.5.1.The Home Screen	
1.5.2.The Tasks Interface	
1.5.3.The Widget	
1.5.4.The System Tray Icon	35
1.6.Understand Security Alerts	
1.7.Password Protection	60
2.General Tasks - Introduction	61
2.1.Scan and Clean Your Computer	
2.1.1.Run a Quick Scan	64
2.1.2.Run a Full Computer Scan	66
2.1.3.Run a Rating Scan	70
2.1.4.Run a Custom Scan	73
2.1.4.1.Scan a Folder	74
2.1.4.2.Scan a File	76
2.1.4.3.Create, Schedule and Run a Custom Scan	
2.1.5.Automatically Scan Unrecognized and Quarantined Files	88
2.2.Instantly Scan Files and Folders	91
2.3.Process Infected Files	93
2.4.Manage Virus Database Updates	
2.5.Manage Blocked Autoruns	
2.6.Manage Quarantined Items	103
3.Firewall Tasks - Introduction	
3.1.Configure internet access rights for applications	
3.2.Stealth your Computer Ports	110
3.3.Manage Network Connections	112
3.4.Stop all Network Activities	113
3.5.View Active Internet Connections	115
4.Containment Tasks - Introduction	118
4.1.Run an Application in the Container	
4.2.Reset the Container	
4.3.Identify and Kill Unsafe Running Processes	125
4.4.Open Shared Space	127
4.5.The Virtual Desktop	128
4.5.1.Start the Virtual Desktop	
4.5.2.The Main Interface	136

4.5.3.Run Browsers inside the Virtual Desktop	139
4.5.4.Open Files and Run Applications inside the Virtual Desktop	142
4.5.5.Pause and Resume the Virtual Desktop	145
4.5.6.Close the Virtual Desktop	149
4.6.Containment Statistics Analyzer	150
5.Advanced Tasks - Introduction	153
5.1.Create a Rescue Disk	153
5.1.1.Download and Burn Comodo Rescue Disk	154
5.2.Remove Deeply Hidden Malware	159
5.3.Manage CCS Tasks	162
5.4.View CCS Logs	165
5.4.1.Antivirus Logs	167
5.4.1.1.Filter Antivirus Logs	
5.4.2.VirusScope Logs	173
5.4.2.1.Filter VirusScope Logs	175
5.4.3.Firewall Logs	180
5.4.3.1.Filter Firewall Logs	
5.4.4.HIPS Logs	189
5.4.4.1.Filter HIPS Logs	
5.4.5.Containment Logs	194
5.4.5.1.Filter Containment Logs	196
5.4.6.Device Control Logs	203
5.4.6.1.Filter 'Device Control' Logs	204
5.4.7.Autorun Event Logs	
5.4.7.1.Filter Autorun Events Logs	
5.4.8.Alert Logs	214
5.4.8.1.Filter 'Alerts' Logs	216
5.4.9.CCS Tasks Logs	224
5.4.9.1.Filter 'Tasks' Logs	
5.4.10.File List Changes Logs	231
5.4.10.1.Filter 'File List Changes' Logs	
5.4.11.Vendor List Changes Logs	238
5.4.11.1.Filter 'Vendor List Changes' Logs	
5.4.12.Configuration Changes	
5.4.12.1.Filter 'Configuration Changes' Logs	
5.4.13.Virtual Desktop Event Logs	
5.4.13.1.Filter Virtual Desktop Event Logs	
5.5.Submit Files for Analysis to Comodo	
5.6.View Active Process List	
6.CCS Advanced Settings	
6.1.General Settings	
6.1.1.Customize User Interface	
6.1.1.Configure Virus Database Updates	

6.1.2.Log Settings	
6.1.3.Manage CCS Configurations	279
6.1.3.1.Comodo Preset Configurations	
6.1.3.2.Personal Configurations	
6.2.Antivirus Configuration	
6.2.1.Real-time Scanner Settings	
6.2.2.Scan Profiles	
6.3.Firewall Configuration	
6.3.1.General Firewall Settings	
6.3.2.Application Rules	
6.3.3.Global Rules	
6.3.4.Firewall Rule Sets	
6.3.5.Network Zones	
6.3.5.1.Network Zones	
6.3.5.2.Blocked Zones	
6.3.6.Port Sets	
6.4.HIPS Configuration	
6.4.1.HIPS Settings	
6.4.2.Active HIPS Rules	
6.4.3.HIPS Rule Sets	
6.4.4.HIPS Groups	
6.4.4.1.Registry Groups	
6.4.4.2.COM Groups	
6.5.Protected Objects	
6.5.1.Protected Objects - HIPS	
6.5.1.1.Protected Files	
6.5.1.2.Blocked Files	
6.5.1.3.Protected Registry Keys	
6.5.1.4.Protected COM interfaces	
6.5.2.Protected Objects - Containment	
6.5.2.1.Protected Files and Folders	
6.5.2.2.Protected Keys	
6.6.Containment Settings	
6.6.1.Containment Settings	
6.6.2.Auto-Containment Rules	
6.6.3.Virtual Desktop Settings	
6.6.4.Containment - An Overview	
6.6.5.Unknown Files: The Scanning Processes	
6.7.File Rating Configuration	
6.7.1.File Rating Settings	
6.7.2.File Groups	
6.7.3.File List	
6.7.4.Submitted Files	

6.7.5.Vendor List	
6.8.Advanced Protection	503
6.8.1.VirusScope Settings	504
6.8.2.Scan Exclusions	506
6.8.3.Device Control Settings	523
6.8.4.Script Analysis Settings	530
6.8.5.Miscellaneous Settings	537
Appendix 1 - CCS How to Tutorials	541
Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily	541
Set up the Firewall For Maximum Security and Usability	544
Block Internet Access while Allowing Local Area Network (LAN) Access	551
Set up HIPS for Maximum Security and Usability	556
Create Rules to Auto-Contain Applications	558
Run an Instant Antivirus Scan on Selected Items	585
Create an Antivirus Scan Schedule	
Run Untrusted Programs inside the Container	594
Run Browsers Inside the Container	596
Restore Incorrectly Quarantined Items	598
Submit Quarantined Items to Comodo Valkyrie for Analysis	600
Enable File Sharing Applications like BitTorrent and Emule	602
Block any Downloads of a Specific File Type	607
Disable Auto-Containment on a Per-application Basis	609
Switch Off Automatic Antivirus Updates	614
Suppress CCS Alerts Temporarily	617
Control External Device Accessibility	618
Appendix 2 - Comodo Secure DNS Service	620
Router - Enable or Disable Comodo Secure DNS	621
Windows - Enable Comodo Secure DNS	622
About Comodo Security Solutions	628

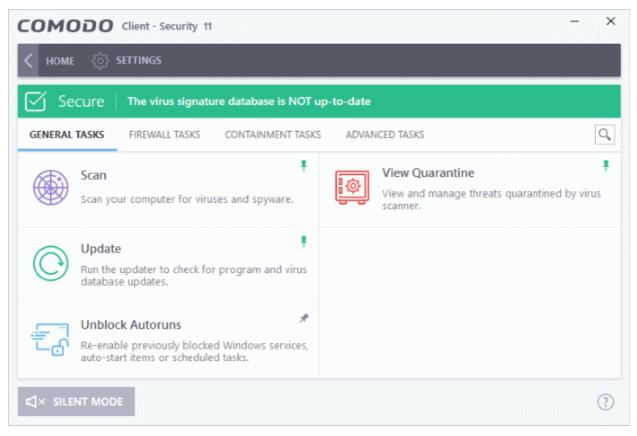
COMODO Creating Trust Online\*

# 1. Introduction to Comodo Client Security

#### **Overview**

Comodo Client Security (CCS) offers complete protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall and an advanced host intrusion prevention system (HIPS).

When used individually, each of these modules delivers superior protection against their specific threat challenge. When used together they provide a complete 'prevention, detection and cure' security system for your computer. Once installed on a Windows endpoint, CCS can be remotely configured and monitored from the Endpoint Manager console.



The software is designed to be secure 'out of the box' - so even the most inexperienced users need not have to deal with complex configuration issues after installation.

### **Comodo Client Security - Key Features:**

- Antivirus Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the always-on virus monitor and scheduled scans, you can instantly check any file by right-clicking on it. The antivirus also scans any removable storage plugged-in to your computer.
- **Firewall** Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.
- Host Intrusion Protection (HIPS) A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **Containment** Authenticates every executable and process running on your computer and prevents them from taking potentially damaging actions. Unrecognized processes and applications will be automatically

COMODO Creating Trust Online\*

run inside a security hardened environment known as a container. Once inside, they will be strictly monitored, will not be able to access other processes and will write to a virtual file system and registry. This gives untrusted (but harmless) applications the freedom to operate while untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

- Virtual Desktop A sandbox environment in which you can run programs and browse the internet without fear those activities will damage the host computer. Applications in the virtual desktop are isolated from the host operating system, write to a virtual file system, and cannot access user data.
- Advanced Protection A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
  - **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. Using a system of behavior 'recognizers', Viruscope not only detects unauthorized actions but also allows you to completely undo them. Apart from representing another hi-tech layer of protection against malware, this also provides you with the granular power to reverse unwanted actions taken by legitimate software without blocking the software entirely.
- **Rescue Disk** Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- Additional Utilities The advanced tasks section contains links that allow you to install other, free, Comodo security products Comodo Cleaning Essentials and KillSwitch.

### **Guide Structure**

This introduction is intended to provide an overview of the basics of Comodo Client Security and should be of interest to all users.

- Introduction
  - Special Features
  - System Requirements
  - Installation
- Start Comodo Client Security
- The Main Interface
- Understand Security Alerts

The remaining sections of the guide cover every aspect of the configuration of Comodo Client Security.

- General Tasks Introduction
  - Scan and Clean your Computer
    - Run a Quick Scan
    - Run a Full Computer Scan
    - Run a Rating Scan
    - Run a Custom Scan
    - Automatically Scan Unrecognized Files
  - Instantly Scan Files and Folders
  - Processing Infected Files
  - Manage Virus Database Updates
  - Manage Blocked Autoruns
  - Manage Quarantined Items
- Firewall Tasks Introduction
  - Configure internet access rights for applications
  - Stealth your Computer Ports
  - Manage Network Connections
  - Stop all Network Activities

- View Active Internet Connections
- **Containment Tasks Introduction** 
  - Run an Application in the Container
  - Reset the Container
  - Identify and Kill Unsafe Running Processes
  - Open Shared Space
  - The Virtual Desktop
  - Containment Statistics Analyzer
- Advanced Tasks An Introduction
  - Create a Rescue Disk
  - Remove Deeply Hidden Malware
  - Manage CCS Tasks
  - View CCS Logs
  - Submit Files for Analysis to Comodo
  - View Active Process List
- CCS Advanced Settings
  - General Settings
    - Customize User Interface
    - Configure Virus Database Updates
    - Log Settings
    - Manage CCS Configurations
  - Antivirus Configuration
    - Real-time Scanner Settings
    - Scan Profiles
  - Firewall Configuration
    - General Firewall Settings
    - Application Rules
    - Global Rules
    - Firewall Rule Sets
    - Network Zones
    - Port Sets
  - HIPS Configuration
    - HIPS Settings
    - Active HIPS Rules
    - HIPS Rule Sets
    - Protected Objects HIPS
    - HIPS Groups
  - Containment Configuration
    - Containment Settings
    - Auto-Containment Rules
    - Protected Objects Containment
    - Virtual Desktop Settings
    - Containment An Overview
    - Unknown Files: The Scanning Processes

COMODO Creating Trust Online\*

- File Rating Configuration
  - File Rating Settings
  - File Groups
  - File List
  - Submitted Files
  - Vendor List
- Advanced Protection Configuration
  - VirusScope Settings
  - Scan Exclusions
  - Device Control Settings
  - Script Analysis Settings
  - Miscellaneous Settings
- Appendix 1 CCS How to... Tutorials
  - Enable / Disable AV, Firewall, Auto-Containment and Viruscope Easily
  - Set up the Firewall For Maximum Security and Usability
  - Block Internet Access while Allowing Local Area Network (LAN) Access
  - Set up the HIPS for Maximum Security and Usability
  - Create Rules for Auto-Containing Applications
  - Run an Instant Antivirus Scan on Selected Items
  - Create an Antivirus Scanning Schedule
  - Run Untrusted Programs inside the Container
  - Run Browsers Inside the Container
  - Restore Incorrectly Quarantined Item(s)
  - Submit Quarantined Items to Comodo for Analysis
  - Enable File Sharing Applications like BitTorrent and Emule
  - Block any Downloads of a Specific File Type
  - Disable Auto-Containment on a Per-application Basis
  - Switch Off Automatic Antivirus and Software Updates
  - Suppress CCS Alerts Temporarily
  - Control External Device Accessibility
- Appendix 2 Comodo Secure DNS Service

### **1.1. Special Features**

### Auto-Containment

- Automatically runs unknown files inside a secure container which is isolated from the rest of your computer
- Contained programs cannot cause damage because they are denied access to the operating system, to the registry, and to user data
- · This nullifies malware and ransomware by totally removing their ability to interact with the host computer
- Simultaneously, the file is analyzed by our cloud systems to establish the trust rating of the file

#### Viruscope

- Monitors the activities of processes running on your computer and alerts you if their actions could
  potentially threaten your privacy and/or security
- Ability to reverse potentially undesirable actions of software without necessarily blocking the software



#### entirely

#### Host Intrusion Prevention System

- · Bulletproof protection against root-kits, inter-process memory injections, key-loggers and more;
- Monitors the activities of all applications and processes on your computer and allows executables and processes to run if they comply with the prevailing security rules
- Blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- Enables advanced users to enhance their security measures by quickly creating custom policies and rulesets using the powerful rules interface.

#### **Comprehensive Antivirus Protection**

- · Detects and eliminates viruses from desktops, laptops and workstations;
- Cloud based scans mean you still get 100% protection even if your database is outdated.
- Heuristic techniques identify previously unknown viruses and Trojans;
- Scans registry and system files for possible spyware infection and cleans them;
- Highly configurable on-demand scanner lets you run custom scans on any file, folder or drive;
- Daily, automatic updates of virus definitions;
- · Automatically scans external devices when they are plugged in;
- Isolates suspicious files in quarantine preventing further infection;
- Built in scheduler allows you to run scans at a time that suits you;
- Simple to use install it and forget it Comodo AV protects you in the background.

#### **Intuitive Graphical User Interface**

- Summary screen gives an at-a-glance snapshot of your security settings;
- Easy and quick navigation between each modules;
- Simple point and click configuration no steep learning curves;
- New completely redesigned security rules interface you can quickly set granular access rights and privileges on a global or per application. The firewall also contains preset policies and wizards that help simplify the rule setting process.

#### **Comodo Client Security - Extended Features**

#### **Highly Configurable Security Rules Interface**

Comodo Client Security offers more control over security settings than ever before. Users can quickly set granular Internet access rights and privileges on a global or per application basis using the flexible and easy to understand GUI. This version also sees the introduction of preset security policies which allow you to deploy a sophisticated hierarchy of firewall rules with a couple of mouse clicks.

#### **Application Behavior Analysis**

Comodo Client Security features an advanced protocol driver level protection - essential for the defense of your PC against Trojans that run their own protocol drivers.

#### Cloud Based Behavior Analysis

Comodo Client Security features cloud based analysis of unrecognized files, in which any file that is not recognized and not in Comodo's white-list will be sent to Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it behaves in a malicious manner. If yes, the file is then manually analyzed by Comodo technicians to confirm whether it is a malicious file or not. The results will be sent back to your computer in around 15 minutes.

### Event logging

Comodo Client Security features a vastly improved log management module - allowing users to export records of

COMODO Creating Trust Online\*

Antivirus, Firewall and Advanced Protection activities according to several user-defined filters. Beginners and advanced users alike are greatly benefited from this essential troubleshooting feature.

#### **Memory Firewall Integration**

Comodo Client Security now includes the buffer-overflow protection original featured in Comodo Memory Firewall. This provides protection against drive-by-downloads, data theft, computer crashes and system damage.

#### 'Training Mode' and 'Clean PC' Mode

These modes enable the firewall and host intrusion prevention systems to automatically create 'allow' rules for new components of applications you have decided to trust, so you won't receive pointless alerts for those programs you trust. The firewall learns how they work and only warn you when it detects truly suspicious behavior.

### Application Recognition Database (Extensive and proprietary application safe list)

The Firewall includes an extensive white-list of safe executables called the 'Comodo Safe-List Database'. This database checks the integrity of every executable and the Firewall alerts you of potentially damaging applications before they are installed. This level of protection is new because traditionally firewalls only detect harmful applications from a blacklist of known malware - often-missing new forms of malware as might be launched in day zero attacks.

The Firewall is continually updated and currently over 1,000,000 applications are in Comodo Safe list, representing virtually one of the largest safe lists within the security industry.

### Self Protection against Critical Process Termination

Viruses and Trojans often try to disable your computer's security applications so that they can operate without detection. CCS protects its own registry entries, system files and processes so malware can never shut it down or sabotage the installation.

#### Containment as a security feature

Comodo Client Security's 'Containment' is an isolated operating environment for unknown and untrusted applications. Because they are virtualized, applications running in the container cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have also integrated auto-containment directly into the security architecture of CCS to complement and strengthen the Firewall, Advanced Protection, Containment and Antivirus modules.

#### Submit Suspicious Files to Comodo

Are you the first victim of a brand new type of spyware? Users can help combat zero-hour threats by using the built in submit feature to send files to Comodo for analysis. Comodo then analyzes the files for any potential threats and update our database for all users.

### **Device Control**

CCS allows you full control over which type of external devices, such as USB pen drives and hard drives, can be connected to endpoints. Allow selected device class or block them all.

### 1.2. System Requirements

For Comodo Client Security to perform optimally, please ensure your systems comply with the following minimum system requirements:

#### Windows Endpoints

Windows 10 (Both 32-bit and 64-bit versions) Windows 8 (Both 32-bit and 64-bit versions) Windows 7 (Both 32-bit and 64-bit versions) Windows Vista (Both 32-bit and 64-bit versions)	<ul> <li>384 MB available RAM</li> <li>210 MB hard disk space for both 32-bit and 64- bit versions</li> <li>CPU with SSE2 support</li> <li>Internet Explorer Version 5.1 or above</li> </ul>
Windows XP (Both 32-bit and 64-bit versions)	256 MB available RAM

- 210 MB hard disk space for both 32-bit and 64bit versions
- CPU with SSE2 support
- Internet Explorer Version 5.1 or above

#### Windows Servers

- Windows Server 2003
- Windows Small Business Server 2003
- Windows Server 2008
- Windows Small Business Server 2008
- Windows Server 2008 R2
- Windows Small Business Server 2011
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

#### All operating systems

You will also need to open some ports on your firewall to allow updates and various Dragon and C1 services to function correctly:

- USA customers Click here for port information
- EU customers Click here for port information

### 1.3. Install Comodo Client Security

You can use the Endpoint Manager (EM) interface to deploy Comodo Client Security (CCS) to your endpoints. You can purchase EM as stand-alone application or as a part of the Comodo Dragon or Comodo One platform.

Please see the following links if you do not already have an EM license:

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

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

- Step 1 Enroll Users
- Step 2 Enroll Devices
- Step 3 Deploy CCS

Note - you can skip to step 3 if you have already enrolled your target devices.

### Step 1 - Enroll Users

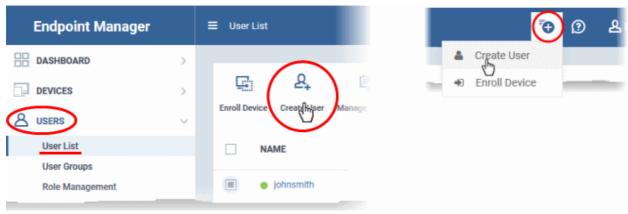
You can deploy CCS onto endpoints only after adding users to Endpoint Manager.

COMODO Creating Trust Online\*

- Dragon MSP / Comodo One MSP customers You can create multiple companies in the Dragon / C1 interface, and can enroll users to any of these companies.
- Dragon Enterprise / C1 Enterprise and stand-alone Endpoint Manager customers All users are enrolled to the default company.

#### Add a user

- Click 'Users' > 'User List' > click the 'Create User' button or
- Click the 'Add' button 😳 on the menu bar and choose 'Create User'.



The 'Create new user' form will open.

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

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Company
  - Dragon MSP and C1 MSP customers can add users from companies/organizations enrolled in their account.
  - Dragon Enterprise, C1 Enterprise, and EM stand-alone customers can only add users to the

COMODO Creating Trust Online\*

#### default company.

#### Role

A 'role' determines user permissions within the Endpoint Manager console itself. Endpoint Manager ships with two default roles:

- Administrator Full administrative privileges in the Endpoint Manager console. The permissions for this role are not editable.
- User In most cases, a 'user' will simply be an owner of a managed device who should not require
  elevated privileges in the management system. Under default settings, 'Users' cannot login to
  Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

A confirmation message is shown:

Create New User	×
You have created «John» user.	
Email: fiatliena@gmail.com	
Company: Star Inc.	
Role: Users	
Within a few minutes the user will get an email with instructions to proceed if his role supports it.	
Ok	

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

Tip: `	You can	also	bulk i	mport	users	from a	a .csv	file.	See	http	s://he	lp.c	omod	lo.coi	n/top	bic-39	99-1-7	86-12	973-
Impo	ort-User	s-fro	m-a-(	CSV-Fi	ile.htn	nl for i	nore	detai	ls.										

#### **Step 2 - Enroll Devices**

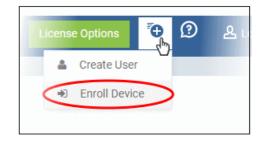
The next step is to enroll user devices so you can manage them with Endpoint Manager.

- Click 'Users' then 'User List'
- Select the user(s) whose devices you wish to enroll then click the 'Enroll Device' button Or

Click the 'Add' button 😳 on the menu bar and choose 'Enroll Device'.

COMODO Creating Trust Online\*

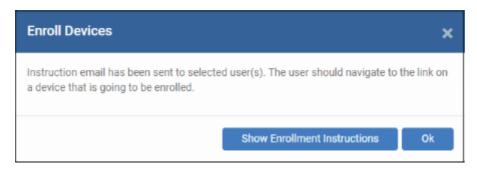
Enroll Device Create User	<b>B</b>	Send Pa Recover
NAME		EMAIL
John		fiatliena@o
🗌 🍵 queen@yopm	ail.com	queen@>>>



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

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

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



An example mail is shown below:

COMODO Creating Trust Online\*

Endpoint Manager

### Welcome to Endpoint Manager!

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

Note:

EM

 Make sure you select the procedure appropriate for your device type i.e. macOS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.

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

Device Enrollment:

Click this link to enroll your device

Sincerely, Endpoint Manager team.

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

COMODO Creating Trust Online\*



### Welcome to Endpoint Manager!

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

#### NOTE:

Make sure you select the procedure appropriate for your device type i.e. mac OS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.

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



### FOR WINDOWS DEVICES

Enroll using this link:

https://domeaspchennai-domeaspchennai-msp.dmdemo.comodo.c om:443/enroll/windows/msi/token/c400cf0776dd77b625b1bbd8a80 a097a

FOR APPLE DEVICES

Run the setup file to install the agent and enroll the target device

The following icon

appears at the bottom-right of the endpoint screen after successful enrollment.

#### **Background Note on Endpoint Manager Agent:**

- The agent is a small application installed on managed endpoints to facilitate communication between the endpoint and the Endpoint Manager server.
- The agent is responsible for receiving tasks and passing them to Comodo Client Security.
  - Example tasks include run a virus scan, update the antivirus database or generate a report.
- Each agent can only communicate with the instance of Endpoint Manager which provisioned the agent. This means the agent cannot be reconfigured to connect to another Endpoint Manager service.

### Step 3 - Deploy Comodo Client Security

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

COMODO

Endpoint Manager allows you to install Comodo applications such as Comodo Client Security (CCS) and other thirdparty MSI packages from the 'Device List' interface.

Install CCS

- Log into Dragon or Comodo One
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
  - Click the funnel icon on the right and select 'Windows', to see only Windows endpoints
  - Click 'All Devices' to view every device added to Endpoint Manager
- Select your target Windows devices using the check-boxes on the left
- Click 'Install or Update Packages' > 'Install Additional Comodo Packages':

<b>،</b> ه	Grou	p Management	Device	Management					
Enroll De		C Remote Control	Remote tools	F Run Procedure	Manage Profiles	Install or Update Packages	C Refresh Device Information	Reboot	Owner
ρs	earch	for devices					nal Comodo Pac n MSI/Packages		C
	OS	NAME		ACTIVE COMP	PONENTS PA	Install macOS	Packages		U
		John Co	omp 😲	AGCCS	Ø	Update Additi	onal Comodo Pa	ackages	20
	۵	comodo	o-Vir	AGAV		;	Saddle and Pe	Herald	20
	i T	I samsun	Ig_S	AG AV		I	Default Compa	Dyanora	20

• Make sure 'Install Comodo Client - Security' is selected in the packages dialog:

COMODO Creating Trust Online\*

Install Additional Comodo Packages	×
Install Comodo Client - Security	
Reboot options	
Force the reboot in	
5 minutes	~
O Suppress the reboot 1	
O Warn about the reboot and let users postpone it	
Reboot message	
Your device will reboot in 5 minutes because it's required by your administrator	
Inst	all
-	

- The endpoint needs to be restarted to complete the installation. You have the following reboot options:
  - **'Force the reboot in...'** restart the end-point a certain length of time after installation. Choice of 5, 10, 15 or 30 minutes:
  - **'Suppress the reboot'** Do not restart the machine after installation. CCS will only become fully functional after the device is restarted.
  - 'Warn about the reboot and let users postpone it' Show an alert to the user which advises them that their computer needs to be restarted. You can enter a custom message which is shown to the user:

COMODO ONE Client - Communication Reboot				
	Your device need reboot because it's required by your administrator			
	Remind me in 10 minutes			
	Reboot now Postpone			

Users can restart immediately by clicking 'Reboot now', or postpone the restart by picking a time in the drop-down.

- Click 'Install' to begin installation.
- The endpoint agent will download and install CCS
- The device will restart depending on the option chosen in the 'Install Additional Comodo Packages' dialog.

COMODO Creating Trust Online\*

Protection is effective immediately after the	computer restarts.	
COMODO Client - Security 11		- ×
금 TASKS 《ⓒ SETTINGS		
	Scan	<b>I</b>
Secure The virus signature database is NOT up-to- date FIX IT!	Update	Open Task Manager
		(?)

• Click 'Fix It!' to update the virus database.

The virus database will start downloading and...

COMODO Update			?	-		×
14%	TASK: Download signatures DOWNLOAD SPEED: 890.00 KB/s DOWNLOADED: 280.00 MB STATUS: Downloading: BASE_END_USER_v2	7385.cav (280.00 MB,	/280.00	MB]		
TASK		STATUS				
Check for sig	nature updates	Completed	ł			
Download signatures		In Progress (80.0%)				
PAUSE STO	P		SEND	то вас	KGROUI	ND

CUMUDO Creating Trust Online\*

COMODO Client - Security 11		- ×
吕 TASKS <ⓒ} SETTINGS		
	Scan	<b>View</b> Quarantine
Secure All systems are active and running MANAGE PROTECTION	Update	Open Task Manager
		(?)

... on completion, the virus signatures will be installed and system updated.

- Please note the settings in CCS will be configured automatically according to the applied Endpoint Manager profile.
- CCS will retain its default settings if no profiles are applied after installation. The default settings are mentioned in the guide for various configuration screens.
- CCS will retain the settings of the last applied profile if no profiles are applied at any point of time.
- Visit https://help.comodo.com/topic-399-1-786-10197-Profiles-for-Windows-Devices.html for help to configure Windows profiles.

### 1.4. Start Comodo Client Security

After installation, Comodo Client Security automatically starts whenever you start Windows.

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 Endpoint Manager (EM) profile active on the device.

#### **Normal Mode**

There are 5 different ways to open CCS if it is in normal mode:

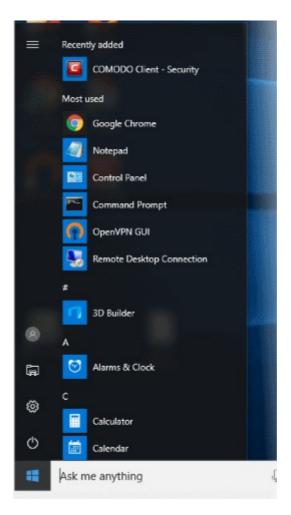
- Windows Start Menu
- Windows Desktop
- Widget
- System Tray Icon
- Windows Defender

COMODO Creating Trust Online

### Start Menu

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

(Please note the start menu varies slightly for different Windows versions.)



#### Windows Desktop

• Double-click the desktop shortcut to start Comodo Client Security. The shortcut is only visible if 'Show Desktop Shortcut' is enabled in the Endpoint Manager profile active on the endpoint.



### Widget

• Click the information bar in the widget to start CCS. The shortcut is only visible if 'Show Widget' is enabled in the Endpoint Manager profile active on the endpoint.

COMODO Creating Trust Online\*



The widget also contains other useful data and features. See 'The Widget' for more details.

### **CCS** Tray Icon

• Double-click the shield icon to start the main interface.



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

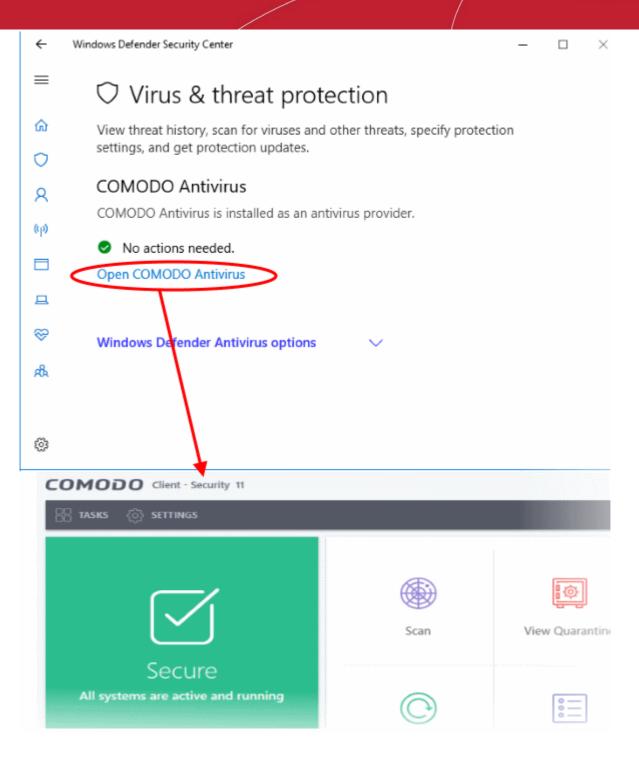
#### **Windows Defender**

- 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' to open the Comodo Client Security interface:

COMODO Creating Trust Online\*



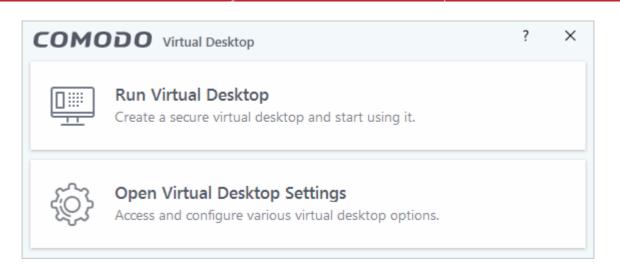
#### Virtual Desktop Only mode

- 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.
  - Endpoint Manager admins You can enable or disable this setting in the 'UI Settings' section of a profile.
  - See https://help.comodo.com/topic-399-1-786-10572-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:

COMODO Creating Trust Online\*



- 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.

#### What is an Endpoint Manager profile?

- Endpoint Manager (EM) is a product which allows admins to manage Comodo Client Security on network endpoints.
- An EM 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-399-1-786-11186-Client-Access-Control.html for help with this.

### 1.5. 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. Each tile on the home screen contains important security and update information and lets you quickly delve further into areas of interest.

- Click the 'Home/Tasks' button at the upper-left to switch between the 'home screen' and the 'tasks' interface.
- Switch on 'Silent Mode' to make sure nothing interrupts you while you are on an important task.
- The tiles on the right give you one-click access to important features, including the antivirus scanner, updates, task manager and more.

COMODO Creating Trust Online\*

Toggle between 'Home' and 'Tasks' screens		
COMODO Client - Security 11		– ×
금 TASKS 《아 SETTINGS		
	Scan	لی View Quarantine
Secure All systems are active and running	Update	Open Task Manager
MANAGE PROTECTION		
Switch to Shortcut to manage Security st information settings	tatus ion Shortcuts for frequently executed tasks	Get help and support information

Click the following links for more information:

- The Home Screen
- The Tasks Interface
- The Widget
- The System Tray Icon

### 1.5.1. The Home Screen

You can switch between the home and tasks screens by clicking the 'Home/Tasks' button at the top-left of the interface:



- The home screen has an easy to use interface that lets you quickly run common tasks and manage program settings.
- The large 'security information' tile on the left shows your overall security level and lets you quickly deal with any threats.

٠

COMODO Creating Trust Online\*

Toggle between 'Home' and 'Tasks' screens interface		
COMODO Client - Security 11		- ×
문 TASKS 《ô›› SETTINGS		
	Scan	र्छि View Quarantine
Secure All systems are active and running	Update	Open Task Manager
Switch to Shortcut to manage Security s		Get help and
silent mode protection settings informat	ion frequently executed tasks	support information

The 'Manage Protection' button lets you turn security components on or off and open advanced settings.

The security information tile on the left will inform you if any component is disabled or if other problems are found:



You can easily rectify the issue by clicking the 'FIX IT' button. 'Silent Mode' and 'Help Window' are common to both home and tasks screen.

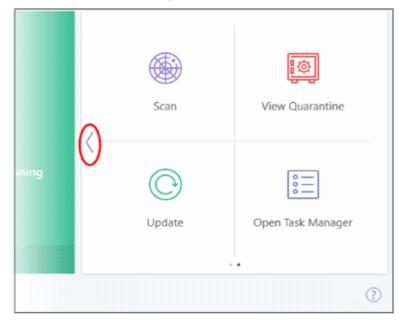
COMODO Creating Trust Online\*

From the home screen you can:

- Add shortcuts tasks
- Manage protection settings
- Set CCS to silent mode
- View the help options

#### Add tasks to the home screen

The tasks pane on the right contains a set of shortcuts which will launch common tasks with a single click. The handles at the right and left allow you to scroll through the tasks pane.



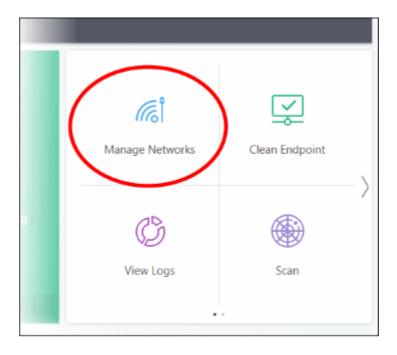
You can add tasks to this pane as follows:

- Open the 'Tasks' interface (click the button at top left to switch between the tasks and home screens).
- · Click any of the 'General', 'Firewall', 'Containment' or 'Advanced' tabs
- Right-click on the task you wish to add then click 'Add to Task Bar':

COMODO Creating Trust Online\*

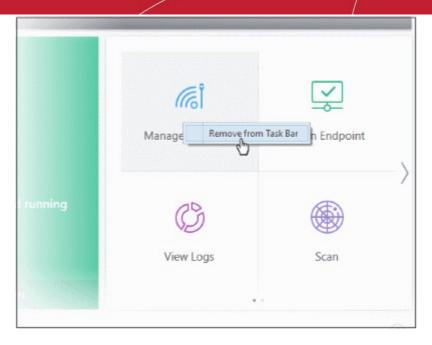
COMODO Client - Security 11	- ×
く номе <ôs settings	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Allow Application Allow an application to connect to the internet.	Allow or block connections from other computers in detected
Block Application Relock an application from accessing the internet.	Stop Network Activity Block all network activity to and from this PC.
Stealth Ports Manage this PC's network visibility from other PC's.	View Connections View applications which are connected to the internet.
r⊄× SILENT MODE	?

- Alternatively, you can add task shortcuts to the home screen by clicking the 'pin' 💌 button at the top-right of any tile.
- The selected task will be added to the tasks pane.



• To remove a task shortcut from the pane, right click on it and choose 'Remove from Task Bar'.

COMODO Creating Trust Online\*



### **Manage Protection Settings**

- Click the 'Manage Protection' button on the home screen to enable or disable various security components.
- Click on any component name to open its dedicated settings screen.

COMODO Creating Trust Online\*

COMODO Client - Security 11		
吕 TASKS {္ဟိ} SETTINGS		
MANAGE PROTECTION X		
Antivirus		EQ.
💫 Firewall		
The Auto-Containment	Scan	View Quarante
Auto-Containment       Image: HIPS		
- O- VirusScope	C	0 — 0 —
<u>↑</u>	Update	Open Task Man
		•
⊄X SILENT MODE		
	Update	Open Task Mar
MANAGE PROTECTION		
		•

See the following sections for more details about each of the protection settings:

- Antivirus Configuration
- Firewall Configuration
- Auto-Containment
- HIPS Configuration
- VirusScope Configuration

#### Silent mode

Silent mode lets you use your computer without interruptions from CCS. Operations that could interfere with your work are either suppressed or postponed.

In silent mode:

- All protection components remain 100% active
- HIPS/Firewall alerts are suppressed.
- AV updates and scheduled scans are postponed

COMODO Creating Trust Online\*

#### Switch to Silent mode

Click the 'Silent Mode' button at the bottom-left of the home screen

		N. S. C.
	View Logs	Scan
MANAGE PROTECTION	•	
		3
COMODO Client - Security 11		- ×
금 TASKS <ි SETTINGS		
Ц×	้ได้	Щ.
UN	Manage Networks	Clean Endpoint
Silent Mode All systems are in silent mode	10	$\rightarrow$
	(Č)	
	View Logs	Scan
MANAGE PROTECTION		
		0

• Deactivate 'Silent Mode' to resume alerts and notifications.

#### **Help Options**

The 'Help' button lets you view our online help guide, run a diagnostics test on your installation, and view the product version.



• Online Help - Opens Comodo Client Security's online help guide at http://help.comodo.com

COMODO Creating Trust Online\*

- Diagnostics Helps to identify any problems with your installation.
- About Contains version details and legal information:

сомодо	About		? ×
	COMODO Client - Security 11		
	Product Version:	11.4.0.7599	
	Database Version:	30983 Import Virus Database	
	File Rating Database Version:	1546416603	
	Valkyrie:	Activated Show	
Patents Pending. Copyright © 2005-2	2019 COMODO.	<u>VirusScope Details</u>	
	arks and logos are property of their re or endorsement by the trademark owr	spective owners. Any use is for identification only an ner.	d does not
			ОК

- Product Version The CCS version number.
- **Database Version** The version of the virus database you currently have installed. Click 'Import Virus Database' to replace the current version with a locally stored database.
- File Rating Database Version The version of the file rating database used by Endpoint Manager. Click 'Security Sub-Systems' > 'Application Control' in Endpoint Manager to view the file rating interface.
- Valkyrie Indicates whether or not Valkyrie is enabled. Click 'Show' to view your Valkyrie account activation number.
- Click VirusScope Details to view the VirusScope recognizers that are active on your system. See 'VirusScope Settings' for more details.

### 1.5.2. The Tasks Interface

- Click 'Tasks' on the top-left of the home screen
- The tasks area lets you configure every aspect of Comodo Client Security.

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K HOME {្រ្ទ័រ SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Scan Scan your computer for viruses and spyware.	View Quarantine View and manage threats quarantined by virus scanner.
Update         Image: The second	
Unblock Autoruns         Re-enable previously blocked Windows services, auto-start items or scheduled tasks.	
r⊈× SILENT MODE	?

Tasks are broken down into four main sections. Click the following links for more details on each:

- General Tasks Run antivirus scans and update the virus database. See 'General Tasks' for more details.
- Firewall Tasks Allow or block internet access for specific applications, manage networks, view active connections, and more. See 'Firewall Tasks' for more details.
- Containment Tasks Run applications in a secure virtual environment, start the virtual desktop, view active processes, and more. See 'Containment Tasks' for more details.
- Advanced Tasks Create a boot disk to clean highly infected systems, submit files to Comodo for analysis, install other Comodo security software, and more. See 'Advanced Tasks' for more details.

### 1.5.3. The Widget

- The CCS widget is a handy control that lets you launch key tasks, view your security status, and more.
- The widget is disabled by default but can be enabled from the 'System Tray Icon' or the 'User Interface' settings screen.
- Right-click on the widget to enable or disable CCS components and configure various settings. The menu is similar to the one available if you right-click on the system tray icon. See 'The System Tray Icon' for more details.

сомодо	сомодо	сомодо	сомодо	
습 Secure	🏠 🛛 At Risk	🏠 Silent Mode	💮 Needs Attention	
0 🗐 0 📰 0	<b>₽</b> ∘ <b>∷</b> ∘ ? <b>`</b> ∘	0 🗄 1 🖓 0	□o 🗄 1 ?`o	
♥ ♥ ● ○	() ¥ 🖗 🕑	() 🖾 🛞 ()	() 🖓 🏵 🕑	
8002	ලි 🙆 🤤 ලි	ලි 🙆 🤤 ලි	ලි 🙆 🤤 🔁	
$\sim$	$\sim$	$\sim$	$\sim$	

COMODO Creating Trust Online\*

- The color-coded bar at the top of the widget shows your current security status.
  - Double-click on 'At Risk' or 'Needs Attention' statuses to view the recommended fixes.
- The second row tells you about various CCS processes:
  - The first button shows the number of programs/processes that are currently running in the container.
    - Click the button to view a list of all processes running in the container.
    - See View Active Process List and Identify and Kill Unsafe Processes for more details.
  - The second button shows the number of CCS tasks that are currently running. Click the button to open the 'Task Manager' interface.
  - The third button shows how many unrecognized files have been added to the file list and are pending submission to Comodo. Click the button to view a list of these files.

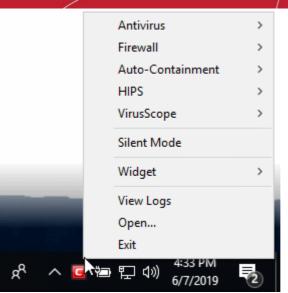
The status pane is disabled by default. Right-click on the tray icon then select 'Widget' > 'Show Status Pane' to enable it.

- The third row contains shortcuts for the common tasks you see on the CCS home screen.
  - Click a shortcut on the widget to run the task.
  - The common tasks row is disabled by default. Right-click on the tray icon then select 'Widget' > 'Common Tasks' to enable it.
- The fourth row shows browsers installed on your computer.
  - Click a browser icon to run the browser in the container. You can tell the browser is running in the container because it has a green border around it. See 'Run an application inside the container' if you want to read more on this.
  - The browsers row is disabled by default. Right-click on the tray icon then select 'Widget' > 'Show Browsers Pane' to enable it.
- You can expand or collapse the widget by clicking the arrow at the bottom.

### 1.5.4. The System Tray Icon

- Double-click the tray icon icon to quickly open the CCS interface
- Right-click on the tray icon to enable or disable various security settings.

COMODO Creating Trust Online\*



- Antivirus Enable or disable the real-time virus monitor.
- Firewall Enable or disable the firewall.
- Auto-Containment Enable or disable auto-containment. See 'Auto-Containment Rules' for more details.
- HIPS Enable or disable the host intrusion protection system.
- VirusScope Enable or disable VirusScope.

The security panel and the widget will turn red if you disable any of the security components listed above. You will also see a pop-up which lets you specify how long to keep the feature disabled:

COMODO Client - Security	? ×
Turn Off You have just turned off a realtime sec	urity component.
Disabling a security component reduces the	protection on this
computer.	
computer. How long should it stay disabled?	

• Select the period and click 'OK'.

Unless you select 'Permanently', the security component will be re-enabled after the set time period. You can manually re-enable the component at any time by right-clicking the tray icon and selecting 'Enable'.

• Silent Mode - Disables CCS alerts and activities that could potentially interrupt your work.

In silent mode:

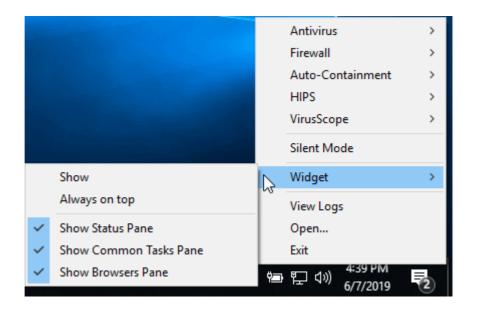
- · All security and protection technologies remain fully active
- HIPS/Firewall alerts are suppressed

COMODO Creating Trust Online\*

• AV updates and scheduled scans are postponed

Deactivate silent mode to resume alerts and scheduled scans.

Widget - Select whether or not the Widget is shown, and configure widget elements:



- Show: Toggle widget visibility. (Default = Disabled)
- Always on top: Shows the widget on top of all windows currently running on your computer. (*Default = Disabled*)
- Show Status Pane: Show overall security status in the widget (Default = Disabled)
- Show Common Tasks Pane: Show shortcuts to common CCS tasks in the widget. (Default = Enabled)
- Show Browsers Pane: Show shortcuts to browsers in the widget. (Default = Enabled)
- View Logs Opens the CCS log viewer module. The log viewer contains a history of events from various CCS security modules. See View CCS Logs for more details.
- **Open** Opens the CCS interface.
- Exit Closes the CCS application.

### 1.6. Understand Security Alerts

- Alerts Overview
  - Alert Types
  - Severity Levels
  - Descriptions
- Antivirus Alerts
- Auto-Scan Alerts
- Firewall Alerts
- HIPS Alerts
  - Device Driver Installation and Physical Memory Access Alerts
  - Protected Registry Key Alerts
  - Protected File Alerts
- Containment Alerts

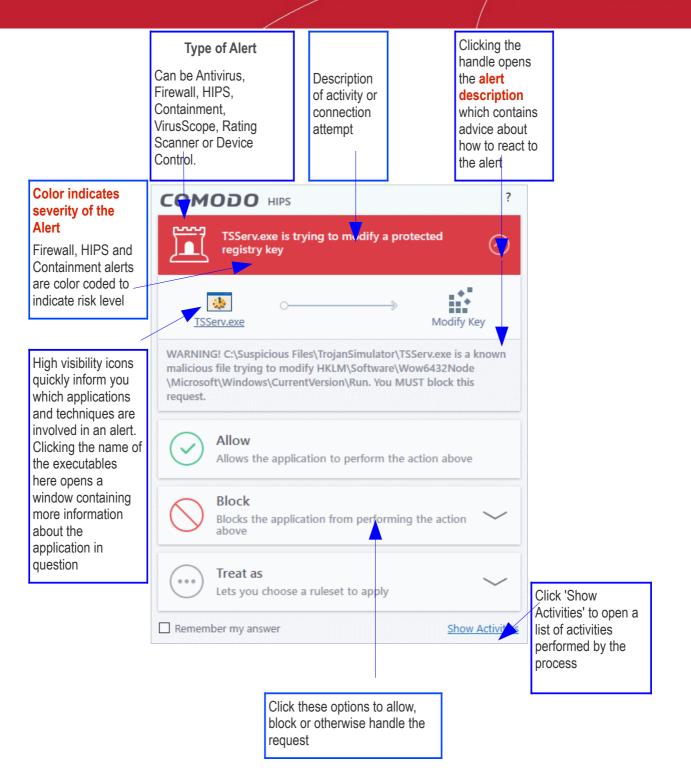
COMODO Creating Trust Online\*

- Containment Notification
- Elevated Privilege Alerts
- File Rating Alerts
- VirusScope Alerts
- Device Control Notifications

#### **Alerts Overview**

- CCS alerts warn you about security related activities at the moment they occur.
- Each alert contains information about a particular issue so you can make an informed decision about whether to allow or block it.
- Alerts also let you specify how CCS should behave in future when it encounters activities of the same type.
- The following screenshot shows the basic layout of a CCS alert:

COMODO



#### **Alert Types**

The type of alert you see depends on the security module which generated the alert. Click the links below to find out more about each alert type.

- Antivirus Alerts Shown whenever virus or virus-like activity is detected. AV alerts are shown if the antivirus is enabled and 'Do not show antivirus alerts' is disabled in Real-time Scanner Settings.
- Auto-Scan Alerts Shown when you connect an external storage device to your computer. Auto-scan alerts are shown if antivirus is enabled and 'Do not show auto-scan alerts' is disabled in Real-time Scanner Settings.
- Firewall Alerts Shown whenever a process attempts unauthorized network activity. Firewall alerts will
  be displayed only if firewall is enabled and the option 'Do not show popup alerts' is disabled in
  Firewall Settings.

- HIPS Alerts Shown when a process attempts an unauthorized action or tries to access protected areas. HIPS alerts are shown if HIPS is enabled and Do NOT show popup alerts is disabled.
- Containment Alerts (including Elevated Privilege Alerts) Shown when CCS automatically contains an file. This usually happens if the file has an 'unknown' trust-rating. If privilege elevation alerts are enabled in Containment Settings, you will also see this type of alert if a program requires admin privileges to run.
- VirusScope Alerts Shown when a running process tries to perform a suspicious action. VirusScope alerts let you quarantine the process & reverse its changes, or let the process go ahead. Be especially wary if a VirusScope alert appears 'out-of-the-blue' when you have not made any recent changes to your computer. VirusScope alerts are generated if VirusScope is enabled in advanced settings.
- **Device Control Notifications** Shown when an external device that is blocked by the admin is connected to your system. These alerts are shown if 'Device Control' and 'Show notifications when devices...' are both enabled in **Device Control Settings**.

Alerts may contain very important security warnings, or may simply occur because you are running a certain application for the first time. Your reaction should depend on the information in he alert.

Note: This section is concerned with alerts generated by CCS security modules (antivirus, firewall, HIPS etc). See Comodo Message Center notifications, Notification Messages and Information Messages for other types of alert.

#### Severity Level

The color of the alert shows the risk level of the reported activity.

- Yellow Low Severity In most cases, you can safely approve these requests. The 'Remember my answer' option is automatically pre-selected for safe requests
- Orange Medium Severity Read the information in the alert description area before making a decision. These alerts could be the result of harmless activity by program you trust, but could also indicate malicious activity. If you know the application to be safe, then it is usually okay to allow the request. If you do not recognize the application or connection request then you should block it.
- **Red** High Severity Known malware discovered, or highly suspicious behavior by an application/process. Carefully read the information provided when deciding whether to allow it to proceed.

Note: Antivirus alerts are not ranked in this way. They always appear with a red bar.

#### **Alert Description**

The description is a summary of the nature of the alert and can be revealed by clicking the handle as shown:

COMODO Creating Trust Online\*

unit.exe is trying to modify a protected file or directory		?
unit.exe is a safe application signed by Comodo Security Solutions, Inc. It is about to modify the contents of C:\ProgramData\Comodo \lps4\lps-ca\vt.db-journal. This usually happens when you try to install		nodify a protected file or
It is about to modify the contents of C:\ProgramData\Comodo \lps4\lps-ca\vt.db-journal. This usually happens when you try to install	unit.exe	Installer or Updater
or update an application. If you are not performing any of these operations, you may consider blocking this request.	It is about to modify the contents \lps4\lps-ca\vt.db-journal. This usu or update an application. If you are	of C:\ProgramData\Comodo ually happens when you try to install e not performing any of these

The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

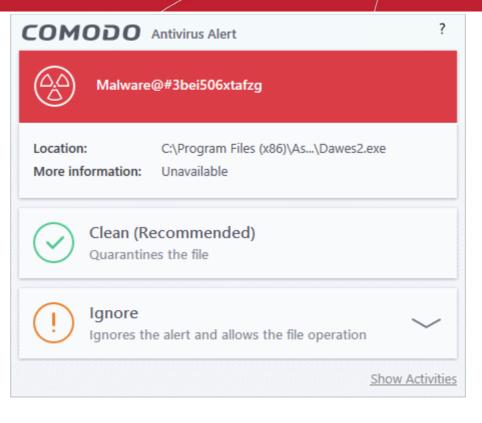
Now that we have outlined the basic construction of an alert, let's look at how you should react to them.

#### **Answer an Antivirus Alert**

Comodo Client Security generates an antivirus alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such as 'Clean' or 'Ignore'.

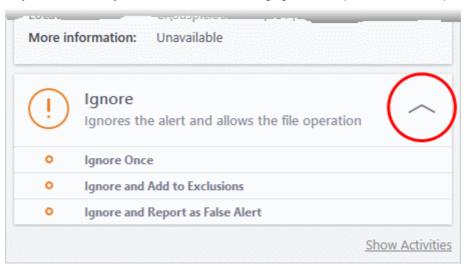
**Note**: Antivirus alerts will be displayed only if the option 'Do not show antivirus alerts' is disabled. If this setting is enabled, only **antivirus notifications** are shown. This option is found under 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** for more details.

COMODO Creating Trust Online\*



The following response-options are available:

- Clean Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to quarantine, an isolated storage in which the item is encrypted and stored. Files in the quarantine cannot be executed. If desired, you can submit the file/application to Comodo for analysis from the Quarantine interface. See Manage Quarantined Items for more details on quarantined files.
- Ignore Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



- Ignore Once -The file is allowed to run this time only. If the file attempts to execute on future
  occasions, another antivirus alert is displayed.
- Ignore and Add to Exclusions The file is allowed to run and is moved to the Exclusions list effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application
  runs again.
- Ignore and Report as a False Alert If you are sure that the file is safe, select 'Ignore and Report as a
  False Alert'. CCS will then submit this file to Comodo for analysis. If the false-positive is verified (and
  the file is trustworthy), it will be added to the Comodo safe list.

COMODO Creating Trust Online\*

#### **Antivirus Notification**

If you have chosen to not to show Antivirus Alerts through **Settings > Realtime Scanner Settings** by leaving the option 'Do not show antivirus alerts' enabled (*default=enabled*) and If CCS identifies a virus or other malware in real time, it will immediately block malware and provide you with instant on-screen notification:

8	Malware Stopped
0	Malware@#3bei506xtafzg
	C:\Program Files (x86)\Astronomy
	Calculators V2\Calculators\Dawes2.exe

#### **Answer Auto-Scan Alert**

Auto-scan alerts appear when you plug a removable device into your computer (USB stick, portable HDD, etc). The alert asks you whether you want to scan the device for viruses.

These alerts are only shown if 'Do not show auto-scan alerts' is disabled in 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** if you want to read more.

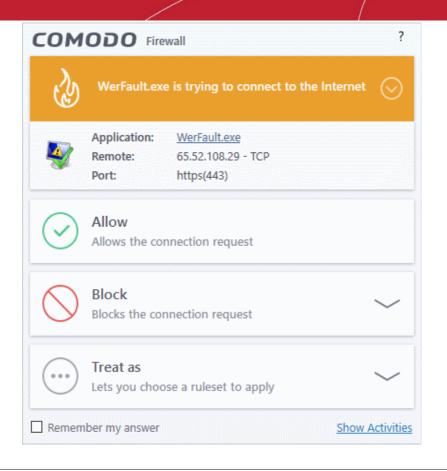
сом	ODO Antivirus ?	
	We've just detected that new removable media device has been connected (D:\). We recommended to scan it.	
$\bigcirc$	<b>Scan</b> Scan the device to make sure it's not infected.	
(!)	Ignore Skip the scan. Note: malware undetected now may harm your and other computers later.	
Remember my answer		

- Scan CCS checks the device for viruses using the settings in the 'Manual Scan' profile. If this is not available then the scan uses the settings in the 'Full Scan' profile.
- Ignore The device is not scanned
  - Remember my answer CCS will automatically carry out your choice of scan or ignore when the device is connected in future. This only applies to the specific device. You will still see an alert if you connect a different device.

#### **Answer Firewall Alerts**

CCS generates a firewall alert when it detects unauthorized network connection attempts or when traffic runs contrary to one of your application or global rules. Each firewall alert allows you to set a default response that CCS should automatically implement if the same activity is detected in future. The followings steps will help you answer a Firewall alert:

COMODO Creating Trust Online\*

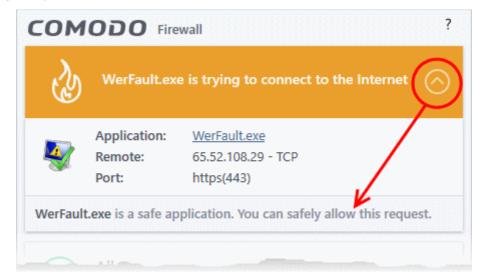


Tip: Click 'Show Activities' to view actions performed by the process in question.

This link is only shown if VirusScope is enabled in **Settings > VirusScope**.

The 'Show Activities' link is grayed-out if the process had not started before the alert was generated.

Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall
can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe
applications). If the application is known to be safe - it is written directly in the security considerations
section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be
recognized you are informed of this.



If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.

In all cases, clicking on the name of the application opens a properties window that can help you determine whether

COMODO Creating Trust Online

or not to proceed:

WerFault Properties	×	COMODO Firewall ?
The second se	Details Previous Versions Comodo Digital Signatures	WerFault.exe is trying to connect to the Internet 📀
WerFault 🛛		Application: (WerFault.exe)
Type of file: Application (.ex Description: Windows Probl		Remote:         65.52.108.29 - TCP           Port:         https(443)
Location: C:\Windows\S Size: 254 KB (260,9) Size on disk: 256 KB (262,1)	50 bytes)	Allow Allows the connection request
Modified: Friday, July 10,	2015, 4:00:34 AM 2015, 4:00:34 AM	Block Blocks the connection request
Accessed: Friday, July 10,	2015, 4:00:34 AM	Treat as       Lets you choose a ruleset to apply
		Remember my answer Show Activitie

If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to 'Block' the connection (connection is not allowed to proceed), 'Block and Terminate' (connection is not allowed to proceed and the process/application that made the request is shut down) or 'Block, Terminate and Reverse' (connection is not allowed to proceed, the process/application that made the request is shut down and the changes made by the process/application to other files/processes in the system will be rolled back).

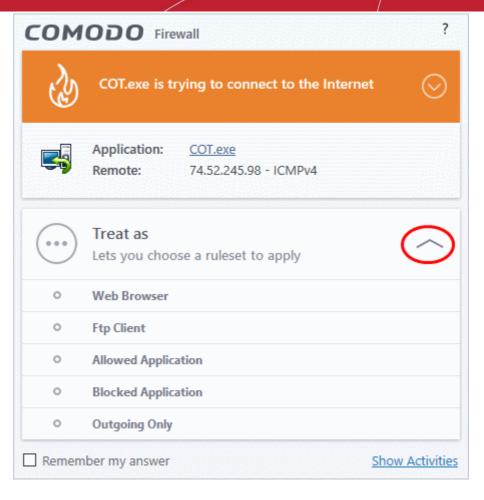
COMODO Creating Trust Online\*

сом	ODO Fire	wall	?
Ì	WerFault.exe	e is trying to connect to the Internet	$\odot$
<b>V</b>	Application: Remote: Port:	<u>WerFault.exe</u> 65.52.108.29 - TCP https(443)	
$\bigcirc$	Block Blocks the con	nnection request	$\bigcirc$
0	Block Only		
0	Block and Term	inate	
•	Block, Terminat	e and Reverse	
	Treat as Lets you choo	se a ruleset to apply	$\sim$
Remem	ber my answer	Show /	<u>Activities</u>

Note: 'Block, Terminate and Reverse':

- This option is only available if VirusScope is enabled in Settings > VirusScope.
- The option is only shown if the process in question has actually started by the time the alert was generated.
- 2. If you are sure that it is one of your everyday application, try to use the 'Treat As' option as much as possible. This allows you to deploy a predefined firewall ruleset on the target application. For example, you may choose to apply the policy Web Browser to the known and trusted applications like 'Comodo Dragon', 'Firefox' and 'Google Chrome'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.

COMODO Creating Trust Online\*



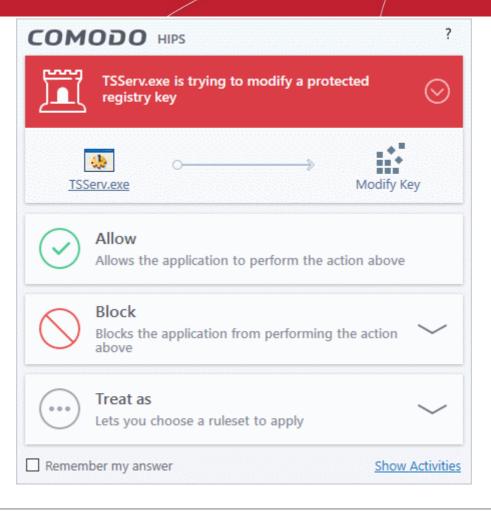
Remember to check the box 'Remember My Answer' for the ruleset to be applied in future.

 If the Firewall alert reports a behavior, consistent with that of a malware in the security considerations section, then you should block the request AND select **Remember My Answer** to make the setting permanent.

#### **Answer HIPS Alerts**

Comodo Client Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:

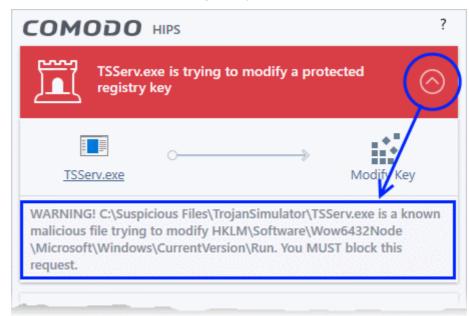
COMODO Creating Trust Online\*



**Tip**: Click 'Show Activities' to view actions performed by the process in question. This link is only shown if VirusScope is enabled in **Settings** > **VirusScope**.

The 'Show Activities' link is grayed-out if the process had not started before the alert was generated.

 Carefully read the information displayed after clicking the handle under the alert description. Comodo Client Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.



If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

If you don't recognize the application then we recommend you select **Block** the application. By clicking the handle to expand the alert, you can choose to

- 'Block' The application is not allowed to run
- 'Block and Terminate' The application is not allowed to run and the processes generated by it are terminated thereby shutting down the application
- 'Block, Terminate and Reverse' The application is not allowed to run, the processes generated by it are terminated and the changes made by the processes/application to other files/processes in the system will be rolled back.

сом	ODO HIPS ?
	TSServ.exe is trying to modify a protected of the second s
[ <u>TSS</u>	Serv.exe Modify Key
$\bigcirc$	Block Blocks the application from performing the action
0	Block Only
0	Block and Terminate
•	Block, Terminate and Reverse
	Treat as Lets you choose a ruleset to apply
Remem	ber my answer Show Activities

Note: 'Block, Terminate and Reverse' is only shown if VirusScope is enabled in Settings > VirusScope.

2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a **predefined HIPS ruleset** to the target application and allows the application to run with access rights and protection settings as dictated by the chosen ruleset.

COMODO Creating Trust Online\*

сом		?
	TSServ.exe is trying to modify a protec registry key	ted 😔
TS	Serv.exe	Modify Key
	Treat as Lets you choose a ruleset to apply	$\bigcirc$
0	Installer or Updater	^
0	Allowed Application	
0	Windows System Application	
0	Isolated Application	
0	Limited Application	¥
Remen	nber my answer	Show Activities

Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select 'Installer or Updater', you may consider using it temporarily with **Remember My Answer** left unchecked.

3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity is legitimate, then Comodo recommends blocking these requests.

COMODO HIPS ?	COMODO HIPS ?
drvinst.exe is trying to modify a protected file or directory	TSServ.exe is trying to access TSServ.exe in memory
drvinst.exe Installer or Updater	ISServ.exe
Allow Allows the application to perform the action above	Allow Allows the application to perform the action above
Block Blocks the application from performing the action	Block Blocks the application from performing the action
Treat as       Lets you choose a ruleset to apply	Treat as       Lets you choose a ruleset to apply
Remember my answer <u>Show Activities</u>	Remember my answer     Show Activities

COMODO Creating Trust Online\*

4. **Protected Registry Key** Alerts usually occur when you install a new application. If you haven't been installing a new program and do not recognize the application requesting the access, then a 'Protected Registry Key Alert' should be a cause for concern.

	?
TSServ.exe is trying to modify a protected registry key	$\odot$
O→ Modir	fy Key
Allow Allows the application to perform the action abo	ove
Blocks the application from performing the action above	on 🗸
•••• Treat as Lets you choose a ruleset to apply	$\sim$
Remember my answer Sh	now Activities

5. **Protected File Alerts** usually occur when you try to download or copy files or when you update an already installed application.

COMODO HIPS ?	COMODO HIPS ?
unit.exe is trying to modify a protected file or directory	taskhostw.exe is trying to access a protected COM interface
unit.exe Installer or Updater	taskhostw.exe
Allow Allows the application to perform the action above	Allow Allows the application to perform the action above
Block Blocks the application from performing the action	Block Blocks the application from performing the action
Image: Treat as       Lets you choose a ruleset to apply	Treat as       Lets you choose a ruleset to apply
Remember my answer     Show Activities	Remember my answer Show Activities

Were you installing new software or trying to download an application from the Internet? If you are

COMODO

downloading a file from the 'net, select **Allow**, without selecting **Remember my answe**r option to cut down on the creation of unnecessary rules within the firewall.

If an application is trying to create an executable file in the Windows directory (or any of its sub-directories) then pay special attention. The Windows directory is a favorite target of malware applications. If you are not installing any new applications or updating Windows then make sure you recognize the application in question. If you don't, then click **Block** and choose **Block Only** from the options, without selecting **Remember My answer** option.

If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking **Treat As** and choosing **'Isolated Application'** from the options.

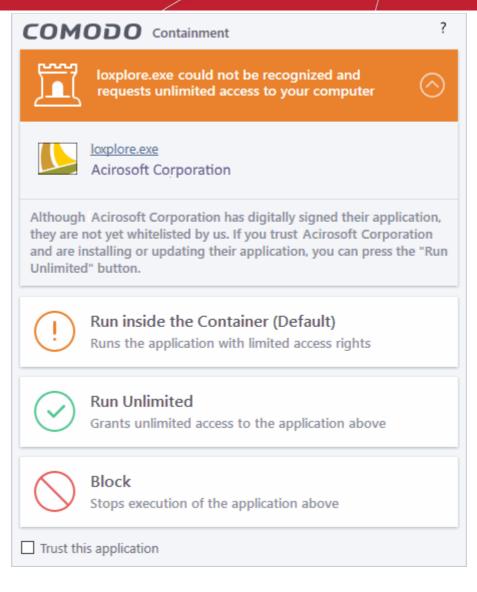
- If a HIPS alert reports a malware behavior in the security considerations area then you should Block the request permanently by selecting Remember My Answer option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.
- 7. Unrecognized applications are not always bad. Your best loved applications may very well be safe but not yet included in the Comodo certified application database. If the security considerations section says "If xxx is one of your everyday applications, you can allow this request", you may allow the request permanently if you are sure it is not a virus. You may report it to Comodo for further analysis and inclusion in the certified application database.
- If HIPS is in 'Paranoid' mode, you probably are seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. If required, you may review files with 'Unrecognized' rating in the 'File List' interface and remove them from the list.
- 9. Avoid using Trusted Application or Windows System Application policies for you email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

#### **Answer a Containment Alert**

Comodo Client Security generates a containment alert if an application or a process tries to perform certain modifications to the operating system, its related files or critical areas like Windows Registry and when it automatically contained an unknown application.

Please read the following advice before answering a Containment alert:

COMODO Creating Trust Online\*



 Carefully read the information displayed after clicking the handle under the alert description. Comodo Client Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.

COMODO

COMODO Containment	?
Ioxplore.exe could not be recognized and requests unlimited access to your computer	$\bigcirc$
Acirosoft Corporation	
Although Acirosoft Corporation has digitally signed their application has digitally signed their application and are installing or updating their application, you can press Unlimited" button.	ration
Run inside the Container (Default)	

 If you are sure that the application is authentic and safe and you simply want it to be allowed to continue then you should select **Run Unlimited**. If you want the application not to be monitored in future, select 'Trust this application' checkbox. The application will be added to **Trusted Files** list.

	nstaning or updating their application, you can press the "kun d" button.
(!)	Run inside the Container (Default) Runs the application with limited access rights
$\bigcirc$	Run Unlimited Grants unlimited access to the application above
$\bigcirc$	Block Stops execution of the application above
Trust th	is application

- If you are unsure of the safety of the software, then Comodo recommends that you run it with limited privileges and access to your system resources by clicking the 'Run Isolated' button. See Unknown Files: The Scanning process for more explanations on applications run with limited privileges.
- If you don't recognize the application then we recommend you select to 'Block' the application.

#### **Run with Elevated Privileges Alert**

The container will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.

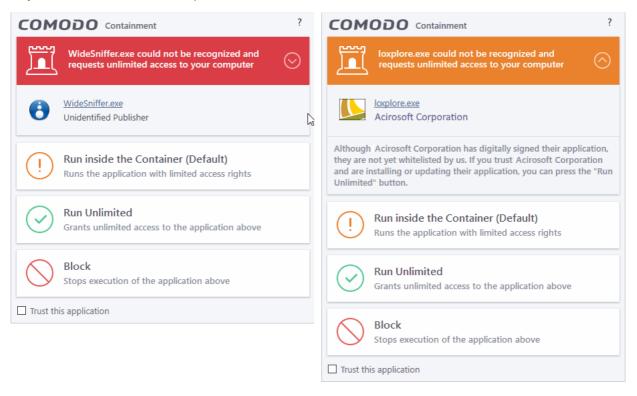
If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.

COMODO Creating Trust Online\*

- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted access to your system resources by clicking the 'Run Isolated' button.
- If this alert is unexpected then you should abort the installation by clicking the 'Block' button (for example, you have not proactively started to install an application and the executable does not belong to an updater program that you recognize)
- If you select 'Trust this application' then CCS will include this to Trusted Files list and no future alerts will be generated when you run the same application.

**Note**: You will see this type of alert only if you have enabled the 'Detect programs which require elevated privileges e.g. installers or updaters' option and disabled the 'Do not show privilege elevation alerts' option in containment settings. See **Containment Settings** for more details.

There are two versions of this alert - one for unknown installers that are not digitally signed and the second for unknown installers that are digitally signed but the publisher of the software has *not yet* been white-listed (they are not yet a 'Trusted Software Vendor').



#### Unknown and not digitally signed

### Unknown and digitally signed but the publisher not yet whitelisted (Not yet a 'Trusted Vendor')

- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

- 'Unknown Files: The Scanning Processes' to understand process behind how CCS scans files.
- 'Vendors List' for an explanation of digitally signed files and trusted software vendors.

#### **Containment Notification**

CCS shows a notification when it run an application inside the container. This usually happens if the application has an 'unknown' trust-rating.

COMODO Creating Trust Online\*



#### Application Contained

LogTable.exe has been Run Virtually COMODO Internet Security Premium

Hide These Alerts Don't Isolate It Again

- Hide These Alerts CCS will not show an alert if the same app is auto-contained in future.
- **Don't Isolate It Again** The application will not be auto-contained in future. An 'Ignore' rule is created for the application in auto-containment rules. See **Auto-Containment Rules** for more on this.

#### **Answer File Rating Alerts**

CCS checks a file's trust rating on our cloud severs as part of a real-time scan. The software can generate alerts when it finds a file with 'Malicious' rating.

You will see these alerts if you have *disabled* 'Do not show popup alerts' in 'Settings' > 'File Rating' > 'File Rating Settings'.

An example alert is shown below:

COMODO Rating	Scanner Alert ?
Policy.User@F0	ຼື 1
Location: C:\Su More information: Unav	ispicious\AntiTest\AntiTest.exe ailable
Quarantines the	
Ignore Ignores the alert	and allows the file operation $\checkmark$
	Show Activities

You can choose from these actions:

- Clean The program is blocked and quarantined
- **Ignore** Allows the file to run. Does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:

COMODO Creating Trust Online\*

(!)	Ignore Ignores the alert and allows the file operation	$\sim$
0	Ignore Once	
0	Ignore and Add to Exclusions	
0	Ignore and Report as False Alert	
	<u>Sh</u>	ow Activities

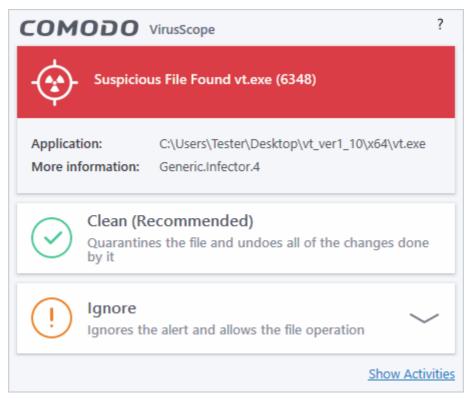
- **Ignore Once** The file is allowed to run this time, but it will still be flagged as a threat by future scans.
- Ignore and Add to Exclusions The file is allowed to run this time, and will not be flagged as
  a threat in future scans. The file is placed on the Exclusions list, meaning it is ignored
  permanently by the scanner.
- **Ignore and Report as a False Alert** The file is allowed to run this time, and submitted to Comodo for analysis. Select this option if you think the file is safe, and that CCS was wrong to flag it as a threat. Comodo will re-examine the file.

#### Answer a VirusScope Alert

Comodo Client Security generates a VirusScope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that VirusScope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a process has taken actions that you ought to review and confirm because they have the potential to be malicious. You can review all actions taken by clicking the 'Show Activities' link.

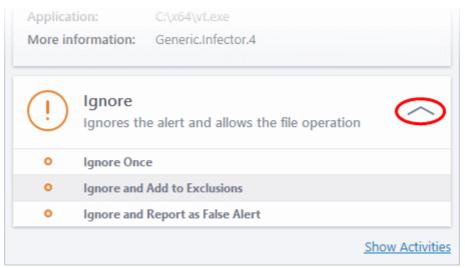
Please read the following advice before answering a VirusScope alert:

1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.



COMODO Creating Trust Online\*

- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking 'Ignore' and selecting the option from the drop-down.



- **Ignore Once** The process is allowed to run this time only. Another alert is shown if the process attempts to execute on future occasions.
- **Ignore and Add to Exclusions** The file is allowed to run and will not be contained in the future. See **Auto-Containment Rules** for help to configure which types of files should be auto-contained.
- **Ignore and Report as False Alert** Select this if you think the file is trustworthy and CCS is wrong to block it. CCS will submit the file to Comodo for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the Comodo safe list.
- Click the 'Show Activities' link to view the actions of the process:

COMODO Creating Trust Online\*

Application Activities	PID	Data	í				
📧 🗆 vt.exe	5576						
🖋 Load image file		C:\Windows\System32\guard64.dll					
📽 Load image file		C:\Windows\System32\imm32.dll					
🦸 Load image file		C:\Windows\System32\version.dll					
📽 Load image file		C:\Windows\System32\oleaut32.dll					
📽 Load image file		C:\Windows\System32\fltLib.dll					
📽 Load image file		C:\Windows\System32\cmdvrt64.dll					
🦸 Load image file		C:\Windows\System32\KernelBase.dll					
			~				

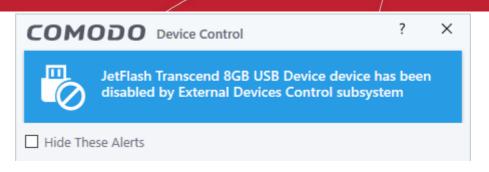
- Application Activities The action executed by each of the processes run by the parent application.
  - 📄 File actions: The process performed a file-system operation (create\modify\rename\delete file) which you might not be aware of.
  - E c Registry: The process performed a registry operation (created/modified a registry key) which might not be authorized.
  - Process: The process created a child process which you may not have authorized or have been aware of.
  - 🔜 Network: The process attempted to establish a network connection that you may not have been aware of.
  - If the process has been terminated, the activities will be indicated with gray text and will appear in the list until you view the 'Process Activities List' interface. If you close the interface and reopen the list within five minutes, the activities will appear in the list. Else, the terminated activities will not be shown in the list.
- PID The process identification number.
- Data The file affected by the action.

#### **Device Control Notifications**

These notifications are shown when you connect an external device to your computer (USB stick, external HDD etc). The alert indicates whether the device is allowed or blocked.

You can add blocked devices in 'Settings' > 'Advanced Protection' > 'Device Control'

COMODO



• See Device Control Settings to find out more.

### 1.7. Password Protection

- In a corporate setup, CCS settings are determined by the Endpoint Manager profile applied to the endpoint.
- One of these settings is the ability to password protect access to the client interfaces. This stops unauthorized users from opening the local clients and making potentially damaging changes.
- Password protection blocks access to the settings area, the various 'Tasks' areas, and the right-click
  options of the CCS tray icon.
- Local users can, however, still run certain tasks. See Exceptions at the end of this section for more details.

There are two password options you can set in Endpoint Manager:

- **Computer administrator** CCS requires a local admin password to access the settings area.
  - Admins that are already logged-in can access the settings area without a password.
  - All other users need to enter the admin username/password.
- Custom password An unique key which is set in the Endpoint Manager profile.
- See https://help.comodo.com/topic-399-1-786-11186-Client-Access-Control.html for details on the difference between these passwords.
- CCS will request a password if a user tries to access a protected area:

COMODO Enter password	?	×
Please enter your credentials in order to con	tinue:	
<ul> <li>Computer administrator (a Windows accordance) administrative privileges)</li> </ul>	ount with	
Domain:		
Login:		
Password:		
Remote access		
Password:		
ОК	CANCEL	

#### **Exceptions**

Users can run the following tasks even if password protection is enabled in the Endpoint Manager profile:

#### **On-demand antivirus scans**

- Click 'Scan' on the CCS home screen and choose a scan option.
- Click 'Tasks' > 'General Tasks' > 'Scan' > Choose a scan option.
- Right-click on an item and choose 'Scan with COMODO antivirus'.
- See Scan and Clean Your Computer and Instantly Scan Files and Folders for more details

#### Virus signature database updates

- Click Tasks > 'General Tasks' > 'Update'.
- See Manage Virus Database Updates for more details.

#### Manually run programs inside the container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'.
- Right-click on an item and choose 'Run in COMODO container'.
- See Run an Application in the Container for more details

#### **Run Virtual Desktop**

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'.
- See Start the Virtual Desktop for more details.

#### Create Comodo Rescue Disk

- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk'.
- See Create a Rescue Disk for more details.

# 2. General Tasks - Introduction

- Click 'Tasks' > 'General Tasks'
- The general tasks area lets you:
  - Quickly run antivirus scans
  - Update the virus database
  - View and manage items moved to quarantine
  - Manage blocked autorun items, Windows services and scheduled tasks.

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
< Home {୍ରି settings	
Secure   The virus signature database is NOT up	-to-date
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Scan Scan your computer for viruses and spyware.	View Quarantine View and manage threats quarantined by virus scanner.
Update Run the updater to check for program and virus database updates.	
Unblock Autoruns Re-enable previously blocked Windows services, auto-start items or scheduled tasks.	
K↓× SILENT MODE	3

See the following sections for help with each area:

- Scan and Clean your Computer
- Instantly Scan Files and Folders
- Process Infected Files
- Manage Virus Database Updates
- Manage Blocked Autoruns
- Manage Quarantined Items

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See 'Password Protection' for more details."

### 2.1. Scan and Clean Your Computer

- Click 'Tasks' > 'General Tasks' > 'Scan'
- CCS leverages multiple technologies, including real-time monitoring and on-demand scans, to keep endpoints totally free of malware
- You can schedule a scan to run at a specific time, and also create your own scan profiles to check specific files, folders and drives.

#### Run an on-demand virus scan

Click the 'Scan' tile on the CCS home screen

OR

• Click 'Tasks' > 'General Tasks' > 'Scan'

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
🗙 HOME {ତ୍ରି SETTINGS	
Secure   All systems are active and runn	ing
GENERAL TASKS FIREWALL TASKS CONTAINMEN	T TASKS ADVANCED TASKS
Scan Scan your computer for viruses and sp	view Quarantine View and manage threats quarantined by virus scanner.
Opdate Update	
	? ×
<b>Quick Scan</b> Scans commonly infecte	ed areas and memory.
Full Scan Scans all the files and fo	lders in the computer.
Quick Rating Scan Scans commonly infecte cloud for file reputation	ed areas and memory in the 24-05-2019
Scan files and folders or	run custom scan profiles.

- 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.

The following sections explain more about each scan type:

- Run a Quick Scan
- Run a Full Computer Scan
- Run a Rating Scan
- Run a Custom Scan
  - Scan a Folder
  - Scan a File

COMODO Creating Trust Online\*

#### Create Schedule and Run a Custom Scan

- Automatically Scan Unrecognized Files
- Instantly Scan Files and Folders
- Process Infected Files

•

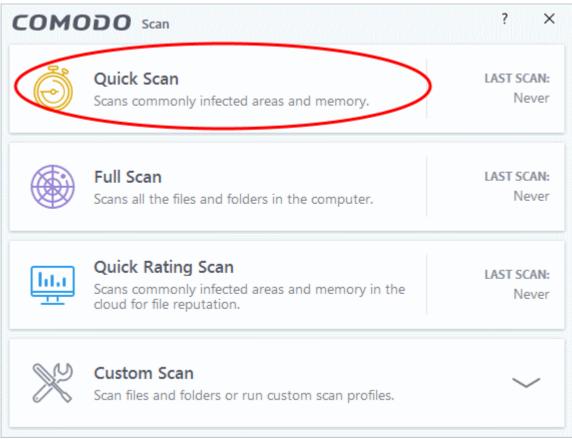
- Manage Blocked Autoruns
- Manage Quarantined Items

### 2.1.1. 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 Antivirus Configuration > Scan Profiles for help with this.

#### Run a Quick Scan

- Click the 'Scan' tile on the CCS home screen
- Select 'Quick Scan' from the 'Scan' interface



The scanner will start and first check whether your virus database is up-to-date:

COMODO Creating Trust Online\*

COMODO Scan		?			×
$\bigcirc$	TASK: Check for signature updates STATUS: Virus Database Update (5.0%): Checking for updates. ELAPSED TIME: 00:00:47				
THREAT(S) FOUND:	0 🛞 SKIPPED FILES: 0				
Threat Name	Threat Name				
Turn off this computer if no threats are found at the end of the scan					
🔳 STOP		SEND	TO BAC	KGROUN	ND

• The scans starts after any updates have been installed:

сомодо	Scan	?	-		×
65%	TASK: Quick Scan STATUS: C:\Windows\System32\rdpclip.exe ELAPSED TIME: 00:08:59				
THREAT(S) FOUN	D: 1 🕑 SKIPPED FILES: 0				
Threat Name					
C:\Windows\System3 Malware@#13tm1uk					
Turn off this com	nputer if no threats are found at the end of the scan				
STOP    PA	USE	SEND	ТО ВАС	KGROUI	ND

**Note** - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

COMODO Creating Trust Online\*

- You can pause, resume or stop the scan by clicking the appropriate button.
- Send to Background Runs the scan as a background process which consumes fewer resources. You can still keep track of the scan in the task manager 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.

Scan results are shown when the scan finishes:

	ican		?	-	
100%	TASK: Quick Scan STATUS: Scan Finished ELAPSED TIME: 00:13:11				
THREAT(S) FOUND	<b>D: 2</b>				
Threat Name	Q	Action	Clean		•
🗏 Malware@ (#13tm1	ukrdwdg0, #3fxg8e8df3its)				
– 📄 C:\Windows\	System32\poison2	🗸 Cle	an		•
C:\Windows\	System32\venom	🗸 Cle	an		-
CLOSE	puter if no threats are found at the end of the so	can	APPLY S	ELECTED	) ACTIONS

The results window contains two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.
- Skipped Files: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

**Note**: You will only see the drop-down menus if 'Automatically clean threats' is disabled for quick scans in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

### 2.1.2. 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.
  - Note You can change the settings of a quick scan in 'Settings' > 'Antivirus' > 'Scans'. See Antivirus Configuration > Scan Profiles for help with this.

#### Run a Full Computer Scan

• Click the 'Scan' tile on the CCS home screen

COMODO Creating Trust Online\*

<ul> <li>Select 'Full</li> </ul>	Scan':	
сомо	DDO Scan	? ×
Ö	Quick Scan Scans commonly infected areas and memory.	LAST SCAN: Never
	Full Scan Scans all the files and folders in the computer.	LAST SCAN: Never
<u>lıl.ı</u> 	Quick Rating Scan Scans commonly infected areas and memory in the cloud for file reputation.	LAST SCAN: Never
$\gg$	Custom Scan Scan files and folders or run custom scan profiles.	$\sim$

• The scanner will start and first check whether your virus database is up-to-date:

COMODO Scan		?	-		×
$\bigcirc$	TASK: Check for signature updates STATUS: Virus Database Update (5.0%): Checking for updates ELAPSED TIME: 00:00:47				
THREAT(S) FOUND:	0 🕑 SKIPPED FILES: 0				
Threat Name	Threat Name				
☐ Turn off this comp	uter if no threats are found at the end of the scan				
		SEND T	FO BAC	KGROUN	ND

COMODO Creating Trust Online\*

The scans starts after any updates have been installed:

COMODO Scan		?	_		×
$\bigcirc$	TASK: Full Scan STATUS: C:\Program Files\WindowsApps\king.com.CandyCrushFi ELAPSED TIME: 00:07:14	riends_1	I.13.5.0_x	86kgq1	/n
THREAT(S) FOUND:	0 🛞 SKIPPED FILES: 0				
Threat Name					
Turn off this computer if no threats are found at the end of the scan					
STOP    PAUS	E	SEND	TO BAC	KGROUN	ND

**Note** - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

- You can pause, resume or stop the scan by clicking the appropriate button.
- Send to Background Runs the scan as a background process which consumes fewer resources. You can still keep track of the scan in the task manager 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.

COMODO Send To Background	×			
What is a Background Task? A task which runs in the background without interfering your normal PC activities.	with			
Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.				
Please use Task Manager in order to access them later.				
Do not show this message again	ĸ			

- You can keep still track of scan progress in 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.
- Scan results are shown when the scan finishes:

COMODO Creating Trust Online\*

	can		7	? —		×
100%	TASK: Full Scan STATUS: Scan Finished ELAPSED TIME: 03:03:06					
THREAT(S) FOUND	0:8 🕑 SKIPPED FILES: 18					
Threat Name	Q	Action	Clean		•	^
🗏 Malware@ (#vigyao	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hr					
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
Turn off this computer if no threats are found at the end of the scan						
CLOSE			APPL	Y SELECTE	D ACTIO	ONS

The results window contains two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.

**Note**: You will only see the drop-down menus if 'Automatically clean threats' is disabled for full scans in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

• **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

Creating Trust Online\*

	can	?	_		×	
100%	TASK: Full Scan STATUS: Scan Finished ELAPSED TIME: 03:03:06					
THREAT(S) FOUND	8 SKIPPED FILES: 18					
Path					^	
C:\Share\Firefox Setup	13.0.1.exe					
C:\Share\Firefox Setup	C:\Share\Firefox Setup 13.0.1.exe					
C:\Share\em_iSTjHX5f_installer.msi						
C:\Share\em_iSTjHX5f_	C:\Share\em_iSTjHX5f_installer.msi					
C:\Share\Paint.NET.3.5.10.Install.exe						
C:\Share\Paint.NET.3.5.10.Install.exe						
C:\Share\Paint.NET.3.5.10.Install.exe						
C:\Share\paint.net.4.1.	5.install.exe				~	
Turn off this com	puter if no threats are found at the end of the scan					
CLOSE		APPLY S	SELECTED		NS	

### 2.1.3. Run a Rating Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Rating Scan'
- A rating scan checks the trust-rating of 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 immediately 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 Rating scan

- Click the 'Scan' tile on the CCS home screen (click here for alternative ways to open the scan interface)
- Select 'Ratings Scan':

COMODO Creating Trust Online\*

COMODO Scan		? ×
õ	Quick Scan Scans commonly infected areas and memory.	LAST SCAN: 10/10/2018
	Full Scan Scans all the files and folders in the computer.	<b>LAST SCAN:</b> 10/10/2018
<u>      </u>	Quick Rating Scan Scans commonly infected areas and memory in the cloud for file reputation.	<b>LAST SCAN:</b> 10/10/2018
$\gg$	Custom Scan Scan files and folders or run custom scan profiles.	$\sim$

CCS will analyze all files on your computer and assign them a trust rating. File ratings are shown in the results table at the end of the scan:

COMODO Creating Trust Online\*

COMODO Quick Rating Scan					?	-		×
TRUST LEVEL:       Trusted File         99.72%       Unrecogni         Malicious I	zed Files: 3		🔅 Aut	ning Files orun Files: rage File A	: 483	month	s	
SHOW All Files								
File Name Q	Rating	Age	Autorun	Action	No A	Action	•	1
shell32.dll	🗸 Trusted	1 day	ø					
Narrator.exe	✓ Trusted	12 months	•					
duartz.dll	🗸 Trusted	2 months	•					
I rdpclip.exe	✓ Trusted	2 months	•					
Cofiredm.dll	✓ Trusted	12 months	•					
userinit.exe	✓ Trusted	12 months	٥					
Turn off this computer if no threats	are found at t	he end of the	e scan					
CLOSE				АРР	LY SEL	ECTED	ΑCTIO	NS

	Rating Scan Results Table - Column Descriptions
Column Header	Description
File Name	The label of the scanned item
Rating	<ul> <li>The trust level of the file as per the cloud based analysis. The possible values are:</li> <li>Trusted</li> <li>Unrecognized</li> <li>Malicious</li> </ul>
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	Select how you want to deal with the listed item. See the explanations given below:

The drop-down menus on the right let you handle unrecognized and malicious items:

COMODO

SHOW Malicious Files					
File Name	Q	Rating	Age	Autorun	Action No Action 💌
mshta.exe		(!) Malici	12 months		Clean Clean No Action Trust

- 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. See Manage Quarantined Items for more details.
- **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 **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.
- CCS logs all actions taken in the results screen. You can view the logs at 'Tasks' > 'Advanced Tasks' > 'View Logs'. See File List Changes Logs for more details.
- Use the drop-down in the 'Action' column header to apply your choice to all listed files:

ile Name Q	Rating	Age Aut	orun Action	Clean	•
mshta.exe	() Malici	12 months	Clean	Clean 🔥 No Action	
AlterHostsFile.exe	() Malici	1 month	Clean	Trust	
📧 <u>cpil.exe</u>	() Malici	4 months	Clean		•
CPIL2.dll	() Malici	4 months	Clean	•	•
CPIL3.dll	() Malici	4 months	Clean		•
mshta.exe	() Malici	12 months	Clean		•

### 2.1.4. 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

COMODO

- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan':

сомо	DDO Scan	? ×
Ö	Quick Scan Scans commonly infected areas and memory.	LAST SCAN: 03-05-2019
R	Custom Scan Scan files and folders or ruthcustom scan profiles.	
	Folder Scan Select and scan a folder.	
	File Scan Select and scan a file.	
	More Scan Options Run custom scan profiles.	

You now have the following options:

- Folder Scan scan individual folders
- File Scan scan an individual file
- More Scan Options create a custom scan profile

### 2.1.4.1. Scan a Folder

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'Folder Scan'
- Folder scans let you check specific folders on your hard drive, CD/DVD, or external device.

Tip: Alternatively, simply right-click on a folder then select 'Scan with COMODO Antivirus'.

#### Scan a specific folder

- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan' > 'Folder Scan'
- Browse to the folder you want to check then click 'OK':

COMODO Creating Trust Online\*

COMODO Scan	? ×
Quick Scan Scans commonly infected areas and memory.	LAST SCAN: 03-05-2019
Custom Scan Scan files and folders or run custom scan profiles.	^
Folder Scan Select and scan a folder Ne Scan Browse For Folder × Videos Local Disk (C:) Astrolog Bistone Sistone Sistone SicClS Federal Bank Statements Old Man Apps Sid Man Apps	
Make New Folder OK Cancel	

• The CCS starts scanning the items in the folder.

**Note** - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

• Scan results are shown when the scan finishes:

Creating Trust Online\*

	can			?	—		×
100%	TASK: C:\Old Man Apps STATUS: Scan Finished ELAPSED TIME: 00:04:33						
THREAT(S) FOUND	e: 1 🛞 SKIPPED FILES: 0						
Threat Name	Q	Action	Clean			•	
🗏 🗋 C:\Old Man App	s\uTorrent.exe	Cl	ean			•	
Malware@#brsxp	pal1o5hg						
C:\Old Man Apps	s\uTorrent.exe Unsfx WizardPages.dll						
Turn off this com	puter if no threats are found at the end of the s	can					
CLOSE			API	PLY S	ELECTE	D ACTIO	NS

The results window has two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

### 2.1.4.2. Scan a File

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'File Scan'
- File scans let you check specific files on your hard drive, CD/DVD, or external device.
- For example, you might have downloaded a file from the internet which you want to scan before running.

Tip: Alternatively, right-click on file then select 'Scan with COMODO Antivirus'.

#### Scan a specific file

- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan' > 'File Scan'
- Browse to the file you want to scan and click 'Open'.

COMODO Creating Trust Online\*

сомо	DO Scan		? ×
(	Quick Scan Scans commonly infected areas and memory.		LAST SCAN: 03-05-2019
N6	Custom Scan Scan files and folders or run custom scan pro	files.	^
	Folder Scan Select and scan a folder.		
	File Scan Select and scatha file.		
	More Scan Options		
🖾 Open			×
Look ir	n: poison1 ~	G 🤌 📂 🖽	•
Quick access	Name 🗍 hazard.bin	Date modified 26-05-2017 10:54	Type BIN File
Desktop Libraries			
This PC			
Network	κ		>
	File name: hazard	~	Open
	Files of type: All Files (*.*)	~	Cancel

**Note** - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed in 'Full Scan' profile. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

• Scan results are shown when the scan finishes:

Creating Trust Online\*

	can	?	—		×
100%	TASK: C:\Old Man Apps\poison1\hazard.bin STATUS: Scan Finished ELAPSED TIME: 00:00:07				
THREAT(S) FOUND	:1 🕑 SKIPPED FILES: 0				
Threat Name	Q Action C	lean		•	
Malware@#3fxg8e8	df3its				
C:\Old Man A	Apps\poison1\hazard.bin			•	
Turn off this comp	puter if no threats are found at the end of the scan				
CLOSE		APPLY S	ELECTED	Ο ΑCTIO	NS

The results window has two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

### 2.1.4.3. Create, Schedule and Run a Custom Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'
- A custom scan profile lets you configure your own scan with your own 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
  - See the following for more help:
    - Create a Scan Profile
    - Run a custom scan

#### Create a custom profile

- Click the 'Scan' tile on the CCS home screen
- 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:

COMODO Creating Trust Online\*

õ	Quick Scan Scans commonly i	nfected area	s and memo	ry.	LAST SCAN: 29-05-2019
×	Custom Scan Scan files and fold	o provacio provacio p			
	Folder Scan Select and scan a	folder.			
	File Scan Select and scan a	file.			
····	More Scan Optio Run custom scan		)		>
00000	dvanced Settings	•	/	3	
<ul> <li>General Settings</li> </ul>	Scans				
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> <li>Scans</li> </ul>	Scans This page allor	1	×	nd edit scan profiles	and scheduled scans
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> <li>Scans</li> <li>Firewall</li> </ul>	Scans This page allo	<b>L</b> Edit		nd edit scan profiles Last Scan	and scheduled scans
<ul> <li>General Settings</li> <li>Antivirus         <ul> <li>Realtime Scan</li> <li>Scans</li> </ul> </li> <li>Firewall</li> <li>HIPS</li> </ul>	Scans This page allow	Edit	<b>X</b> Remove		
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> <li>Scans</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> </ul>	Scans This page allow Add	Edit	* Remove Action	Last Scan	Status
<ul> <li>General Settings</li> <li>Antivirus         <ul> <li>Realtime Scan</li> <li>Scans</li> </ul> </li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> </ul>	Scans This page allow Add Name Full Sc Quick	Edit	Remove Action Scan	Last Scan Never	Status

• Click 'Add' to create a new custom scan profile.

Creating Trust Online\*

сомо	<b>DO</b> Scan					?		×
Scan Name:	Old man do	ocuments						
Define items	to be scanned	d, scanning op	tions and run	ning schedule				
ITEMS	OPTIONS	SCHEDULE						
C.	<b>₽</b> ⊋	8	×					
Add Files		Add Area	Remove					
Pro Pro	file							
					ок	C	ANCEL	

First, create a name for the profile. The next steps are:

- Select items to scan
- Configure scan options for the profile (optional)
- Configure a scan schedule (optional)

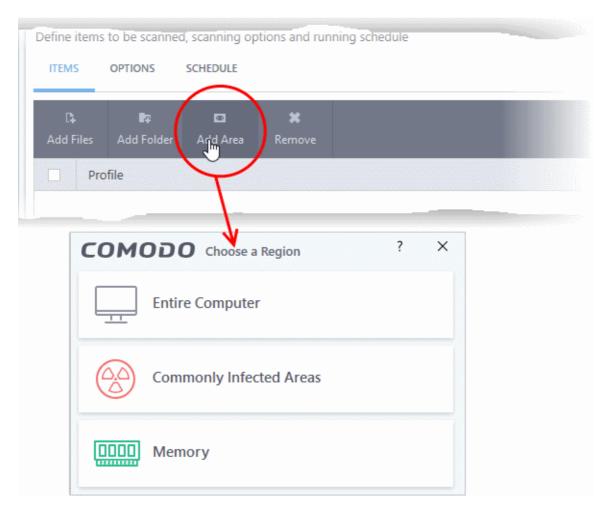
#### Select items to scan

• 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' and 'System Memory'. See screenshot below:

COMODO Creating Trust Online\*



Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

### **Configure Scan Options**

Click 'Options' at the top of the scan interface

COMODO Creating Trust Online\*

.0110	DO Scan ?
can Name:	
Define items	to be scanned, scanning options and running schedule
ITEMS	OPTIONS SCHEDULE
🗹 Decomp	ress and scan compressed files
This optic	on allows scanner to decompress archive files e.gzip, .rar, etc. during scanning
Use clou	d while scanning
This optic	on allows scanner to connect to cloud to query file ratings
Automat	ically clean threats Quarantine Threats
When the	e threats are identified, perform the selected action automatically
Show sca	an results window
	on enables to view results of scans launched as per schedule or from the management portal, as well as le media scans.
🗹 Use heur	istics scanning Low 🔻
Use the s	elected level of sensitivity while scanning heuristically
🗹 Limit ma	ximum file size to 40 MB
While sca	nning, if a file size is larger than specified, it is not scanned
Run this	scan with Background 🔻
Priority of	f scanner determines how much of the computer resources are used among other tasks
🗹 Update v	virus database before running
This optic	on makes sure the database is updated before running the scan
Detect p	otentially unwanted applications
Potentiall download	y unwanted applications are programs that are unwanted despite the possibility that users consented to I them.
Apply thi	is action to suspicious autorun processes Terminate and Disable 💌
	ted action will be automatically applied if unrecognized Windows services, autostart entries or d tasks are detected.
Limit scan t	ime of a single file to 9 🖨 min(s)
When the	e set time limit is reached, the file will be skipped and antivirus will proceed scanning other files.
	OK CANCEL

- **Decompress and scan compressed files** The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (*Default = Enabled*).
- Use cloud while scanning Improves accuracy by augmenting the local scan with an online lookup of Comodo's latest virus database. This means CCS can detect the latest malware even if your virus database is out-dated. (*Default = Disabled*).
- Automatically clean threats Select whether or not CCS should automatically remove any malware found by the scan. (*Default = Enabled*).

- Disabled = Results are shown at the end of the scan with a list of any identified threats. You
  can manually deal with each threat in the results screen. See Process Infected Files for
  guidance on manually handling detected threats.
- **Enabled** = Threats are handled automatically. Choose the action that CCS should automatically take:
  - Quarantine Threats Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See 'Manage Quarantined Items' for more details.
  - Disinfect Threats If a disinfection routine exists, CCS will remove the virus and keep the original file. If not, the file will be quarantined. (*Default*)
- Show scan results window You will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.
- Use heuristic scanning Select whether or not heuristic techniques should be used in scans on this profile. You can also set the heuristic sensitivity level. (*Default = Enabled*).

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

If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

• Low - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (Default)

- **Medium** Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- High Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.
- Limit maximum file size to Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (*Default = 40 MB*).
- Run this scan with If enabled, you can set the priority of scans on this profile The available
  options are:
  - High
  - Normal
  - Low
  - Background
  - Disabled = The scan will be run in the background (Default)
- Update virus database before running CCS checks for and downloads the latest virus signatures before starting a scan. (*Default = Enabled*).
- Detect potentially unwanted applications The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility 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 your activity on the internet. (Default = Enabled).
- Apply this action to suspicious autorun processes Specify how CCS should handle unrecognized auto-run items, Windows services and scheduled tasks.
  - Ignore The item is allowed to run (Default)
  - Terminate CCS stops the process / service

COMODO Creating Trust Online\*

- **Terminate and Disable** Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- **Quarantine and Disable** Auto-run processes are quarantined and the corresponding autorun entry removed. In the case of a service, CCS disables the service.

Note 1 - This setting only protects the registry during the on-demand scan itself. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

See Miscellaneous Settings for more details

Note 2 - CCS runs script analysis on certain applications to protect their registry records. You can manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See 'Autorun Scans' in Script Analysis Settings for more details
- **Limit scan time of a single file to** Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

#### Schedule the scan

• Click 'Schedule' at the top of the 'Scan' interface.

COMODO Scan	?		×
Scan Name:			
Define items to be scanned, scanning options and running schedule			
ITEMS OPTIONS SCHEDULE			
Frequency:			^
O not schedule this task			
O Every few hours			
O Every Day			
O Every Week			
O Every Month			
Additional Options			
Run only when computer is not running on battery			
Run only when computer is IDLE			
Turn off computer if no threats are found at the end of the scan			
Run during Windows Automatic Maintenance			~
ОК	c	ANCEL	

- **Do not schedule this task** The scan profile is created but not run automatically. The profile will be available for on-demand scans.
- Every few hours Run the scan at the frequency set in 'Repeat scan every NN hour(s)'
- Every Day Run the scan every day at the time specified in the 'Start Time' field.

- Every Week Run the scan on the days specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- Every Month Run the scan on the dates specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery** The scan only runs when the computer is plugged into the power supply. This is useful when you are using a laptop or other mobile device.
- Run only when computer is IDLE The scan only runs if the computer is in an idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- Turn off computer if no threats are found at the end of the scan Will turn off your computer if
  no threats are found during the scan. This is useful when you are scheduling scans to run at
  nights.
- Run during Windows Automatic Maintenance Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.

The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See **Automatically Clean Threats**.

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

• Click 'OK' to save the profile.

The profile will be available for deployment in future.

#### Run a custom scan

- Click 'Tasks' > 'General Tasks' > 'Scan'
- Click 'Custom Scan' from the 'Scans' interface
- Click 'More Scan Options' from the 'Custom Scan' pane

The 'Advanced Settings' interface will open at the 'Scans' panel.

• Click 'Scan' beside the required scan profile.

COMODO Creating Trust Online

COMODO Advance	ed Settings		?	- 🗆 X
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> </ul>	Scans This page allows you to add, remo	ove and edit sc	an profiles and schedu	led scans.
Scans	+ 2 ×			
✓ Firewall	Add Edit Remov	e		
✓ HIPS	Name	Action	Last Scan	Status
✓ Containment	Full Scan	Scan	Never	
✓ File Rating	Quick Scan	Scan	6/11/2019 11:52:5	9 AM 💽
✓ Advanced Protection	Shared Folder Scan	Scan	Never	
			ок	CANCEL

The scan will start immediately. Results are displayed afterwards:

COMODO Creating Trust Online\*

	can		?	_		×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48					
THREAT(S) FOUND	SKIPPED FILES: 24					
Threat Name	Q	Action	Clean		•	^
🗏 Malware@ (#vigyao	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hr					
– 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
C:\Share\Ma	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	J
Turn off this complete the second	puter if no threats are found at the end of the	scan				111
CLOSE			APPLY	SELECTED	Ο ΑCTIO	NS

The results window contains two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.

**Note**: You will only see the drop-down menus if 'Automatically clean threats' is disabled for the selected scan profile in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

 Skipped Files: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (*default = 9 mins*).

Creating Trust Online\*

	ican	?	_		×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48				
THREAT(S) FOUND	D: 8 🕑 SKIPPED FILES: 24				
Path					^
C:\Share\Firefox Setup	13.0.1.exe				
C:\Share\Firefox Setup	13.0.1.exe				
C:\Share\icedragonset	up.exe				
C:\Share\icedragonset	up.exe				
C:\Share\Firefox Setup	13.0.1.exe				
C:\Share\Paint.NET.3.5	.10.Install.exe				
C:\Share\Paint.NET.3.5	.10.Install.exe				
C:\Share\Paint.NET.3.5	.10.Install.exe				~
Turn off this com	puter if no threats are found at the end of the scan				
CLOSE		APPLY	SELECTE	Ο ΑCTIO	NS

### 2.1.5. Automatically Scan Unrecognized and Quarantined Files

- Click 'Settings' > 'File Rating' > 'File Rating Settings'
- CCS can periodically re-scan unknown and quarantined files to check whether a new trust rating is available for them.
- This area lets you specify a schedule and settings for these scans.

### File Rating

- CCS checks files when they are run and rates them as 'trusted', 'malicious' or 'unrecognized'.
- The rating is obtained by checking the file's reputation on our master whitelist and blacklist
- If no file rating is available then CCS checks the trust rating of the software vendor
  - CCS will apply the vendor reputation to the file if one exists. CCS first checks the vendor's local reputation in the 'Vendor List'. If no local rating is available then it checks the file lookup service.
- There are two ways a file can get an 'unrecognized' rating:
  - 1. Because there is no rating for the file on Comodo's black or whitelists, and no user has assigned a malicious/trusted rating to the file.

OR

2. Because an admin, user or Comodo specifically assigned an 'unrecognized' rating to the file.

To view the rating:

- Go to 'Settings' > 'File Rating' > 'File List' > select an unrecognized file > Click 'File Details'
- Click the 'File Rating' tab

The following examples show files with and without ratings:

<ul> <li>Unknown files with no i gray ? Icon.</li> </ul>	ating are shown with a	<ul><li>Yellow - Unreco</li><li>Green - Trusted</li></ul>	•
OMODO File Details	? ×	Red - Malicious	
OVERVIEW	FILE RATING	COMODO File Details	?
Final Rating:	Unrecognized	OVERVIEW	FILE RATING
Provider Date	File Rating	Final Rating:	Unrecognized
Administrator	? Unrecognized	Provider Date	File Rating
User	? Rate Now	Administrator	? Unrecognized
Comodo	? Unrecognized	User	? Rate Now
		Comodo Valkyrie 10/10/2018 8	23:09 PM ? Unrecognized
	OK CANCEL		

CCS will handle unrecognized files differently depending on whether the rating was proactively applied or not:

- Files awarded an unrecognized rating by admin, user or Comodo are not uploaded to Valkyrie.
- All other unrecognized files are uploaded to Valkyrie when executed or discovered by a rating scan. You can also submit them manually.

Regardless of the above, all unrecognized files are run in the container by default. If required, you can change autocontainment rules in 'Settings' > 'Containment' > 'Auto-Containment'. See 'Auto-Containment Rules' for more information.

### **Quarantined Files**

- The antivirus scanner moves threats to quarantine to prevent them from infecting your system.
- All files in quarantine are encrypted, so they cannot run or cause harm.
- You can also manually move suspicious items to quarantine. See Manage Quarantined Items for more details.

### Configure scan settings for unrecognized and quarantined files

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Rating Settings'

COMODO Creating Trust Online\*

COMODO Advanced	Settings ? - □ ×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	File Rating Settings
<ul> <li>✓ Firewall</li> </ul>	Enable Cloud Lookup (Recommended)
✓ HIPS	<ul> <li>Analyze unknown files in the cloud by uploading them for instant analysis (Privacy Policy)</li> </ul>
✓ Containment	☑ Upload metadata of unknown files to the cloud
- File Rating	☑ Do not show popup alerts
File Rating Settings File Groups Submitted Files ✓ Advanced Protection	<ul> <li>This option, when enabled, automatically terminates and quarantines malware detected by rating scan.</li> <li>Rate applications according to their vendor rating</li> <li>Trust files installed by trusted installers</li> <li>Detect potentially unwanted applications</li> <li>Automatically purge the file list from invalid records every 4 hour(s)</li> <li>The file list will be cleaned from records on files no longer existing on this computer. It will not affect records on quarantined files and files rated by administrators.</li> <li>Use proxy when performing cloud lookup</li> </ul>
	Automatically scan unrecognized files and re-evaluate quarantined files at equal intervals Edit scan options OK CANCEL

- Automatically scan unrecognized files and re-evaluate quarantined files at equal intervals Activate periodic re-scans of unrecognized and quarantined files. CCS will check whether new trust ratings are available for the files on Comodo's master black and white lists. (*Default = Enabled and set for every 4 hours*)
- · Click 'Edit scan options' to open the predefined 'Unrecognized File Scanning' profile

? COMODO Scan × Scan Name: Unrecognized and Quarantined Files Scanning Define items to be scanned, scanning options and running schedule OPTIONS ITEMS SCHEDULE Profile Unrecognized Files Quarantined Files ОК CANCEL

- Scan Name The label of the scan. This is pre-configured and cannot be edited.
- **Items** The files that are scanned by the profile. 'Unrecognized' and 'Quarantined' files are the defaults. You cannot edit or add files to this profile.
- Scan Options Configure scan technolgies, how to handle threats, and more. See Configure scan options for the profile in the previous section for help with this.
- Schedule Specify the frequency of the automated scans. See Configure a scan schedule in the previous section for help with this. (*Default = Every 4 hours*).
- Click 'OK' to save your changes
- · Click 'OK' in the 'Advanced Settings' screen for your settings to take effect.

### 2.2. Instantly Scan Files and Folders

- You can scan individual files, folders or drives to instantly to check whether they contain threats.
- For example, 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 the item and select 'Scan with Comodo Antivirus' from the menu:

na Trust Online

COMODO Creating Trust Online\*

File Home Share View     File Home Share View     Pin to Quick Copy Paste   Paste Paste shortcut     Organize New   Clipboard Organize   Name Date modified     Type   Quick access   Desktop   Documents   Pictures     Pictures     Scan with COMODO antivirus   Ruo in COMODO container   Share   Restore previous versions   Send to   Cut   Copy   Create shortcut   Delete   Rename   Properties	/		
Pin to Quick Copy   Paste Copy path   Paste Paste   Paste Paste   Poperties Properties   Properties Proper	📙   🛃 📙 🖛   poison1		
Pin to Quick Copy Paste Paste shortcut Clipboard Cryanize Copy or Paste Properties Pro	File Home Share View		
Name Date modified Type   Desktop Image: hazard.bin 26-05-2017 10:54 BIN   Downloads Image: hazard.bin Open with   T-Zip Image: hazard.bin CRC SHA   Pictures Image: hazard.bin CRC SHA   Pictures Image: hazard.bin CMODO antivirus   Pictures Image: hazard.bin CMODO container   Image: hazard.bin Conton Container   Image: hazard.bin Conton Container   Image: hazard.bin Cut   Copy Create shortcut   Delete Rename	Pin to Quick Copy Paste access Paste Rest	h ortcut 🕒 Copy to 👻 📑 Rena	ame New Properties
<ul> <li>✓ Quick access</li> <li>✓ Desktop</li> <li>✓ Downloads</li> <li>✓ Documents</li> <li>✓ Pictures</li> <li>✓ Scan with COMODO antivirus</li> <li>✓ Run in COMODO container</li> <li>✓ Share</li> <li>Restore previous versions</li> <li>✓ Send to</li> <li>✓ Cut</li> <li>✓ Copy</li> <li>✓ Create shortcut</li> <li>✓ Delete</li> <li>Rename</li> </ul>	← → × ↑ 🔄 > This PC > Loc	al Disk (C:) > Suspicious > po	oison1 ∨ Ö Searc
<ul> <li>Desktop</li> <li>Downloads</li> <li>Pocuments</li> <li>Pictures</li> <li>CRC SHA</li> <li>CRC SHA</li> <li>CRC SHA</li> <li>CRC SHA</li> <li>Scan with COMODO antivirus</li> <li>Run in COMODO container</li> <li>E<sup>2</sup> Share</li> <li>Restore previous versions</li> <li>Send to</li> <li>Cut</li> <li>Copy</li> <li>Create shortcut</li> <li>Delete</li> <li>Rename</li> </ul>		^	Date modified Type
<ul> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> <li>CRC SHA</li> <li>CRC SHA</li> <li>CRC SHA</li> <li>Scan with COMODO antivirus</li> <li>Run in COMODO container</li> <li>Share</li> <li>Restore previous versions</li> <li>Send to</li> <li>Cut</li> <li>Copy</li> <li>Create shortcut</li> <li>Delete</li> <li>Rename</li> </ul>	hazar	d.bin	26-05-2017 10:54 BIN
Image: Scan with COMODO antivirus         Image: Run in COMODO container         Image: Share         Restore previous versions         Send to         Cut         Copy         Create shortcut         Delete         Rename	🕂 Downloads 🚿	7-Zip	>
Restore previous versions         Send to       >         Cut		-	
Cut Copy Create shortcut Delete Rename			
Copy Create shortcut Delete Rename		Send to	>
Delete Rename			
Properties		Rename	
		Properties	

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.

Click 'Settings' > 'Antivirus' > 'Scans', then open the 'Full Scan' profile to view these thresholds.

• Scan results are shown when the scan finishes:

Creating Trust Online\*

	can			?	—		×
100%	TASK: C:\Old Man Apps\poison1\hazard.bin STATUS: Scan Finished ELAPSED TIME: 00:00:07						
THREAT(S) FOUND	: 1 🕑 SKIPPED FILES: 0						
Threat Name	۵	Action	Clean			T	
Malware@#3fxg8e8	df3its						
C:\Old Man A	pps\poison1\hazard.bin	🗸 Cle	an			•	
Turn off this computer if no threats are found at the end of the scan							
CLOSE			AP	PLY SI	ELECTED	Ο ΑCTIO	NS

The results window has two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (*default = 9 mins*).

### 2.3. Process Infected Files

The results screen at the end of a scan lets you clean, quarantine or ignore any detected threats. The screen contains two tabs:

- **Threats Found**: Number of malicious items discovered by the scan. You can clean, quarantine or ignore the threats.
- Skipped Files: Files that were omitted because they took longer to scan than the time limit.

### View identified threats and take actions

• Click the 'Threats Found' tab (if it is not already open)

COMODO Creating Trust Online\*

	can		?	_		×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48					
THREAT(S) FOUND	8 SKIPPED FILES: 24					
Threat Name	Q	Action	Clean		•	^
🗏 Malware@ (#vigyao	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hr					
– 🗋 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		T	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		T	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
Turn off this comp	puter if no threats are found at the end of the	scan				
CLOSE			APPLY	SELECTE	D ACTIO	NS

• Use the drop-down menus to apply actions to individual files:

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

Creating Trust Online\*

	can		?	— C	) ×
100%	TASK: Share Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:06				
THREAT(S) FOUND	: 8 🕑 SKIPPED FILES: 18				
Threat Name		Q Action	Clean		Â
🗏 Malware@ (#vigyaol	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hi	·			
— 🗋 C:\Share\Malv	ware-Samples-master\Malware-Samples-mas	t Cle	ean	•	
— 🗋 C:\Share\Malv	ware-Samples-master\Malware-Samples-mas	it → Igr	ean 🔓		
C:\Share\Malv	ware-Samples-master\Malware-Samples-mas	and the second second	d to Trusted Files		
		-	eport as a False A dd to Exclusions	lert	

• Or use the 'Action' drop-down at top-right to apply your choice to all threats at once.

	can		?	-		×
100%	TASK: Share Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:06					
	9:8 🛞 SKIPPED FILES: 18					
Threat Name	Q	Action	Clean		•	^
Alware@ (#vigvag			Clean			
inalware@ (#vigyaokin/gw, #jgitomojxnivk, #sbquivsosiryi, #zin			Ignore Once			
- C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	Add to Trusted	Files		
			Report as a Fal	se Alert		
			Add to Exclusion	ons		

Available actions are:

- **Clean** The virus is removed from the file if a disinfection routine is available. The cleaned file is left in its original location. If no routine exists, the file is quarantined. Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine' to view this area. You can restore or permanently delete files from quarantine as required. See Manage Quarantined Items for more details.
- Ignore Once Allows the file to run this time only. The file will still get flagged as a threat by future antivirus scans.
- Add to Trusted Files Creates an exception for the file by giving it a 'Trusted' rating in the File
  List ('Settings' > 'File Rating' > 'File List'). The AV scanner will not detect the file as a threat in
  future scans. Only select this option if you are sure the file is trustworthy.

COMODO Creating Trust Online\*

# Comodo Client Security - User Guide

- **Report as a False Alert** Sends the file to Comodo for further analysis. Submitting a false positive will also add the item to trusted files, so it won't get flagged by future scans. The file will be added to the global whitelist if Comodo confirms the false-positive
- Add to Exclusions Creates an exception for the file so it won't get flagged by future virus scans. You can review exclusions at 'Settings > 'Advanced Protection' > 'Scan Exclusions'. The file's trust rating does not change.
- Click 'Apply Selected Actions'. The result is shown in the 'Actions' column:

	can			?	-		×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48						
THREAT(S) FOUND	SKIPPED FILES: 24						
Threat Name	Q	Action	Clean			¥	^
ApplicUnwnt@#2bz	zoprs4rq6r6						
C:\Share\Wo	orkingTimeManagerSetup.exe	Cleaned	d				
🗏 Malware@ (#vigyao	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hrwdh						
— 🗸 C:\Share\Ma	alware-Samples-master\Malware-Samples-master\	. Cleaned	d				
— 🗸 C:\Share\Ma	alware-Samples-master\Malware-Samples-master\	. Cleaned	d				
— 🗸 C:\Share\Ma	alware-Samples-master\Malware-Samples-master\	. Cleaned	d				
— 🗸 C:\Share\Ma	alware-Samples-master\Malware-Samples-master\	. Cleaned	d				
<							> ~
Turn off this com	puter if no threats are found at the end of the s	can					
CLOSE			AP	PLY SE	LECTED	ACTIO	NS

### View skipped files

Click the 'Skipped Files' tab

Creating Trust Online\*

	ican	?			×
100%	TASK: Share Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:06				
THREAT(S) FOUND	D: 8 🕑 SKIPPED FILES: 18				
Path					^
C:\Share\patch_manag	gement_agent.msi				
C:\Share\TeamViewer_	Setup.exe				
C:\Share\TeamViewer_	Setup.exe				
C:\Share\TeamViewer_	Setup.exe				
C:\Share\Silverlight.ex	e				
C:\Share\Silverlight.ex	e				
C:\Share\Silverlight.ex	e				
C:\Share\Silverlight.ex	e				~
□ Turn off this com	puter if no threats are found at the end of the scan				
CLOSE		APPLY S	ELECTED	ACTION	NS

The 'Skipped Files' tab shows files that were omitted from the scan. These files took longer than the max. time allowed to scan a single file. The max. time allowed depends on the profile used for the scan. To view the max. scan time

- Click 'Settings' > 'Antivirus' > 'Scans'
- Open the profile used by the scan
- View/edit the max. scan time as required.

**Note** - The skipped files tab does not show excluded files, or files that were skipped because they exceeded the maximum file size. It only shows files skipped because they exceeded the max. scan time.

### 2.4. Manage Virus Database Updates

• Click 'Tasks' > 'General Tasks' > 'Update'

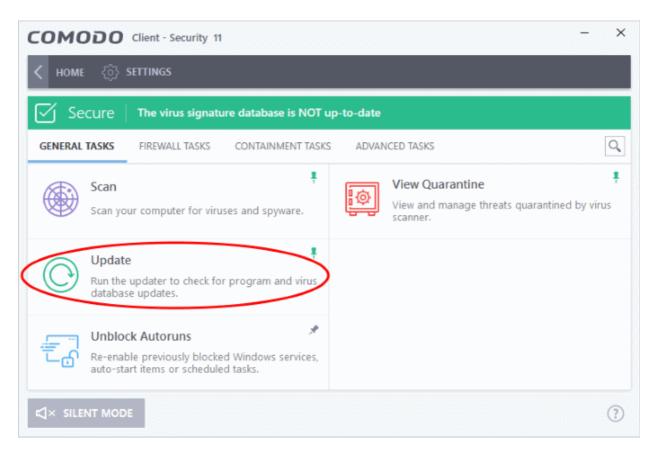
In order to guarantee continued and effective antivirus protection, it is imperative that your virus database is kept up to date. Updates can be downloaded **manually** or **automatically** 

Prerequisite - You must be connected to the internet to download updates.

### Manually check for the latest virus and program updates

COMODO Creating Trust Online\*

- Click 'Tasks' > 'General Tasks'
- Click the 'Update' tile:



Signature updates are downloaded first if they are available:

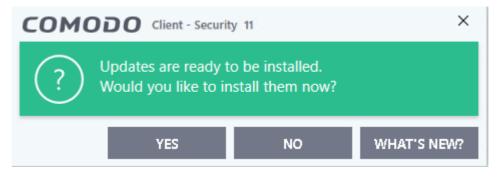
соморо	Update	?	—		×
18%	TASK: Install signatures STATUS: Finalizing				
TASK		STATUS			
Check for sign	nature updates	Completed			
Oownload sig	natures	Completed			
Install signat	ures	In Progress (90.0	%)		
				<u>View L</u>	.ogs
PAUSE STO	P	SEND T	ГО ВАСК	GROUN	ID

The updater then checks for web filter, VirusScope, and program updates:

COMODO Creating Trust Online\*

соморо и	Jpdate	? – 🗆 ×
80%	TASK: Check for program updates STATUS:	
TASK		STATUS
Check for sign	ature updates	Completed
Oownload sign	natures	Completed
Install signatur	res	Completed
Check for web	sites database updates	Completed
Check for reco	ognizer updates	Up to date
Check for pro	gram updates	In Progress
		<u>View Logs</u>
PAUSE STOP		SEND TO BACKGROUND

CCS will ask you to confirm the update at the following dialog:



• Click 'Yes' to begin installation:

You need to restart the computer to complete the update process. You can restart immediately or postpone the restart until later:

COMODO Creating Trust Online\*

COMODO Client - Security 11	?
$\frac{1}{2}$ Restart Computer Your computer needs to be restarted to complete the process	55.
You may choose to restart it now or postpone this to a later time	
Remind me in:	
30 minutes	
RESTART NOW POSTPON	IE

### **Automatic Updates**

By default, CCS automatically checks for and downloads database updates. You can modify these settings in **Settings > General Settings > Updates.** 

COMODO Advance	d Settings ? - 🗆 🗙
<ul> <li>General Settings</li> <li>User Interface</li> </ul>	O Updates
Updates	Check for database updates every
Logging	Options
Configuration	Do not check for updates if I am using these connections
✓ Antivirus	Do not check for updates if running on battery
✓ Firewall	Check for updates during Windows Automatic Maintenance
✓ HIPS	Send requests to COMODO online services only if internet connection is present
✓ Containment	Proxy and Host Settings
✓ File Rating	
✓ Advanced Protection	
	OK CANCEL

You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. See 'Scan Profiles' for more details.

COMODO Creating Trust Online\*

### 2.5. Manage Blocked Autoruns

- Click 'Tasks' > 'General Tasks' > 'Unblock Autoruns'
- The 'Unblock Autoruns' area shows applications that were blocked by the boot protection feature of CCS.
- The feature monitors changes attempted to the registry records of Windows services, auto-start entries and scheduled tasks. The feature can be managed in the following locations:
  - **Realtime Scans** Click 'Settings' > 'Advanced Protection' > 'Miscellaneous' > ' Apply the selected action to unrecognized autorun entries to new/modified registry items'
  - On-Demand Scans Click 'Settings' > 'Antivirus Settings' > 'Scans' > 'select the scan profile' > 'Options' > 'Apply this action to suspicious auto-run processes'
- CCS will terminate and disable apps that attempt to modify protected registry items, if 'Terminate and Disable' is chosen for 'Apply this action to suspicious auto-run processes'
- If you feel that a particular application is safe, you can unblock it.

### View and manage blocked autorun items

- Click 'Tasks' > 'General Tasks'
- Click the 'Unblock Autoruns' tile
- The interface shows all auto-run items blocked by CCS:

COMODO Creating Trust Online\*

	ME {ô} SETTING						
НО	ME (0) SETTING	<b>)</b>					
<u> </u>	Secure   All sys	tems are active	and running				
GENER	AL TASKS CONTA	INMENT TASKS	ADVANCED TASKS				Q.
	Scan Scan your comp	uter for viruses a	ind spyware.	View Quarantir View and manage scanner.		rantined by viru:	₹ 5
C	Update Run the updater database update	to check for pro	द्र gram and virus				
	Re-enable previo auto-start items	ously blocked Wi		>			
<b>∆</b> × si	LENT MODE	Τ					(?)
0		ock Autoruns				? –	
			utanun itana Vau a	an unblank anu af th			
alow	is the list of curre	ility disabled a	diorum items. Tou ca	an unblock any of the	em, n you a	ite sure they a	are sale.
elow Vnbl	is the list of curre Ock Delete	<b>⊘</b> Delete All					
~	· 0		▲ Detected By ▼	Date/Time	Action 🝸	Location	م
Vnbl	ock Delete	Delete All	▲ Detected By      ▼     Autoruns Scanner	Date/Time 1/10/2019 11:06:5			
Unbl	ock Delete	Delete All Type 🍸			Disabled	r⊌ C:\Progr	Q am Files (x86) am Files (x86)

	Unblock Autoruns - Column Descriptions				
Column Header	Description				
Name	The label of the blocked item				
Туре	The category of item. For example, 'Autorun File', 'Scheduled Task' or 'Windows Service'.				
Detected By	The security module which identified the threat				
Date/Time	When the item was detected				
Action	The response to the threat. The possible actions are: <ul> <li>Ignore</li> </ul>				

COMODO Creating Trust Online\*

	Terminate	
	Terminate and Disable	
	Quarantine and Disable	
Location	Path of the identified application	

### Restore blocked autorun items

- Click 'Tasks' > 'General Tasks' > 'Unblock Autoruns'
- Select the items you want to release
- Click the 'Unblock' button:

elow i	todo uni		utorun items. You c	an unblock any of t	hem if you	are sure th	nev are safe
Unblo	Ø	Delete All	atorun iterns. Tou c	an unblock any of t	nem, n you	are sure th	icy are sare.
	Name Q	Type 🍸	▲ Detected By	Date/Time	Action 🍸	Location	n Q
	nuWIRE	Autorun File	Autoruns Scanner	1/10/2019 11:06:5.	. Disabled	<b>س</b> C:\Pr	rogram Files (x86)
$\bowtie$	Application R	Autorun File	Autoruns Scanner	1/11/2019 2:41:54.	. Disabled	C:\Pr	rogram Files (x86),
	сом (!	Would you excluded fi	like to add these f	iles to your antivir	× us		
			YE	is I	10		

An option will be provided to add the file(s) to Scan Exclusions list.

- Click 'Yes' to add the item(s) to the 'Scan Exclusions' list. The items will be restored to their original locations and will be skipped in the future scans.
- Click 'No' to ignore the item once. The item will restored to its original location. It will be flagged as a threat during the next scan.

### Delete blocked autoruns entries

- Click 'Tasks' > 'General Tasks' > 'Unblock Autoruns'
- Select the items you want to remove
- Click the 'Delete' button

The item will be removed from your computer.

### 2.6. Manage Quarantined Items

- Click 'Tasks' > 'General Tasks' > 'View Quarantine'
- The 'Quarantine' interface contains a list of malicious files which CCS has isolated to prevent them from

COMODO Creating Trust Online\*

infecting your system.

- All files in quarantine are encrypted, so they cannot run or cause harm.
- Items are usually quarantined by the antivirus scanner, but it is also possible to manually quarantine items.
   See 'General Tasks' > 'Scan and Clean Your Computer' if you want to learn about the AV scanner.

### Open the 'Quarantine' interface

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'

_	ure All system	s are active a	ind running		
GENERAL TA	ASKS FIREWALL T	ASKS CON	TAINMENT TASKS	ADVANCED TASKS	(
	Scan Scan your computer f	for viruses an	d spyware	View Quarantine View and manage the scanner.	nreats quarantined by virus
	Update Run the updater to cl database updates.		and virus		2
ОМО	DDO Quarant	tine			? – 🗆
<b>∔</b> Add	<b>⊘</b> Delete	C Restore	<b>⊘</b> Delete All S	vbmit	
	tem	Q	Location	۹	Date/Time 🕻
				s\Malware-Samples-mas	5/29/2019 3:58:15 PM
	1alware@#jgft8m0j	xmvk	(a) c.(Suspiciou	s (maiware samples mas	
	1alware@#jgft8m0j 1alware@#vigyaokl		_	s\Malware-Samples-mas	
		h7gw	C:\Suspiciou		5/29/2019 3:58:07 PM
	1alware@#vigyaokI	h7gw h7gw	<ul> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> </ul>	s\Malware-Samples-mas	5/29/2019 3:58:07 PM 5/29/2019 3:58:02 PM
	1alware@#vigyaokl 1alware@#vigyaokl	h7gw h7gw xrw2dy	<ul> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> </ul>	s\Malware-Samples-mas	5/29/2019 3:58:07 PM 5/29/2019 3:58:02 PM
	1alware@#vigyaokl 1alware@#vigyaokl 1alware@#1ienpeu:	h7gw h7gw xrw2dy kcvjrs	<ul> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> <li>C:\Suspiciou:</li> </ul>	s\Malware-Samples-mas s\Malware-Samples-mas s\8200755cbedd6f15eec	5/29/2019 3:58:07 PM 5/29/2019 3:58:02 PM 5/29/2019 3:57:40 PM 5/29/2019 3:54:06 PM

• Item - The name of the malicious component

COMODO Creating Trust Online\*

- Location The file path of the item
- **Date/Time** When the item was moved to quarantine.

The interface lets you review quarantined files and take the following main actions:

- Permanently delete the file
- Restore the file to its original location
- Submit the file to Comodo Valkyrie for analysis
- Manually add files to quarantine

#### Search and filter options:

- · Click any column header to sort the items in alphabetical order
- Click the search icon in the 'Item' column to search for a file by name.
- Click the search icon in the 'Location' column to search by file-path.
- Click the icon in the 'Date/Time' column to filter results by time period.

Item       Q       Location       Q       Date/Time         Malware@#1ljgilp93a2m7       C:\Suspicious\po       Image: C:\Suspicious\po       Image: Within last       Image: C:\Suspicious\po         Backdoor.Win32.Rbot.~gen       C:\Suspicious\po       Image: Within last       Image: C:\Suspicious\po         Malware@#1ljgilp93a2m7       C:\Suspicious\po       Image: C:\Suspicious\po       Image: C:\Suspicious\po         Image: C:\Suspicious\po       Image: C:\Suspicious\po       Image: C:\Suspicious\po       Image: C:\Suspiciou	+ Add	<b>⊘</b> Delete	C Restore	<b>⊘</b> Delete All	Submit	
□       Imainance + Hyginpose Linit       □       et(suspicious)po       □         □       Backdoor.Win32.Rbot.~gen       □       C:\Suspicious\po       ○       Within last       1        hour(s)          □       Application Win22.Element of C:\Suspicious\po       ○       Except last       1        hour(s)          □       Application Win22.Element of C:\Suspicious\po       ○       Today       ○       Current week	Iter	m	Q	Location		Q 🔻 Date/Time
Backdoor.Win32.Rbot.~gen       C:\Suspicious\po         ○ Except last       1 < hour(s)	🗌 Ma	lware@#1ljgilp	93a2m7	C:\Suspi	icious\po	(No filtering)
O Today O Current week	Bac	kdoor.Win32.F	Rbot.~gen	C:\Suspi	cious\po	
	An				cionntain	⊖ Today
O Current month						O Current week
						O Current month
						05/02/2019 👻 - 05/02/2019 👻

### Manually add files to quarantine

Files or folders that you are suspicious of can be manually moved to quarantine:

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Click the 'Add' button at the top
- Navigate to the file you want to add to the quarantine and click 'Open'.

Creating Trust Online\*

UM	ODO Quar	antine				?	—
+ Add	Ø Delete	<b>C</b> Restore	<b>⊘</b> Delete All	<b>↓</b> Submit			
Y	Item	Q	Location		Q	▼ Date/	Time
	Malware@#1ljgilp	o93a2m7	C:\Susp	cious\poison2\	smb-id9dl67p	5/2/201	<b>19</b> 11:08:43 A
	Backdoor.Win32.F	Rbot.~gen	C:\Susp	cious\poison1\	smb-b_8ti77	4/30/20	) <b>19 2:43:</b> 03 P
ni ana ana ana ana ana ana ana ana ana a	Application Mina	lafalafitast.a					
	🔄 Open						×
	Look in:		~		✓ G Ø  Date modi	° <u></u>	Туре
	Quick access	venom			13-10-201	4 19:10	Applicatic
	Desktop						
	Libraries						
	This PC						
	This PC						
	This PC	<	venom				> Open

The file will be added to 'Quarantine'. You can even send the file for analysis to Comodo Valkyrie, for inclusion in the white list or black list, by clicking the 'Submit' button.

#### Remove a quarantined item

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items in the quarantine interface and click the 'Delete' button at the top.
- Click the 'Delete All' button if you want to permanently remove all quarantined items.
- The files will be deleted from your computer

#### Restore a quarantined item

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items to be moved back to their original locations and click the 'Restore' button at the top.

COMODO

COMODO Quarantine			?	-		×
+ ⊗ C Add Delete Rest						
✓ Item	Q Location	Q	Date/	Time		Ť
Generic.Infector.4	C:\Users Desktop\x86\vt.exe		4/10/2	2017 6:2	0:16 AN	1
Vould you like to add these files to your antivirus excluded files too?						
	YES	NO				
	R	EFRES	н		CLOSE	

You will be asked if you want to add the item to the Scan Exclusions list:

- 'Yes' The file will be restored to its original location. It will not be flagged as dangerous nor quarantined by future antivirus scans.
- 'No' The file will be restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.

### Submit selected quarantined items to Valkyrie for analysis

Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items you want to submit. You can send several files at once.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

Tip: Alternatively, right click an item then choose 'Submit to Valkyrie' from the menu.

 All submitted files are analyzed at Valkyrie. If they are found to be trustworthy, they will be added to the Comodo safe list (white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (blacklisted).

# 3. Firewall Tasks - Introduction

- Click 'Tasks' > 'Firewall Tasks'
- The firewall offers the following main benefits:
  - · Monitors all network traffic to protect your computer against inbound and outbound threats
  - Hides your computer's ports from hackers
  - Blocks malicious software from transmitting your confidential data over the internet.
- The firewall tasks area lets you configure internet access rights per-application, stealth your computer ports, view active connections, and even block all traffic in-and-out of your computer.

Creating Trust Online\*

In addition to this tasks screen, you can also **configure advanced firewall settings** at 'Settings' > 'Firewall'.

COMODO Client - Security 11	– ×
K HOME () SETTINGS	
Secure   All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	S ADVANCED TASKS
Allow Application Allow an application to connect to the internet.	Manage Networks Allow or block connections from other computers in detected networks.
Block Application Slock an application from accessing the internet.	Stop Network Activity Block all network activity to and from this PC.
Stealth Ports Manage this PC's network visibility from other PC's.	View Connections View applications which are connected to the internet.
⊄]× SILENT MODE	0

See the following sections for help with each area:

- Configure internet access rights for applications
- Stealth your computer ports
- Manage network connections
- Stop all network activity

•

View active Internet connections

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See 'Password Protection' for more details."

#### 3.1. Configure internet access rights for applications

- Click 'Tasks' > 'Firewall Tasks' > 'Allow Application' or 'Block Application'
- The firewall tasks screen lets you quickly allow or block applications from accessing the internet.

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K номе ေ{ွ်} settings	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS ADVANCED TASKS	0
	etworks * ck connections from other n detected networks.
Block Application	
Stealth Ports Manage this PC's network visibility from other PC's. View Conr View Conr View conr View conr View conr View conr	ections *
	(?)

#### Allow an application to connect to the internet

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Allow Application'
- Browse to the main executable file of the application
- Click 'Open'.
- This will create an 'Allow Request' rule for the application in 'Settings' > 'Firewall' > 'Application Rules'

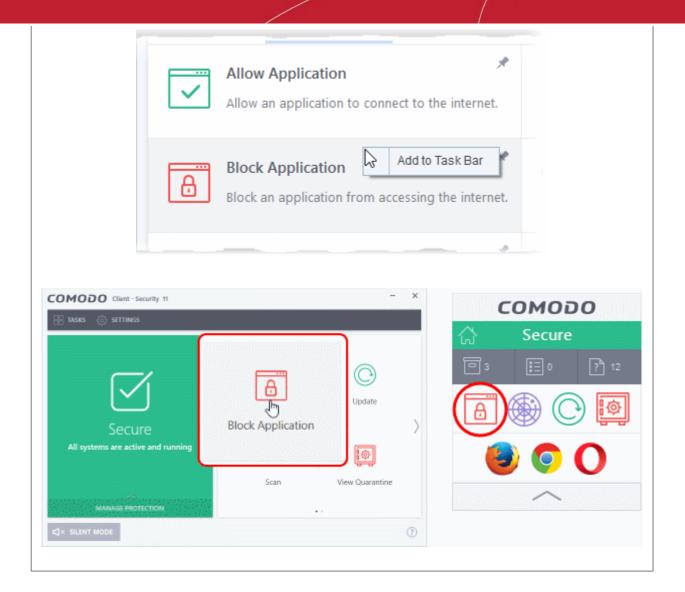
#### Block an application's Internet access rights

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Block Application'
- · Browse to the main executable file of the application
- Click 'Open'.
- This will create an 'Block Request' rule for the application in 'Settings' > 'Firewall' > 'Application Rules'

See 'Application Rules' for more info about creating internet access rules.

**Tip**: If you plan to regularly allow/block applications, right-click on the appropriate tile then select 'Add to Task Bar'. You can then quickly access the action on the CCS home screen and the widget:

COMODO Creating Trust Online\*



#### 3.2. Stealth your Computer Ports

- Click 'Tasks' > 'Firewall Tasks' > 'Stealth Ports'
- Port stealthing is a security feature which hides your ports to the outside world, providing no response to port scanners.

**What is a port?** Your computer sends and receives data through an interface called a 'port'. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to the internet using ports 80 and 443. Your email application connects to your mail server through port 25. A 'port scanning' attack consists of sending a message to each of your computer ports, one at a time. This information is used by hackers to find out which ports are open, and which ports are being used by services on your machine. With this knowledge, a hacker can determine which attacks are likely to work against your machine.

- Stealthing a port effectively makes your computer invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt. A closed port responds with a 'closed' reply, which reveals that there is a PC in existence.
- If a hacker or automated scanner cannot 'see' your computer then they will move on to other targets. You can still connect to the internet and transfer information as usual, but remain invisible to outside threats.

Stealth ports on your computer

• Click 'Tasks' > 'Firewall Tasks'

COMODO Creating Trust Online\*

Click 'Stealth Ports'

٠

	COMODO Stealth Ports ?				
	Ports allow your computer to communistication stealthing them, you may configure the	nicate with other computers in a network. By nis computer's visibility to others.			
GENERAL TASKS FIREWA	computers	ections tions and make this PC invisible to all			
Block Applicat	Alert Incoming Connect	<b>ctions</b> nake this PC invisible on a case basis by			
Block an applicat	on from coessing the internet.	BIOCK all network activity to and			
		View Connections			
Stealth Ports					
	C's network visibility from other	View applications which are contra- internet.			

Block incoming connections - Your computer's ports are invisible to all networks, regardless of whether
you trust them or not. The average home user (using a single computer that is not part of a home LAN) will
find this option the most convenient and secure. You are not alerted when the incoming connection is
blocked, but the rule adds an entry to the firewall event log file. Specifically, this option adds the following
rule in the 'Global Rules' interface:

Block And Log| IP | In| From Any IP Address| To Any IP Address | Where Protocol is Any



If you would like more information on the meaning and construction of rules, please click here.

 Alert incoming connections - You will see a firewall alert every time there is a request for an incoming connection. The alert asks your permission on whether or not you want the connection to proceed. This can be useful for peer-to-peer and remote desktop applications which need to access your ports in order to connect. Specifically, this option adds the following rules in the 'Global Rules' interface:

Block ICMPv4 In From <Any IP Address> To <Any IP Address> Where Message is <Message>

COMODO

Solock ICMPv4 Out From MAC Any To MAC Any Where ICMP Message Is PROTOCOL UNREACHABLE
Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 17.0
S Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 15.0
S Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 13.0
S Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is ECHO REQUEST

If you would like more information on the meaning and construction of rules, please click here.

#### 3.3. Manage Network Connections

- Click 'Tasks' > 'Firewall Tasks' > 'Manage Networks'
- The manage connections interface lets you quickly view all wired and wireless networks to which your computer is connected.
- The lower half of the panel show each network's name, IP address and gateway.
- · You can choose to allow or block a connection from this interface

#### View all network connections

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Manage Networks'

COMODO Creating Trust Online\*

MODO Client - Security 11	- ×
HOME (3) SETTINGS	
Secure All systems are active and running	
SERAL TASKS FIREWALL TASKS CONTAINMENT TASK	ADVANCED TASKS
Allow Application Allow an application to connect to the interne	Allow or block connections from other commers in detected networks.
Block Application	Stop Network Activity Block all network activity to and from this PC.
COMODO Manage Networks	? ×
	QF9QT (This Computer)
m	<u> </u>
Work #1	Work #2
	✓ TRUST NETWORK × BLOCK NETWORK
REFRESH	OK CANCEL

- Use the handles (< >) to scroll through all available networks or computers
- **Trust Network and Block Network** You can allow or ban a network by clicking the appropriate button under the network in question. You will not receive any inbound or outbound traffic from blocked networks.
- **Refresh** Reloads the list with the latest network connections. Click this button if you have recently made network changes that are not yet visible in the interface.
- To view, create or block Network Zones, click 'Settings' > 'Firewall' > 'Network Zones'

#### 3.4. Stop all Network Activities

- Click 'Tasks' > 'Firewall Tasks' > 'Manage Networks'
- The 'Stop Network Activity' feature terminates all inbound/outbound communication between your computer and outside networks (including the internet).
- Connections will remain closed until you re-enable them by clicking 'Restore Network Activity'.

Creating Trust Online\*

• This lets you quickly take your computer offline without having to delve into Windows network settings, and without unplugging cables.

COMODO Client - Security 11	- ×
K HOME (j) SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	S ADVANCED TASKS
Allow Application * Allow an application to connect to the internet.	Allow or block connections from other computers in detected networks.
Block Application Block an application from accessing the inter	Block all not work activity to and from this PC.
Stealth Ports Manage this PC's network visibility from other PC's.	View Connections View applications which are connected to the internet.
r∰× SILENT MODE	(?)

Manage network activities from your computer:

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Stop Network Activity' to disconnect your computer from all networks
- · Click 'Restore Network Activity' to re-enable connectivity



- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have
  previously blocked in 'Manage Network Connections' or 'Network Zones' will remain blocked
- · You can assign networks to network zones in the 'Network Zones' area
- · You can configure rules per network zone in the 'Global Rules' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the 'Manage Network Connections' area

COMODO Creating Trust Online\*

#### 3.5. View Active Internet Connections

- Click 'Tasks' > 'Firewall Tasks' > 'View Connections'
- View connections shows which applications and services currently have an active internet connection.
- You can view the individual connections that each application is responsible for, the direction of the traffic, the source IP/port, and the destination IP/port.
- You can also see the total amount of traffic that has passed in and out of your system over each connection. The list is updated in real time whenever an application opens or drops a connection.
- 'View Connections' is extremely useful when testing firewall configurations or troubleshooting firewall policies and rules. You can also use it to terminate unwanted connections.

#### View active internet connections on your computer

- Click 'Tasks' > 'Firewall Tasks'
- Click 'View Connections'

**Tip**: You can also get to this screen by clicking the number below 'Inbound' or 'Outbound' in the home screen (advanced view).

Protocol	Source	Destination	Bytes In	Bytes Out
🗊 🗏 smartscreen	.exe [3752]			
	10.108.51.194:57606	23.101.182.153:443	7.5 KB {5.7 K	2.6 KB {2.0
😡 🗏 MyWeather.	exe [7160]			
- TCP OUT	10.108.51.194:57616	23.203.134.90:443	436.0 KB {68	9.8 KB {14
- TCP OUT	10.108.51.194:57623	185.53.178.8:80	0 B	198 B
	10.108.51.194:57636	185.53.178.8:80	0 B	198 B {14
🚦 🗏 Evernote.ex	e [1984]			
- TCP OUT	10.108.51.194:57617	35.186.213.138:443	66 B	66 B
- TCP OUT	10.108.51.194:57619	35.186.213.138:443	66 B	66 B

- Protocol The application that is making the connection, the protocol it is using, and the direction of the traffic. Each application may have more than one connection at any time. Click + to expand the list of connections.
- **Source (IP : Port)** The IP address and port number of the origin of the traffic. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** The IP address and port number of the target. This is blank if the 'Source' column is 'Listening'.

COMODO Creating Trust Online\*

- Bytes In The total bytes of incoming data since the session started.
- Bytes Out The total bytes of outgoing data since the session started.

#### **Context Sensitive Menu**

• Right-click on an item to open the context sensitive menu:

	Source		Destination
ITSMService.exe	e [1664]		
- TCP OUT	10.0.2.15:4	9162	<b>69.4.89.243:44</b> 3
TCP OUT	10.0.2.	Show Full Path Terminate Connection	<b>5.157.49.4</b> :443
System [4]		Jump to Folder	

- · 'Show Full Path' view the location of the application
- 'Terminate Connection' close the application's connection
- · 'Jump to Folder' Open the folder containing the application executable

#### Identify and kill unsafe network connections

KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

Comodo KillSwitch can show *ALL* running processes in granular detail - exposing even those that were invisible or very deeply hidden. You can simultaneously shut down every unsafe process with a single click and can even trace the process back to the parent malware.

Click the 'More' button in the 'View Connections' to directly access Comodo KillSwitch

— TCP OUT	10.0.2.15:49304	54.88.32.157:80	60 B	66 B
TCP OUT	10.0.2.15:49305	178.18.231.91:80	60 B	66 B

If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CCS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.

COMODO Creating Trust Online\*

COMODO Client - Security 11		- ×
Install Required Packages The feature requires installation of ac	dditional packages.	
Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	7 MB
By pressing "Agree and Install", you agree with us	er license agreements for all the pa	ckages listed above.
		AGREE AND INSTALL
Click 'View License Agreement' to read the	license agreement	

• Click 'Agree and Install' to download and install the application.

COMODO Client - Security 11	- ×
Install Required Packages The feature requires installation of additional packages.	
Installing COMODO KillSwitch	99 %
	CANCEL

• KillSwitch will open when installation finishes:

COMODO Creating Trust Online\*

Network Connections (54)			😗 <u>Show netw</u>	ork traffic	-25.0	0% (K: 17.00%, U: 8.00%
Protocol	Local Address	Local Port Remote Address	Remote Port State	Owner		
🖃 💷 svchost.exe(824)						
- тср	jbvm2	135 jbvm2	Listen	RpcSs		
L TCP6	jbvm2	135 jbvm2	Listen	RpcSs	44.60	
🖃 💷 System(4)						
- тср	jbvm2	139 jbvm2	Listen		I/O	
- тср	jbvm2	49155 192.168.70.39	445 Establis		-R+0	): 122,37 KB, W: 0
- ТСР	jbvm2	445 jbvm2	Listen			
– тср	jbvm2	5357 jbvm2	Listen			
— ТСР6	jbvm2	445 jbvm2	Listen			
— ТСР6	jbvm2	5357 jbvm2	Listen			- Awa
– UDP	jbvm2	137				
L UDP	jbvm2	138				
ITSMService.exe(1664)					Phys	ical Memory
- тср	jbvm2	20777 jbvm2	Listen		-482	46 MB
– тср	localhost.cmdm	20777 localhost.cmdm.comodo.net	49173 Establis			
- тср	jbvm2	49162 243.89.4.69.in-addr.arpa	443 Establis			
- тср	jbvm2	49291 ec2-35-157-49-4.eu-central	443 Establis			
– тср	jbvm2	21185 jbvm2	Listen			
— ТСР6	jbvm2	21185 jbvm2	Listen			
L TCP	jbvm2	49454 ec2-52-59-11-165.eu-centra	443 Establis		Neb	
🖃 💷 wininit.exe(480)					New	70rk
- ТСР	jbvm2	49152 jbvm2	Listen		-10 6	05 07 00L 540 D
L тср6	jbvm2	49152 jbvm2	Listen			
🖃 💷 svchost.exe(984)					-	
<pre></pre>						

# 4. Containment Tasks - Introduction

- Click 'Tasks' > 'Containment Tasks'
- 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.
- This makes it an ideal environment for surfing the internet, because nothing you download can spread to your host system.
- 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.

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K HOME () SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Open Shared Space         *           Open the storage space shared between virtual and real applications.
Reset the Container Clean container data by erasing all its content.	Watch Activity Open COMODO KillSwitch to monitor advanced process and system activity.
Run Virtual Desktop Create a secure virtual desktop and start using it.	Containment Statistics Analyzer View analysis of Containment events and protection statistics of the component.
r⊈× SILENT MODE	?

#### Note: Containment is not supported on Windows XP or Windows Server 2003

Containment tasks has the following areas:

- Run Virtual Run individual applications in the container.
- Open Shared Space Shared space is a folder which you can access from both your real desktop and the virtual desktop. When in the virtual desktop, save your files in shared space if you want to open them on your host computer.

Background. Applications in the container write to a virtual file system and not your local drive. This prevents them from making potentially malicious changes to your files and folders.

The one exception to this is a folder called 'Shared Space'. This folder can be accessed by both your host operating system and contained programs. Use the folder to share files between your computer and the container.

The folder is located at 'C:\Documents and Settings\All Users\Application Data\Shared Space'.

- **Reset Containment** Clears all data written by programs inside the container.
- Watch Activity Open Comodo KillSwitch to identify unsafe processes and manage system activity.
- Run Virtual Desktop Start the virtual desktop environment.
- **Containment Statistics Analyzer** Detailed information about the processes running on your computer. Processes are split into contained and non-contained processes.

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See 'Password Protection' for more details."

#### 4.1. Run an Application in the Container

Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'

COMODO Creating Trust Online\*

- Choose the program you want to run
- Click 'Open'

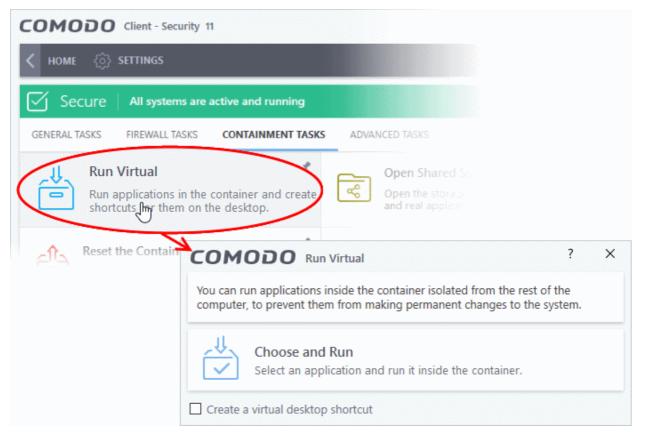
This method above will run the application in the container one-time only. On subsequent executions it will not run in the container. You need to create an **auto-containment rule** if you want it to always run in the container.

You can also create desktop shortcuts to always launch an application in the container:



#### Run an application in the Container

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



- 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.

COMODO Creating Trust Online\*

🛿 Open			×
← → ~ ↑ 📙 « Pr	ogra > DrivingSpeed2 > V Č	Search DrivingSpeed2	<i>م</i>
Organize 👻 New fold	er		. ?
A Quick access	Name	Date modified	Туре
📃 Desktop 🛛 🖈	🔥 data	28-10-2016 16:43	File fold
🕹 Downloads 🖈	🛷 DrivingSpeed	06-01-2012 15:58	Applica
Documents 🖈	🔂 unins000	28-10-2016 16:42	Applica
E Pictures	🔊 website	26-08-2007 15:13	Internet
🏪 Local Disk (C:)			
👌 Music			
SpreadSheets			
📑 Videos			
a OneDrive			
💻 This PC	٢		
Filer	ame: DrivingSpeed	<ul> <li>Applications (*.exe)</li> </ul>	
		Open 🚽 Ctiv 🖓	ancelVin o
		Go to Set	tings to

You can also run an applications in the container from the right-click menu:

COMODO Creating Trust Online\*

<ul> <li>← → * ↑ </li> <li>✓ Local Disk (C:) &gt; Program Files (x86) &gt; DrivingSpeed2 &gt; ✓ </li> <li>✓ Quick access</li> <li>✓ Desktop // </li> <li>✓ data</li> <li>✓ Date modified</li> <li>✓ Date modified</li> <li>✓ Type</li> <li>✓ Size</li> <li>✓ File folder</li> <li>✓ Downloads // </li> <li>✓ PrivingSpeed // </li> <li>✓ Open // </li> <li>✓ Run as administrator // </li> <li>✓ Troubleshoot compatibility // </li> <li>✓ Into Start // </li> <li>✓ Scan with COMODO antivirus // </li> <li>✓ Scan with COMODO antivirus // </li> <li>✓ Nusic // </li> <li>✓ Unins000.</li> <li>✓ SpreadSheets // </li> <li>✓ Videos // </li> <li>✓ This PC</li> </ul>	Image: Solution of the province of		inage		~
Network Cut	Create shortcut	★ Quick access       Name         ■ Desktop       ★         ↓ Downloads       ★         ● Documents       ★         ■ Pictures       ★         ■ Local Disk (C:)       ↓         Music       ↓         ■ SpreadSheets       ↓         ■ Videos       ↓         ▲ OneDrive       ↓	<ul> <li>Date modified 28-10-2016 16:43</li> <li>06-01-2012 15:58</li> <li>Open</li> <li>Run as administrator Troubleshoot compatibility Pin to Start</li> <li>Scan with COMODO antivirus</li> <li>Run in COMODO container</li> <li>Pin to taskbar Restore previous versions</li> <li>Send to  </li> </ul>	Type File folder Application Text Document Firefox HTML Doc Text Document DAT File Application	Size 1,157 KB 9 KB 3 KB 4 KB 208 KB 699 KB

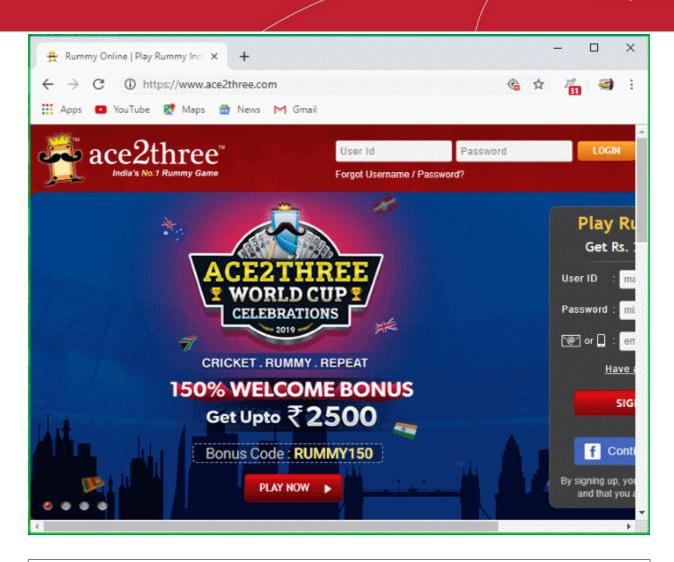
Choose 'Run in Comodo container' from the context sensitive menu

#### Run browsers in the container

The CCS widget contains shortcuts to run your browsers in the container:



• The green border indicates that the browser is in the container:



**Tip**: Running a browser in the container deletes all traces of your activities. This includes your browsing history, cookies, and offline data stored by the websites you visit. Virtualization protects your computer from anything malicious that is downloaded. See **The Virtual Desktop** for more details.

#### 4.2. Reset the Container

- Click 'Tasks' > 'Containment Tasks' > 'Reset the Container'
- Programs in the container write all data and system changes to a virtual file system. This means the program cannot harm your computer or sensitive data.
- Files saved in the container could contain malware downloaded from websites, or private data in your browsing history.
- Periodically resetting the container will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then a reset will also help the container operate more smoothly.
- The 'Reset the Container' option lets you delete all items saved in the container.

#### Clear the container

- Click 'Tasks' > 'Containment Tasks'
- Click 'Reset the Container'
- Click 'Erase Changes':

COMODO Creating Trust Online\*

K HOME <ြို SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Copen Shared Space Open the storage space shared between writed and real applications.
Clean container data by erasing all its content	Watch Activity Open COMODO KillSwitch to monitor advance process and system activity.
Run Virtual Desitop     *       Create a secure virtual desktop and start using it.     Image: Create a secure virtual desktop and start using it.	Containment Statistics Analyzer View analysis of Containment executive protection statistics whether an
COMODO Reset the Container	? ×
You may reset the container to eradicate all the applications.	changes made by contained
Erase Changes	

The contents in the container will be deleted immediately.

COMODO Reset the Container	×
The container has been successfully reset.	
CONTINUE	

• Click 'Continue' to close the dialog.

COMODO Creating Trust Online\*

### 4.3. Identify and Kill Unsafe Running Processes

Click 'Tasks' > 'Containment Tasks' > 'Watch Activity'

KillSwitch is an advanced system monitor that lets you identify and terminate any unsafe processes on your computer. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides another powerful layer of protection for Windows computers.

KillSwitch can even show processes that were invisible or very deeply hidden. You can identify all unsafe processes with a single click then quickly shut them down. You can also trace back to the software that generated the process.

#### **Open KillSwitch**

- Click 'Tasks' > 'Containment Tasks'
- Click the 'Watch Activity' tile

COMODO Client - Security 11 -	×
K HOME (j) SETTINGS	
Secure The virus signature database is NOT up-to-date	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS ADVANCED TASKS	Q
Run Virtual Run applications in the container and create shortcuts for them on the desktop. Run applications. Automatic and create shortcuts for them on the desktop. Automatic and create shortcuts for them on the desktop.	📌 tual
Reset the Container Clean container data by erasing all its content.	iced
Run Virtual Desktop Create a secure virtual desktop and start using it. Containment Statistics Analyzer View analysis of Containment events and protection statistics of the component.	*
≪ SILENT MODE	?

If Comodo KillSwitch is already installed in your computer, clicking 'Watch Activity' will open the application. If not, CCS will download and install KillSwitch.

COMODO Creating Trust Online\*

COMODO Client - Security 11		– ×
Install Required Packages           The feature requires installation of action	lditional packages.	
Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	7 MB
By pressing "Agree and Install", you agree with us	er license agreements for all the pa	ickages listed above.
		AGREE AND INSTALL
Click 'View License Agreement' to read the	C C	

Click 'Agree and Install' to download and install the application.

COMODO Client - Security 11	- ×
Install Required Packages The feature requires installation of additional packages.	
Installing COMODO KillSwitch	99 %
	CANCEL

KillSwitch will open when the installation is over:

.

COMODO

System K Network  Processes (57)  Name PID A Rating Restriction Virtualizati CPU Working Set User N System Idle Process 0 85.93 4 KB	Name A
Name PID A Rating Restriction Virtualizati CPU Working Set User N System Idle Process 0 85.93 4 KB	
E System Idle Process 0 85.93 4 KB	Name 201
	122201120220122
- EL DPCs	
🖃 🔤 System 4 None Disabled 132 KB LOCA	
	UTHORITY\SY.
Memory Compression 2032 191,372 KB NT AU	
E csrss.exe 444 Trusted None Disabled 3,728 KB NT AU	UTHORITY\SY.
Ewininit.exe 508 Trusted None Disabled 4,280 KB NT AU	UTHORITY\SY.
Imservices.exe 592 Trusted None Disabled 3.12 8,324 KB NT AU	UTHORITY\SY.
I svchost.exe 228 Trusted None Disabled 68,266 KB NT AU	UTHORITY\SY.
- Trusted None Disabled 7,640 KB NT AU	UTHORITY\LO
La IIII Tab Tip.exe 4924 Trusted None Disabled 14,924 KB DESKT	TOP-HI950BN\
L III Tab Tip32.exe *32 4984 Trusted None Disabled 5,892 KB DESKT	
🖃 🗊 svchost.exe 716 Trusted None Disabled 20,732 KB NT AU	UTHORITY\SY.
- 💽 SearchUl.exe 1788 Trusted None Disabled 85,016 KB DESKT	TOP-HI950BN
<ul> <li>WmiPrvSE.exe *32</li> <li>2700 Trusted</li> <li>None</li> <li>Disabled</li> <li>34,092 KB NT AU</li> </ul>	UTHORITY\SY.
- TR RuntimeBroker.exe 3964 Trusted None Disabled 19,208 KB DESKT	TOP-HI950BN\
- I ShellExperienceHost.exe 4184 Trusted None Disabled 54,420 KB DESKT	TOP-HI950BN\
- @WmiPrvSE.exe 4444 Trusted None Disabled 9,760 KB NT AU	UTHORITY\SY.
<ul> <li>Image: ApplicationFrameHost.exe</li> <li>4760 Trusted</li> <li>None</li> <li>Disabled</li> <li>20,628 KB DESKT</li> </ul>	TOP-HI950BN\
- 💽 SystemSettings.exe 5380 Trusted None Disabled 38,952 KB DESKT	TOP-HI950BN\
Cavwp.exe 6096 Trusted None Disabled 51,888 KB NT AU	UTHORITY\SY.
- Telsvchost.exe 764 Trusted None Disabled 11,628 KB NT AU	UTHOR/TY\NE
- Trusted None Disabled 19,880 KB NT AU	UTHORITY\NE 🗸
	Q.
Applications (8)	
	( v

 See the KillSwitch guide for help to use the product - http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html.

### 4.4. Open Shared Space

- Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space'
- Applications in the container are not allowed to write to your local drive for security reasons. Instead, they write all data, and save all files, to a special folder called 'Shared Space'.
- Files in shared space can also be accessed by non-contained applications (those running as normal on your computer).
- If you want to access files in the container from your local system, then you should download them to shared space.
- The default location of shared space is 'C:/Program Data/Shared Space'

#### Open shared space

• Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space':

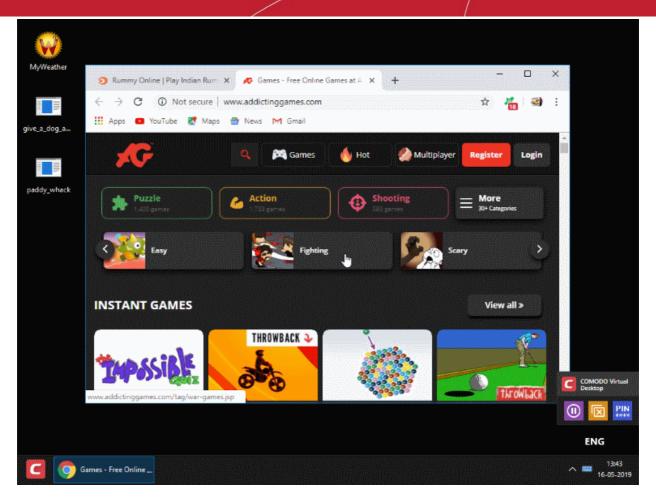
COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K HOME {ِنَ} SETTINGS	
Secure   The virus signature database is NOT up	p-to-date
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Open Shared Space Open the storage space shared between virtual and real applications.
Reset the Container Clean container data by erasing all its content.	Watch Activity Open COMODO KillSwitch to monitor advanced process and system activity.
Run Virtual Desktop Create a secure virtual desktop and start using it.	Containment Statistics Analyzer           View analysis of Containment events and protection statistics of the component.
⊄T× SILENT MODE	3

### 4.5. The Virtual Desktop

- Go to 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- The virtual desktop is a sandbox environment in which you can run programs and browse the internet without fear those activities will damage your computer.
- Applications in the virtual desktop are isolated from the rest of your computer, write to a virtual file system, and cannot access your personal data.
- This makes it ideal for risk-free internet surfing and for testing out beta/unstable software.

COMODO Creating Trust Online\*



Virtual Desktop at a glance:

- The virtual desktop can run any program that you normally run in Windows. It is ideal for running untested, unknown and beta software. You can also use it to visit websites that you are not sure about.
- Any changes made to files and settings in the virtual desktop will not affect the originals on your host system. Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Use the 'Shared Space' folder to save any files you want to access from Windows. This folder is the only place that the virtual desktop can write to on the host file system.
- You can also configure virtual desktop to access removable storage devices like USB sticks and external hard disk drives to store data from it.
- The virtual keyboard lets you to securely enter confidential passwords without fear of key-logging software.
- Apart from testing software, parents may want to consider the virtual desktop as a secure area for children to run programs and surf the web. Any actions they take will not damage the host computer. The virtual desktop can be reset and all changes cleared at the end of every session.
- The virtual desktop can be password-protected and configured to start automatically at user logon.
- You can create shortcuts on the host desktop to launch applications in the virtual environment.
- You can white-label the virtual desktop with your own company logos in the Endpoint Manager console.
  - See https://help.comodo.com/topic-399-1-786-10572-Communication-Client-and-Comodo-Client---Security-Application-UI-Settings.html for more on this

See the following sections for more help:

- Start the Virtual Desktop
- The Main Interface

COMODO Creating Trust Online\*

- Run Browsers inside Virtual Desktop
- Open Files and Run Applications inside Virtual Desktop
- Pause and Resume the Virtual Desktop
- Close the Virtual Desktop

#### 4.5.1. Start the Virtual Desktop

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

You can start the virtual desktop from the home-screen shortcut, from the widget, or from the 'Containment Tasks' screen. You can also configure the virtual desktop to start automatically after you login to Windows.

Note. If CCS is in Virtual Desktop mode, you can start the application by simply clicking the desktop shortcut.

See the following sections for more help:

- Open the virtual desktop from CSS or the widget
- Launch the virtual desktop at user logon
- Start the virtual desktop from the containment tasks screen

#### Start the virtual desktop from CCS or the widget

• Click the virtual desktop icon on the CCS home screen, or on the CCS widget:

COMODO Client - Security 11		- ×	
음 tasks 《ô》 settings			сомодо
			🟠 Secure
			<b>D</b> • <b>E</b> • <b>P</b> •
		©	
	Run Virtual Desktop	Update	
Secure		$\rangle$	
The virus signature database is NOT up-to- date		Ø	
FIX IT!	Scan	View Quarantine	
		,	
		0	

Note: The home screen and widget shortcuts are only available if you have added the 'Virtual Desktop' shortcut:

- Click 'Tasks' on the home screen
- Click 'Containment Tasks'
- Right-click on the virtual desktop tile
- Select 'Add to Task Bar'

See 'Add tasks to the home screen' if you need more help with this.

COMODO Creating Trust Online\*

#### The virtual desktop opens at the session selection screen.

#### Launch the virtual desktop at user logon

- You can configure the virtual desktop to start automatically whenever certain users login to Windows.
- This means the virtual desktop becomes the default operating environment for those users.

#### Add users

- Click 'Settings' on the home screen
- Click 'Containment ' > 'Virtual Desktop'
- Select the 'Users' tab
- Click 'Add'

	termination	Ľ	min(s)
otainment	APPLICATIONS USERS		
d Objects esktop	Users for whom Virtual Desktop will be launched as a	primary working environm	ent:
rotection	Add Remove Reset to Default		
lotection	User or Group	Q Enable	
	Guests		
	Alice		
		ОК	CANCEL
	<b>V</b>		
	Select User or Group	×	
	Select this object type: User, Group, or Built-in security principal	Object Types	
	From this location:		
	DESKTOP-BGTT5H7	Locations	
	Enter the object name to select ( <u>examples</u> ):	Check Names	
	Advanced	OK Cancel	

- Select the users or groups to whom you want the rule to apply.
  - Type the names of users or groups in the format <domain name>\<user/group name> or <user/group name>@<domain name>.

COMODO Creating Trust Online\*

JS	)ι	fic	cif	spe	) S	te	ocat	bl	to	low'	1 1	Find	n'	the	1 't	ced	/an	Ad	<b>&lt;</b> '	click	, (	vely,	rnativ	Alte	•	•
JSe	ι	fic	cif	spe	e s	te	ocat	bl	to	low'	11	Find	n'	the	1 't	ced	/an	Ad	<b>(</b> '	click	, (	vely,	rnativ	Alte	•	•

• Click 'OK' to confirm.

Select User or Gro	up		×			
Select this object ty	/De:					
User, Group, or Bu	Object Types					
From this location:						
DESKTOP-BGTT5	Locations					
Enter the object na	me to select ( <u>examples</u> ):					
			Check Names			
Advanced	)	ОК	Cancel			
Select User or Gro	up			×		
Select this object ty	/pe:					
User, Group, or Bu	ilt-in security principal		Object Types			
From this location:						
DESKTOP-BGTT5	iH7		Locations			
Common Queries						
Name: S	itarts with 🖂		Colu	mns		
Description: S	itarts with $$		Find	Now		
Disabled acc	counts		St	ор		
Non expiring	password					
Days since last	logon: 🗸		÷	7		
Search results: 🛩		[	OK Car	ncel		
lame	In Folder					
Access Contr	DESKTOP-BGT					
Administrator	DESKTOP-BGT					
Administrators Alice	DESKTOP-BGT DESKTOP-BGT					
Backup Oper	DESKTOP-BGT					
Bob	DESKTOP-BGT					
Cryptographic	DESKTOP-BGT					
DefaultAccount	DESKTOP-BGT					
Device Owners	DESKTOP-BGT					
C	DESKTOP-BGT					

The user / user group will be added to the list.

COMODO Creating Trust Online\*

t Settings	termination	Timi(s)
Objects	APPLICATIONS USERS	
	Users for whom Virtual Desktop will be launched	as a primary working environment:
otection	Add Remove Reset to Default	
recuon	User or Group	Q Enable
	Guests	
	Alice	
	Bob	
		OK CANCEL

- Repeat the process to add more users.
- Click 'OK' to save your settings
- Click 'OK' in the 'Advanced Settings' dialog for your changes to take effect
  - See 'Virtual Desktop Settings' if you need more help with this

The virtual desktop opens at the **session selection screen** when the selected users log-in.

#### Start the virtual desktop from the containment tasks screen

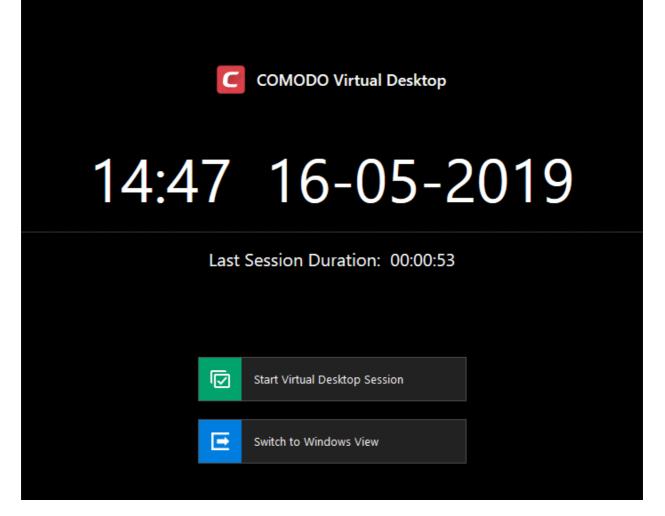
• Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
< HOME र्िु SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	NCED TASKS
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Open Shared Space * Open the storage space shared between virtual and real applications.
Reset the Container Clean container data by erasing all its content.	Watch Activity Open COMODO KillSwitch to monitor advanced process and system activity.
Run Virtual Desktop Create a secure virtual desktop and start using it.	Containment Statistics Analyzer View analysis of Containment events and protection statistics of the component.
⊄X SILENT MODE	0

The virtual desktop opens at the session selection screen.

COMODO Creating Trust Online



- Click the 'Start Virtual Desktop Session' button
- Click 'Accept' at the disclaimer screen to open the virtual desktop.

С	Virtual Desktop - Disc	laimer		×	<
	You are about to laur before you continue.	nch new Virtual Desktop s	ession. Please read the f	ollowing carefully	
	<insert discla<="" td=""><td>imer text here≻</td><td></td><td></td><td></td></insert>	imer text here≻			
		Accept	Decline		

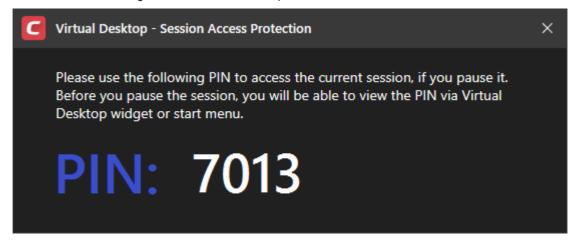
**Note**: This screen is only relevant for customers who white-label the interface. It can be safely ignored by most customers and end-users.

COMODO Creating Trust Online\*

If you do want to white-label the interface, you can configure the disclaimer message at 'Settings' > 'Containment' > 'Virtual Desktop'. You can also disable the disclaimer entirely from there.

See 'Show disclaimer upon Virtual Desktop startup' to view help with this. Details on how to white-label CCS are in a wiki article here.

You will see a four digit access code If session protection is enabled:

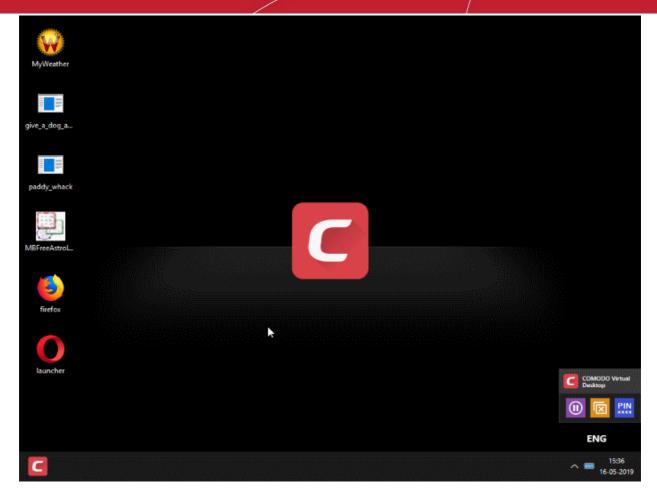


- This feature lets you suspend a virtual desktop session and resume it later without losing any data. The PIN is required to unlock the suspended session.
- Please make a note of the PIN number. See Pause and Resume the Virtual Desktop for more details
- Tip: You can view the PIN at any time by clicking the 'Show PIN' icon in the virtual desktop start menu

#### 4.5.2. The Main Interface

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button
- The virtual desktop contains shortcuts for selected applications on the left.
- The start menu contains shortcuts for selected applications and controls for pausing the session and closing the virtual desktop.
  - You can add desktop shortcuts and start menu items for applications you frequently want to open in the virtual desktop from the 'Settings' > 'Containment' > 'Virtual Desktop' interface. See Add applications to virtual desktop in Virtual Desktop Settings for more details.
- The tools box at the bottom-right contains controls for pausing and closing the virtual desktop session.

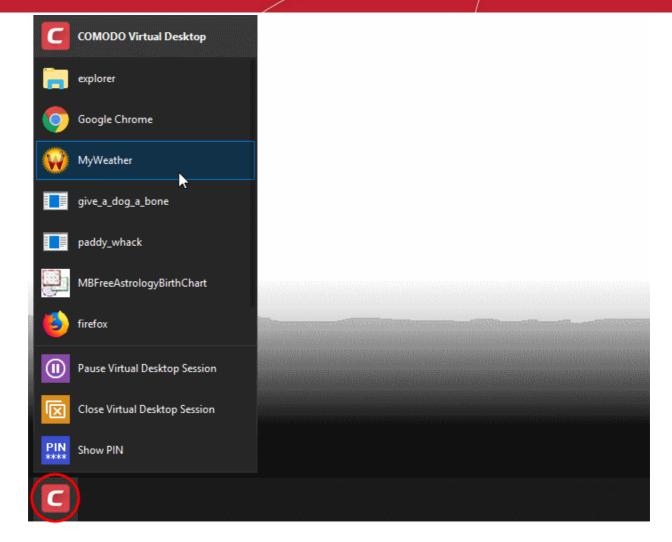
COMODO Creating Trust Online\*



#### The 'Start' menu

• Click the red 'C' icon to open the start menu:

#### COMODO Creating Trust Online\*



The menu has the following options:

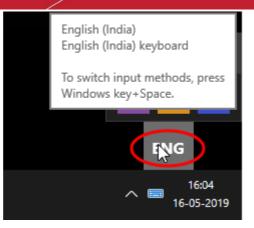
- Browsers and other applications The start menu contains shortcuts for Windows Explorer and the default browser of your computer by default. You can add shortcuts for other browsers and applications that you often open inside the virtual desktop. See Add applications to virtual desktop in Virtual Desktop Settings for more details.
  - Click on an item to open it inside the virtual desktop.
- Pause Virtual Desktop Session Temporarily close the virtual desktop. If PIN protection is enabled, you need the PIN to resume a paused session. See Pause and Resume the Virtual Desktop for more details.
- Close the Virtual Desktop Session Exit the virtual desktop and return to your Windows system. If your virtual desktop is password protected, you have to enter the password to exit. See Close the Virtual Desktop for more details.
- Show PIN Displayed only if PIN protection is enabled for virtual desktop. Shows the PIN number generated for the current session. This is required for you to resume a paused session. See Pause and Resume the Virtual Desktop for more details.

ENG

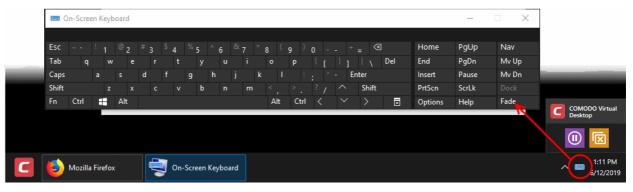
**Tools and Taskbar** 

 Keyboard layout - Click the language button want to use . at bottom-right and select the keyboard layout you

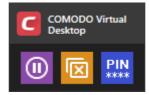
COMODO Creating Trust Online\*



• Virtual keyboard - Click the keyboard icon on the system tray to open a virtual keyboard.



- You can use this to enter confidential data online (usernames, passwords and credit card numbers etc).
- The keyboard can also be used with touch screen displays.
- **Tools Box** The tools box at the bottom-right contains controls for pausing and closing the virtual desktop.



- Pauses the virtual desktop session. If PIN protection is enabled, you need the PIN to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.

- Closes the session and returns to real windows system. If your virtual desktop is password protected, you have to enter the password to exit. See **Close the Virtual Desktop** for more details.
- Displayed only if PIN protection is enabled for virtual desktop. Shows the PIN number generated for the current session. This is required for you to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.

#### 4.5.3. Run Browsers inside the Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button
- The virtual desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.

COMODO

- Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer.
- 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 your user-names and passwords without fear of key-loggers recording your keystrokes.

#### Add browser shortcuts inside the virtual desktop

•

- The virtual desktop start menu contains a shortcut to your default browser.
- You can add shortcuts for other browsers as follows:
  - Click 'Settings' > 'Containment' > 'Virtual Desktop Settings'
  - Click the 'Add' button in the applications section:

COMODO Advanced	I Settings ? - $\Box$ ×
✓ General Settings	Virtual Desktop
✓ Antivirus	
✓ Firewall	Request password when exiting Virtual Desktop <u>Create/Change password</u>
✓ HIPS	Launch Virtual Desktop upon user login
— Containment	☑ Protect paused Virtual Desktop session with PIN
Containment Settings	Duration of paused Virtual Desktop session before its automatic termination
Auto-Containment	APPLICATIONS
Protected Objects	
Virtual Desktop	Applications quickly accessible via Virtual Desktop shortcuts or start menu:
✓ File Rating	+ × Cr Add Pamava Reset to
<ul> <li>Advanced Protection</li> </ul>	Add Remove Default
	Application Q Desktop Start Menu
	Running Processes
	C:\Program Files (x86)\Google\Chrome\Applic
	OK CANCEL

- Add a browser as follows:
  - Click 'Add' > 'Applications' > locate the executable file of the browser > click 'OK'.
     OR
  - · Start the browser on the host computer
  - Click 'Add' > 'Running Processes' > locate the browser process > click 'OK'.
- Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut.
- Click 'OK' to save your settings
- Click 'OK' in the 'Advanced Settings' dialog for your changes to take effect

COMODO Creating Trust Online\*

See Add applications to virtual desktop in Virtual Desktop Settings if you need more help on this.

The shortcuts are now available inside the virtual desktop.

#### Run browsers inside virtual desktop

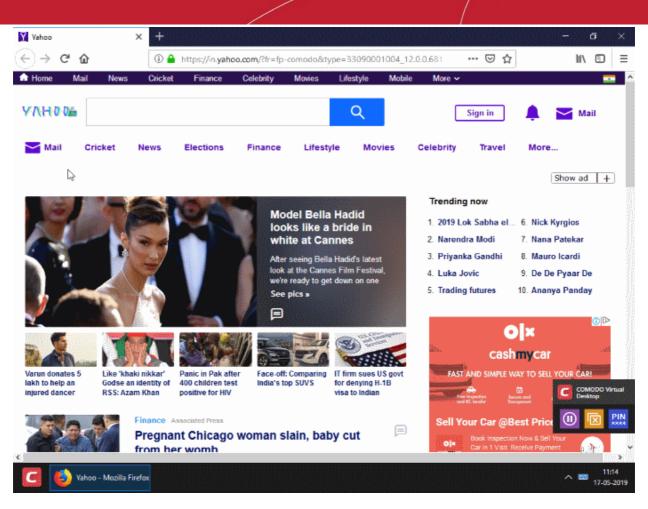
•

· Use the desktop shortcuts or start menu items of the browser that you want to run

C	COMODO Virtual Desktop	
	explorer	
9	Google Chrome	
Ģ	MBFreeAstrologyBirthChart	
٨	firefox	
0	r launcher	
	Pause Virtual Desktop Session	
	Close Virtual Desktop Session	
<b>PIN</b> ****	Show PIN	
C		

The selected browser will open at its home page.

COMODO Creating Trust Online\*



• Your browsing history and other internet activity are not stored on your computer when you close the session.

#### 4.5.4. Open Files and Run Applications inside the Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button

You can use any of the following methods to launch a local program or file in the virtual desktop:

- · Open applications/files from the desktop shortcuts and start menu items
- Navigate to the application/file

#### Desktop shortcuts and start menu items

- The virtual desktop start menu contains a shortcuts to Windows Explorer and your default web browser.
- You can create desktop shortcuts / start menu items which will open your favorite applications in the virtual desktop.
  - Click Settings > Containment > 'Virtual Desktop Settings'
  - Click the 'Add' button in the applications section:

COMODO Creating Trust Online\*

COMODO Advanced Settings ? - □ ×								
<ul> <li>✓ General Settings</li> <li>✓ Antivirus</li> </ul>	Virtual Desktop							
<ul> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>Containment Settings</li> <li>Auto-Containment</li> </ul>	<ul> <li>Request password when exiting Virtual Desktop <u>Create/Change password</u></li> <li>Launch Virtual Desktop upon user login</li> <li>Protect paused Virtual Desktop session with PIN</li> <li>Duration of paused Virtual Desktop session before its automatic termination</li> <li>APPLICATIONS</li> </ul>							
Protected Objects Virtual Desktop	Applications quickly accessible via Virtual Desktop shortcuts or start menu:							
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	+       *       C         Add       Remove       Reset to Default         Applications       Q       Desktop         Running Processes       C:\Windows\explorer.exe       Image: Complex							
	OK CANCEL							

- Add an application as follows:
  - Click 'Add' > 'Applications' > navigate to the file OR
  - Start the application on the host computer
  - Click 'Add' > 'Running Processes'
  - Select the application's process and click 'OK'
- Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut.
- Click 'OK' to save your settings
- Click OK in the 'Advanced Settings' dialog for your changes to take effect
- See Add applications to virtual desktop in Virtual Desktop Settings if you need more help on this.

The shortcuts are now available inside the virtual desktop.

- Use the desktop shortcuts or the start menu items to open the application / file.
- Changes made in the virtual desktop are not be saved to the host system.

#### Navigate to Application / File

Click the 'C' button at bottom-left, then 'explorer'

#### COMODO Creating Trust Online\*

COMODO Virtual Desktop	
explorer	
Google Chrome	
MBFreeAstrologyBirthChart	
🤨 firefox	
launcher	
swriter	
give_a_dog_a_bone	
Pause Virtual Desktop Session	
Close Virtual Desktop Session	
PIN Show PIN	

• Navigate to the application / file and open it. The file will open in the virtual desktop.

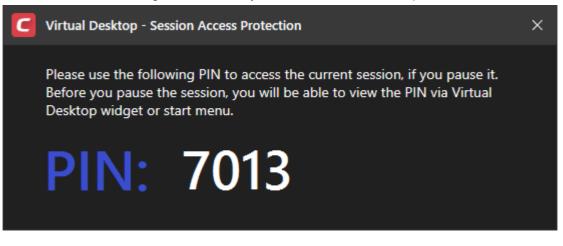
COMODO Creating Trust Online\*

Image: Provide the second	Application Tools MB Free Astrolo	ogy Birth Chart		>
	Cut ■ Copy path Paste shortcut Paste shortcut Copy to • ► Rename Organize	New New New	Edit	Select all Select none Invert selection Select
← → × ↑ 📙 « Prog	gram Files (x86) → MB Free Astrology Birth Chart	~ 0	Search MB Free	Astrology Birt 🔎
old man files \land	Name	Date modified	Туре	Size
Share Suspicious System32	<ul> <li>birthchart</li> <li>Bmp2Jpeg.dll</li> <li>INSTALL</li> </ul>	16-07-2007 07:19 16-07-2000 16:20 12-04-2019 14:05	lcon Application extens Text Document	3 KB 182 KB 4 KB
	MBFreeAstrologyBirthChart	17-03-2010 16:12	Application	3,016 KB
<ul> <li>ConeDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> </ul>	Wnwise	17-03-2010 15:23	Application	500 KB
<ul> <li>Local Disk (C:)</li> <li>5 items</li> <li>1 item selected</li> <li>2.</li> </ul>	94 MB			

• The changes made will not be saved to your real Windows system.

### 4.5.5. Pause and Resume the Virtual Desktop

- You can pause a virtual desktop session and resume it at a later time without data loss.
- If pause PIN protection is enabled, you will need to enter a (randomly generated) 4-digit number to resume the virtual desktop.
  - Other users of the computer cannot resume the paused session without knowing the PIN.
  - The PIN is auto-generated for every session and shown at start up:



- Click 'Show PIN'
   \*\*\*\*\*
   in the start menu / tools box to view the number at any time.
- See Secure virtual desktop sessions with a PIN in Virtual Desktop Settings for more details on configuring PIN protection for virtual desktop

COMODO Creating Trust Online\*

#### Pause a virtual desktop session

• Click the 'Pause' button in the tools box at the bottom-right



Alternatively, click the 'C' button at bottom-left, then 'Pause Virtual Desktop Session'

The session temporarily closes:

C	COMODO Virtual Desktop
12:34	17-05-2019
Curre	nt Session Duration: 00:45:43
$\bigcirc$	Continue Paused Session
	Close Virtual Desktop Session
	Switch to Windows View

- Click 'Switch to Windows View' if you want to open your real Windows system.
- If password protection is enabled, you will be asked to enter the exit password for the virtual desktop.

COMODO Creating Trust Online\*

сомо	DO Enter password	×
Password:		
	OK CAN	ICEL

Enter the password and click 'OK'

The virtual desktop tool box is shown at the bottom-right corner of the screen:

		COMODO V Desktop	îrtual
		<mark>→</mark> ×	<b>PIN</b> ****
누 딸	d)) ENG	12:40 17-05-2019	

The box contains the following controls:

•

- Returns to the paused virtual desktop session



- Closes the paused desktop session. See Close the Virtual Desktop for more details.

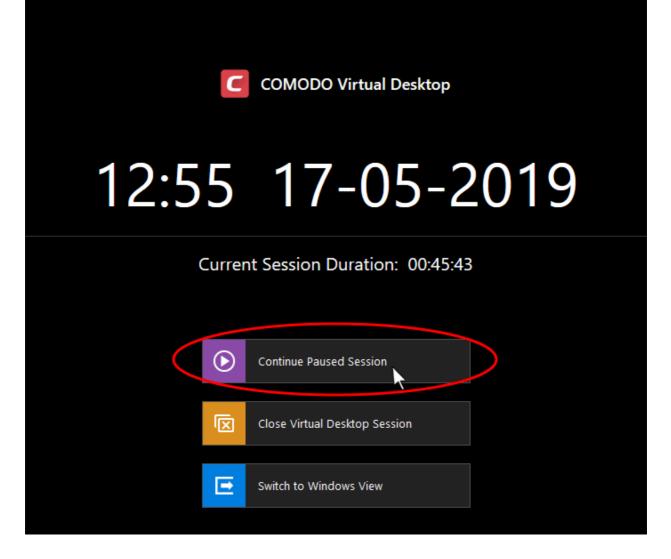


 Only shown if PIN protection is enabled. Click to view the PIN for the current session.

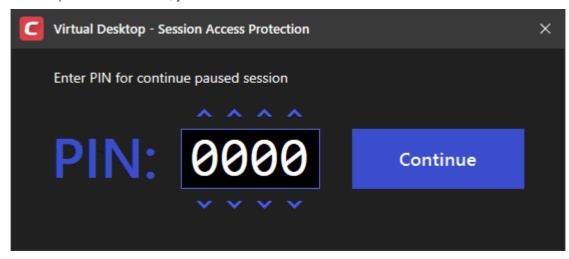
#### Resume a paused virtual desktop session

• Click the return icon the to re-open the virtual desktop:

COMODO Creating Trust Online\*



- Click 'Continue Paused Session'
- If PIN protection is enabled, you will be asked to enter the PIN:

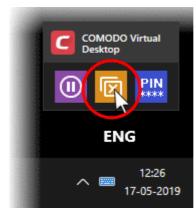


- Enter the PIN you noted down during the start of the session and click 'Continue'
- If PIN protection is not enabled, you will be directly taken to your virtual desktop.

COMODO Creating Trust Online\*

### 4.5.6. Close the Virtual Desktop

· Click the 'Close' button in the tools box at the bottom-right



- Alternatively, click the 'C' button at bottom-left then select 'Close Virtual Desktop Session'.
- You will return to the Virtual Desktop start screen:

C	COMODO Virtual Desktop	
13:30	17-05-2019	
Last	Session Duration: 00:07:09	
	Start Virtual Desktop Session	
	Switch to Windows View	

- Click 'Start Virtual Desktop Session' to open a new session
- Click 'Switch to Windows View' to return to the host desktop
- You will need to enter an exit password if password protection has been enabled:

COMODO

сомо	DO Enter password	×
Password:		
	OK CAN	CEL

- Enter the password and click 'OK'
- The virtual desktop tools box is displayed at the bottom-right corner of your Windows screen.



Click for completely close the virtual desktop

#### Terminate a paused virtual desktop session

When a virtual desktop session is paused, it shows the tools box at the bottom-right of your Windows screen.

	COMODO Virtual Desktop
	ー 宇 ロッ)ENG 12:40 17-05-2019 <b>そ</b>
•	Click to return to the virtual desktop and start a new session
•	Click to completely close the virtual desktop

- Enter password if configured in 'Advanced Settings' > 'Containment' > 'Virtual Desktop' > 'Request password when exiting Virtual Desktop'
- Click 'OK'.

### 4.6. Containment Statistics Analyzer

• Click 'Tasks' > 'Containment Tasks' > 'Containment Statistics Analyzer'

COMODO Creating Trust Online\*

• The containment statistics area lets you view the activities of processes on your computer and those in the container.

#### **Open Containment Statistics Analyzer**

- Click 'Tasks' > 'Containment Tasks'
- Click the 'Containment Statistics Analyzer' tile

COMODO Client - Security 11 -	×
K HOME () SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS ADVANCED TASKS	Q,
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	📌 rtual
Reset the Container Clean container data by erasing all its content.  Watch Activity Open COMODO KillSwitch to monitor advan process and system activity.	,≉ nced
Run Virtual Desktop       Containment Statistics Analyzer         Create a secure virtual desktop and start us       View analysis of Containment events and protect statistics of the component.	>
	?

#### CCS will install the analyzer if it is not yet on your system:

•

Install Required Packages The feature requires installation of a	dditional packages.	
Package Name	License Agreement	Size
Containment Stats Analyzer	View License Agreement	1 MB
By pressing "Agree and Install", you agree with us	er license agreements for all the	packages listed above.
		AGREE AND INSTALL

• Click 'Agree and Install' to download and install the application.

COMODO Creating Trust Online\*

соморо о	lient - Security 11	– ×
	Required Packages ure requires installation of additional packages.	
Installing Contain	iment Stats Analyzer	77 %
		CANCEL

• The main interface opens when installation is complete:

Search 🗙						
SECURED/VALIDATED	)			CONTAINMENT		
YOUR PC						
> All Processes				> All Processes		
<ul> <li>svchost.exe(96)</li> <li>smss.exe(316)</li> </ul>						
<ul> <li>csrss.exe(404)</li> </ul>						
• wininit.exe(472)	FILES	Q	2127		VIRTUAL HD	
<ul> <li>csrss.exe(484)</li> <li>winlogon.exe(560)</li> </ul>	REGISTRY		49377		REGISTRY	
<ul> <li>services.exe(596)</li> <li>lsass.exe(604)</li> <li>svchost.exe(692)</li> </ul>	СОМ	0	32422		COM	۰ (و
<ul> <li>fontdrvhost.exe(704)</li> <li>fontdrvhost.exe(712)</li> </ul>	IMA	0	21294		IMA	• (
<ul> <li>svchost.exe(780)</li> <li>SandboxStat.exe(792)</li> </ul>	APIs	0	325		APIs	•
• dwm.exe(880)						
• svchost.exe(900)						

- · Processes running on your host computer are shown on the left
- Process running in the container are shown on the right.
- Click a process to view its child processes and resource usage:.
  - Files Number of files accessed by the process
  - Registry Number of registry keys accessed by the process
  - COM The inter-process component object model (COM) interfaces used by the process
  - IMA Other processes, to which the selected process performs write operation

COMODO Creating Trust Online\*

APIs - The protected API's accessed by the process

# 5. Advanced Tasks - Introduction

• Click 'Tasks' > 'Advanced Tasks'

•

 Advanced tasks lets you view event logs, manage CCS tasks and to take advantage of several other Comodo utilities.

COMODO Client - Security 11	– ×
🗙 HOME {୍ରି SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Create Rescue Disk Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.	Clean Endpoint * Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager Open the task manager to view running security tasks in progress.	View Active Processes View the details of the processes active on this computer.
View Logs View a record of security events, activity and alerts.	Submit Files         *           You can submit as many files as you wish to COMODO for analysis.
⊄T× SILENT MODE	?

See the following sections to find out more about each feature:

- Create Rescue Disk Burn a bootable ISO that lets you run virus scans in pre-boot environments
- Task Manager Stop, pause and resume currently running CCS tasks like antivirus scans and updates
- Clean Endpoint Deploy Comodo Cleaning Essentials to remove persistent infections from your PC
- View Active Process List Manage processes which are currently running on your PC. Click the 'More' button to open Comodo KillSwitch.
- CCS Logs View the event logs of firewall, antivirus, containment and HIPS modules
- Submit Files Upload unknown/suspicious files to Comodo Valkyrie for analysis

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See 'Password Protection' for more details."

### 5.1. Create a Rescue Disk

• Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk'

Comodo Rescue Disk (CRD) is a bootable disk image that lets you run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system.

COMODO Creating Trust Online\*

It is a powerful virus, spyware and root-kit cleaner which works in both GUI and text mode.

- CRD can eliminate infections that are preventing Windows from booting in the first place.
- It is useful for removing malware which has embedded itself so deeply that regular AV software cannot remove it.
- CRD contains tools to explore files in your hard drive, take screen-shots and browse web pages.
- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk' to download and burn to ISO, CD/DVD, USB or other drive. See Download and Burn Comodo Rescue Disk for a walk-through of this process.

сомодо	Client - Security 11	I		
🗙 номе (ဂ္ဂ်) s	ETTINGS			
🗹 Secure	All systems are a	active and running		
GENERAL TASKS	FIREWALL TASKS	CONTAINMENT TASKS	ADVANCED TASKS	
( ( ) Create	e <b>Rescue Disk</b> a bootable CD o phe y infected	r USB Flash Drive to I PC's.	Clean Endpoint Run COMODO Cleaning Essentials tool persistent infections.	
Open the tasks in	ask Manager	Rescue Disk	View Active Processes ? –	- X
		otable CD/DVD or L e rescue disk ISO imag	USB Rescue Disk ge is required to create a bootable disk.	
	1 [150	Select ISO File (Op If you have already d Otherwise it will be d	<b>ptional)</b> downloaded the ISO file, click here to choose it. downloaded from the internet.	
	2 😥	Select Target Drive Select where the reso writable CD/DVD driv	cue disk should be created e.g. a USB drive or	a
	з ⊳	Start If you have selected t	the target drive, start burning process now.	

After you have burned the ISO, you need to boot your system to the rescue disk. This will open the scanner in your pre-boot environment.

- Change the boot order on your computer http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html
- Start using CRD http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html
- Run scans on your pre-boot environment http://help.comodo.com/topic-170-1-493-5216-Starting-Comodo-Cleaning-Essentials.html and http://help.comodo.com/topic-170-1-493-5217-CCE-Interface.html

### 5.1.1. Download and Burn Comodo Rescue Disk

Click 'Advanced Tasks' on the CCS home screen

COMODO Creating Trust Online\*

Click 'Create	Rescue Disk':	, i		
сомојо	Client - Security 11	I		
< номе {୍ରି s	ETTINGS			
🗹 Secure	All systems are a	active and running		
GENERAL TASKS	FIREWALL TASKS	CONTAINMENT TASKS	ADVANCED TASKS	
(() Create	a bootable CD o	r USB Flash Drive to I PC's.	Clean Endpoint Run COMODO Cleaning Essentials tool to persistent infections.	
Open Ta Open th tasks in	ask Manager	Rescue Disk	View Active Processes ? –	×
		otable CD/DVD or U e rescue disk ISO imag	USB Rescue Disk ge is required to create a bootable disk.	
	1 [[50	Select ISO File (Op If you have already of Otherwise it will be o	<b>ptional)</b> downloaded the ISO file, click here to choose it. downloaded from the internet.	
	2 🝥	Select Target Driv Select where the reso writable CD/DVD driv	scue disk should be created e.g. a USB drive or a	
	з ⊳	Start If you have selected	the target drive, start burning process now.	

The setup screen shows the steps to create a new rescue disk:

#### Step 1- Select the ISO file

Optional. If you have already downloaded the rescue disk ISO from Comodo then please select it here. If you haven't yet downloaded then please ignore this step - it will be downloaded automatically during Step 3.

#### Step 2 - Select target drive

Select the CD/DVD or USB on which you want to burn the rescue disk. You will boot to this disk to run the antivirus product.

#### Burn to CD or DVD

- Label a blank CD or a DVD as "Comodo Rescue Disk Bootable" and load it in your CD/DVD drive.
- Click 'Select Target Drive' in the 'Rescue Disk' then choose the drive in the 'Select Target Drive' dialog
- Click 'OK'

COMODO Creating Trust Online\*

COM	Rescue Disk		?	—	×
() () +	Bootable CD/DVD or USB Rescue Disk The rescue disk ISO image is required to cre	ate a bootable d	isk.		
1 [	Select ISO File (Optional) If you have already downloaded the ISO Otherwise it will be downloaded from the	) file, click here t ne Internet.	o choos	se it.	
2	Select Target Drive Select where the rescue disk should be writable CD/DVD drive.	created e.g. a U	SB drive	or a	>
				-	
	COMODO Select Target Drive		?	×	
	Disk	Туре			
<	D:\	CD\DVD RW Dri	ve		>
	E:\	Removable Disk			
	ок	с	ANCEL		

#### Burn to a USB drive

- Insert a formatted USB stick in a free USB port on your computer
- Click 'Select Target Drive' in the 'Rescue Disk' dialog
- Select the drive from the 'Select Target Drive' dialog and click 'OK'

COMODO Creating Trust Online\*

CON	10D0 Rescue Disk	?	-	×
(© +	Bootable CD/DVD or USB Rescue Disk The rescue disk ISO image is required to create a bootable	e disk.		
1	Select ISO File (Optional) If you have already downloaded the ISO file, click her Otherwise it will be downloaded from the Internet.	e to choo	ose it.	
2	Select Target Drive Select where the rescue disk should be created e.g. a writable CD/DVD drive.	USB driv	e or a	>
	COMODO Select Target Drive	?	×	
	Disk Type			
	D:\ CD\DVD RW	Drive		
<	E:\ Removable D	isk		>
	ок	CANCEL		

#### Step 3 - Burn the Rescue Disk

- Click 'Start'
- If you selected a local ISO in step 1 then burning will start immediately. If not, the ISO will be downloaded from Comodo servers:

COMODO Creating Trust Online\*

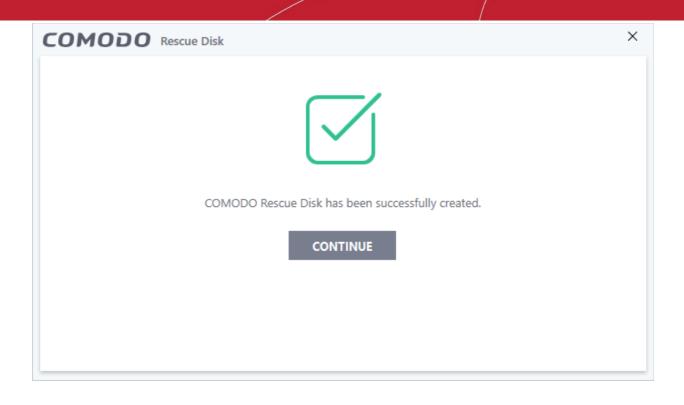
COMODO Client - Security 11	- ×
Install Required Packages The feature requires installation of additional packages.	
Downloading COMODO Rescue Disk	
	CANCEL

After downloading, setup will burn the ISO to your target drive:

isk X
age 79%
$r_{\rm SS}$ is complete , do not eject the CD/DV/D/USB drive early. The CD/DV/D/U

Wait until the write process is complete - do not eject the CD/DVD/USB drive early. The CD/DVD/USB will
be ejected automatically once the burning process is finished.

COMODO Creating Trust Online



Your bootable Comodo Rescue Disk is ready.

• Click 'Continue' to go back to the CCS interface

### 5.2. Remove Deeply Hidden Malware

- Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'
- Comodo Cleaning Essentials (CCE) help users identify and remove malware and unsafe processes from infected computers.

Major features include:

- KillSwitch A system monitoring tool that lets you identify and terminate unsafe processes on your computer.
- **Malware scanner** Fully customizable scanner capable of unearthing and removing viruses, rootkits and malicious registry keys hidden deep in your system.
- Autorun Analyzer Allows you to view and control the services and programs which are loaded when your computer boots-up.

#### Run CCE from CCS interface

- Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'
- If you have already installed Comodo Cleaning Essentials, clicking 'Clean Endpoint' will open the CCE interface directly.
- When you click 'Clean Endpoint' for the first time, CCS will download and install Comodo Cleaning Essentials. After it is installed, clicking this tile in future will open the CCE interface.

COMODO Creating Trust Online\*

Client - Security 11	- ×
🕻 HOME {៊ូ} SETTINGS	
Secure   The virus signature database	s NOT up-to-date
GENERAL TASKS FIREWALL TASKS CONTAINMEN	IT TASKS ADVANCED TASKS
Create Rescue Disk Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.	• Clean Endpoint Run COMODO Cleaning Essentials tool to clean persistent infections.
COMODO Client - Security 11 Install Required Packages The feature requires installation of ac	- × Iditional packages.
Package Name	License Agreement Size p
COMODO Cleaning Essentials	View License Agreement 7 MB
	(7)
By pressing "Agree and Install", you agree with us	er license agreements for all the packages listed above.
	AGREE AND INSTALL

- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.

COMODO Creating Trust Online\*

COMODO Client - Security 11	-	×
Install Required Packages The feature requires installation of additional packages.		
Installing COMODO Cleaning Essentials	50 %	
	CANCE	L

After installation, the Comodo Cleaning Essentials application will open:



See http://help.comodo.com/topic-119-1-328-3525-The-Main-Interface.html if you'd like more information on

COMODO Creating Trust Online\*

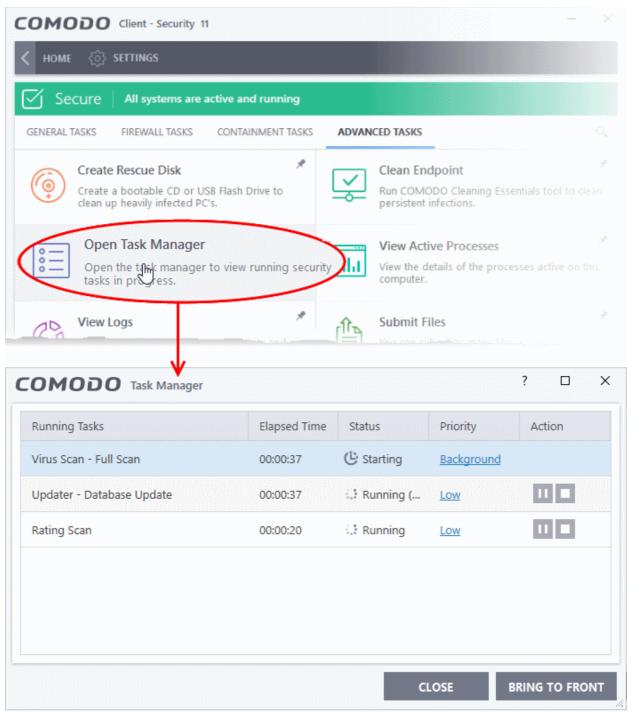
using Comodo Cleaning Essentials.

### 5.3. Manage CCS Tasks

- Click 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'
- · Comodo Client Security can run several tasks simultaneously.
- · For example, virus scans and virus signature database updates can run concurrently.
- The 'Task Manager' interface lets you view all currently running tasks.

#### Open the task manager

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'Open Task Manager'



COMODO Creating Trust Online\*

From the 'Task Manager' interface, you can:

- Reassign task priorities to the tasks
- · Pause, resume, or stop a running task
- Bring a selected task to foreground

#### **Reassign task priorities**

The 'Priority' column show the level of resources committed to the task at run. A higher priority means the task runs more smoothly, but consumes more system resources.

#### Change the priority of a task

· Click the current priority and select the new one you want to assign:

Running Tasks	Elapsed Time	Status	Priority	Action	
Rating Scan	00:01:27	😳 Running	Low		
Virus Scan - Full Scan	00:01:23	🕒 Starting	Low High		
Updater - Database Update	00:01:23	🐮 Running (	Normal Low Backgroun	d	
			LOSE B	RING TO FRO	

#### Pause/resume or stop running tasks

•

Use the buttons in the action column to pause, resume or stop a process:

Click the 'Pause' button to temporarily stop a running task

(	Task Manager				?	×
	Running Tasks	Elapsed Time	Status	Priority	Action	
	Virus Scan - Full Scan	00:02:09	II Paused	Normal		
	Virus Scan - C:\install	00:01:58	ំ Running (	Background		

Click the 'Resume' button to restart a suspended task

COMODO Creating Trust Online\*

OMODO Task Manager				?
Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	II Paused	Normal	
Virus Scan - C:\install	00:01:58	🔅 Running (	Background	

· Click the 'Stop' button to terminate a running task

OMODO Task Manager				?
Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	II Paused	Normal	
Virus Scan - C:\install	00:01:58	🕄 Running (	Background	

#### Bring a running task to the foreground

· To view the progress of a background task, select the task and click 'Bring to Front'

C	Task Manager				?		×
	Running Tasks	Elapsed Time	Status	Priority	Acti	ion	
	Rating Scan	00:04:00	🔅 Running (	Normal			
	Virus Scan - Full Scan	00:03:55	🕒 Starting	Low			
	Updater - Database Update	00:03:54	🔅 Running (	Background	П		
			CI	.OSE	BRING	to froi	NT

COMODO Creating Trust Online\*

### 5.4. View CCS Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- CCS logs all events generated by the antivirus, firewall, HIPS, containment and other modules.

#### Open the log viewer

- Click 'Tasks' on the CCS home screen.
- Click 'Advanced Tasks' then 'View Logs':

COMODO Client - Security 11	– ×
K HOME کې settings	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS ADVAN	
Create Rescue Disk Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.	Clean Endpoint Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager Open the task manager to view running security tasks in progress.	View Active Processes * View the details of the processes active on this computer.
View Logs View a record for security events, activity and alerts.	Submit Files You can submit as many files as you wish to COMODO for analysis.
	(?

• Alternatively, right-click on the CCS tray icon and select 'View Logs'.

The logs dashboard contains a summary of recorded events:

COMODO Creating Trust Online\*

COMODO View Log	gs - Ent	ire period				?			>
SHOW Events Summary		Filter by Date and Time	🖬 Open log file	K Cleanup log file	C) Refresh				
SECURITY EVENTS		4	PROTECTION						
			Infections pr	evented:					89
			Unknown pro	ograms detect	ed:				371
67.0%			Suspicious a	ctivities blocke	d:				18
			Network activities blocked:					146	
				UP OF UNKNO	WN FILES				
10.2% 14.9%			Good files de	etected:					7
	<b>0.1</b> %	7.7%	Bad files det	ected:					6
<ul> <li>Antivirus Events</li> </ul>			Submitted fil	es:					(
<ul> <li>HIPS Events</li> </ul>			UPDATES						
Containment Events			Last update:			5/31/2	2019 11	1:21:04	AM
<ul><li>VirusScope Events</li><li>Firewall Events</li></ul>			Program version:			11.2.2.737			
								CLOSE	

- Use the drop-down at top-left to view a specific type of log.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs

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

'Logs per Module':

- Antivirus
- VirusScope
- Firewall
- HIPS
- Containment

'Other Logs':

- Device control
- Autorun events
- Alerts displayed
- Tasks launched
- File List settings changes
- Vendors List changes
- Configuration changes

COMODO Creating Trust Online\*

#### Virtual Desktop events

### 5.4.1. Antivirus Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Antivirus Events' from the 'Show' drop-down
- CCS documents all antivirus actions in extensive but easy to understand logs.
- Each log contains stats about scanned objects, the settings used for each task, and a history of actions performed on individual files.
- Logs are also recorded for real-time protection events, antivirus database updates and more.

#### View the 'Antivirus' Logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Antivirus Events' from the 'Show' drop-down:

SHOW Antivirus Events	<ul> <li>Advanced Filter b</li> </ul>	<b>_</b>	log file Cleanu	י <b>ב</b> וplog <sub>בעתר</sub>		
Date & Location	Malware Name	Action	Status	Alert	Activities	'
11/11/20 C:\Suspicious File	. Application.Win32.Le	Ignore	Success	Related alert		
11/11/20 📄 C:\Suspicious File	. Application.Win32.Le	Quarantine	Success	Related alert		
11/11/20 🗋 C:\Suspicious File	. Application.Win32.Le	Ignore	Success	Related alert		
11/11/20 🗋 C:\Suspicious File	. Application.Win32.Le	Ignore	Success	Related alert		
11/11/20 📋 C:\Suspicious File	. Application.Win32.Le	Quarantine	Success			
11/11/20 📄 C:\Suspicious File	. Application.Win32.Le	Quarantine	Success			
11/11/20 🗋 C:\Program Files	Malware@#3ri4ye99	Quarantine	Success	Related alert		
11/11/20 📄 C:\Program Files	Malware@#2nm567u	Quarantine	Success	Related alert		
11/11/20 🗋 C:\Program Files	Malware@#1i04f6cq	Quarantine	Success	Related alert		

- Date & Time When the event occurred.
- Location The installation path of the suspicious application
- Malware Name The malicious item that was detected
- Action How the malware was handled by CCS.
- Status Whether the action taken was a success or failure
- Alert Click 'Related Alert' to view the notification generated by the event

Note: Alerts are only shown if 'Do not Show Antivirus Alerts' is disabled in 'Settings' > 'Antivirus' > 'Real-time Scan'.

Creating Trust Online

#### See Real-time Scan Settings for more details.

- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs
- · Click any column header to sort the entries in ascending \ descending order

#### 5.4.1.1. Filter Antivirus Logs

Filters allow you to view a specific sub-set of logs.

You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters:**

• Click 'Filter by Date and Time' to view logs for a specific time period:

COMODO View Logs - Tod	ay				?	-		$\times$
SHOW Antivirus Events	<b>⊤</b> Advanced Filter	Tilter by Date and Time	Gen log file	X Cleanup log file		<b>₽</b> (port	t) Refres	h
Date & Location	Malware Name	<ul> <li>(No filterin</li> <li>Within las</li> <li>Except las</li> <li>Today</li> <li>Current w</li> <li>Current m</li> <li>Within the 07/31/</li> </ul>	t <u>1</u> st <u>1</u> eek nonth period of	<ul> <li>hour(s)</li> <li>hour(s)</li> <li>hour(s)</li> </ul>	¥	Activiti	es	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- · Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

COMODO Creating Trust Online\*

омо	DO View Log	gs - Curren	it week		
SHOW Antivirus Ev	rents	٠	<b>⊤</b> Advanced Filter	Filter by Date and Time	Open I
Date &	Location	Malware	Name	Action	Status
4/11/201	D:\Suspic	Virus.Wir Refres	132.Parite.a	Remove	Succes
4/11/201	D:\Suspic	Show	advanced filter	gnore	Succes
4/11/201	D:\Suspic	Export		lock	Succes
		Curre	nt week nt month period		

Having chosen a **preset time filter**, you can further refine which events are shown by using the following additional parameters:

- Action Events according to the response (or action taken) by the antivirus
- Location Displays only events logged from a specific location
- Malware Name Displays only those events that reference a specific piece of malware
- Status Show events according to whether the logged action was successful or not. Status options are 'Success' or 'Fail'.

#### Configure advanced filters for antivirus events

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply the filter:

COMODO Creating Trust Online\*

COMODO View Logs	- Current week				? —	
SHOW Antivirus Events	T Advanced Filter	Filter by Date and Time	Copen log file	¥ Cleanup log file	Export	
Date &    Location	Malware Name	Action	Status	Alert	Activities	
4/11/201 D:\Suspici	Virus Win32.Parite.ge	Remove	Success	Related alert		
4/11/201 D:\Suspici	Virus.Win32.Parite.ge	Ignore	Success	Related alert		
4/11/201 D:\Suspici	.Unclassified Malware	Block	Success			
COMODO Advanced Filt	ter				?	×
ADVANCED FILTER Action Action	Add					
Location Malware Name						
Status						
				APPLY	CANCEL	

There are four categories of filters you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. Action: The 'Action' option allows you to filter logs based on the action taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

Creating Trust Online\*

COMODO Advanced Filter		1	? ×
ADVANCED FILTER Action	<b>H</b> Add		
Action Equal 💌			$\otimes$
Quarantine	Remove	Ignore	
Detect	Ask	Restore	
Block	Reverse	False positive	
Add to exclusions	Add to trusted files	Restore from Quarantine	
Delete from Quarantine			
		APPLY	CANCEL

You should now choose the actions by which you want to filter the logs:

- a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
- Quarantine: Displays events at which the user chose to quarantine a file
- · Remove: Displays events at which the user chose to delete the detected threat
- Ignore: Displays events at which the user chose to ignore the detected threat
- · Detect: Displays events involving only the detection of malware
- Ask: Displays events where an alert was shown to the user so they could choose an action against a piece
  of detected malware
- · Restore: Displays events at which guarantined applications were restored
- · Block: Displays event where suspicious applications were blocked
- · Reverse: Displays events where VirusScope reversed potentially malicious actions
- False positive: Displays events where files flagged as threats by CCS were submitted to Comodo by the user as a false positive.
- Add To exclusions: Displays events in which the user chose to add an item to antivirus exclusions
- · Add To trusted files: Displays events in which the user changed the file rating to 'Trusted'

For example, if you check the 'Quarantine' box then select 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

- · Restore from Quarantine: Displays events in which files were restored from quarantine
- Delete from Quarantine: Displays events in which files were deleted from quarantine
- ii. Location: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.

COMODO Creating Trust Online\*

COMODO Advanced Filter	? ×
ADVANCED FILTER Add	
Location Contains C:\Program Files\	$\otimes$
APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field
- b. Enter the text or word that needs to be filtered

For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:/Program Files/' in the text field, then all events containing the entry 'C:/Program Files/' in the 'Location' field will be displayed. If you select the 'Does Not Contain' option from the drop-down field and enter the phrase 'C:/Program Files/' in the text field, then all events that do not have the entry 'C:/Program Files/' will be displayed.

iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.

обомо	Advanced Filter	? ×
ADVANCED FILTER Malware Name	+ Add	
Malware Name	Contains  Contains Does Not Contain	×
		APPLY CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and type 'siins' in the text field, then all events with 'siins' in the 'Malware Name' field will be shown. If you choose 'Does Not Contain' and type 'siins', then all events that do not have 'siins' in the 'Malware Name' field will be shown.

iv. Status: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter			? ×
ADVANCED FILTER Status	+ Add		
Status Equal ▼ Equal Not Equal	☑ Success	☐ Failure	$\otimes$
		APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
- Success: Displays events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined)
- Failure: Displays events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

• Click 'Apply' for the filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

### 5.4.2. VirusScope Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'VirusScope Events' from the 'Show' drop-down

Event logs are created whenever VirusScope blocks or reverses a suspicious activity.

#### View VirusScope Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- · Click the 'Show' drop-down at top-left
- Select 'VirusScope Events':

COMODO Creating Trust Online\*

HOW /irusScope	Events •	<b>▼</b> Advanced Filter	Image: Filter by Date and Time	Gpen log file	X Cleanup log file	Export	🗘 Refresh
Date &	Location	Malware Name	Action	Statu	s Alert	Activiti	ies
5/27/201	C:\Suspicious\vt	Generic.Infector.5	Quarar	tine Succe	255		
5/27/201	C:\Suspicious\vt	Generic.Infector.5	Reverse	e Succe	255		
5/27/201	C:\Suspicious\vt	Generic.Infector.5	Detect	Succ	255	Proces	s Activities

- Date & Time When the event occurred.
- Location The installation path of the suspicious application
- Malware Name The malicious item that was detected
- Action How VirusScope handled the malware.
  - Reverse VirusScope attempted to undo any changes made by the malicious item
  - Quarantine VirusScope placed the suspicious file in quarantine
  - **Detect** VirusScope observed malicious activity, but did not quarantine the file or reverse its changes
  - **Ask** VirusScope detected malicious activity and showed an alert. The alert asks whether you want to quarantine the file or reverse its changes
- Status Whether the action taken was a success or failure
- Alert Click 'Related Alert' to view the notification generated by the event

**Note**: VirusScope alerts are only shown if 'Do not show pop up alerts' is disabled in 'Settings' > 'Advanced Protection' > 'VirusScope'.

See VirusScope Configuration for more details.

Application Activities	PID	Data	Ŷ
🗊 🖻 vt.exe	7040		
📽 Load image file		C:\Windows\System32\apphelp.dll	
📽 Load image file		C:\Windows\apppatch\sysmain.sdb	
📽 Load image file		C:\Windows\System32\imm32.dll	
📽 Load image file		C:\Windows\System32\oleaut32.dll	
📽 Load image file		C:\Windows\System32\guard64.dll	
📽 Load image file		C:\Windows\System32\version.dll	
🦸 Load image file		C:\Windows\System32\cmdvrt64.dll	
			~

- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- Open log file Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs
- · Click any column header to sort the entries in ascending \ descending order

### 5.4.2.1. Filter VirusScope Logs

Filters allow you to view a specific sub-set of logs.

The following types of filters are:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters:**

• Click 'Filter by Date and Time' to view logs for a specific time period:

Creating Trust Online\*

COMODO View Logs - Curr	ent week				?	-		×
SHOW VirusScope Events	<b>⊤</b> Advanced Filter			X Cleanup log file	up log Evport		C Refresh	
Date & Location	Malware Name	<ul> <li>(No filterin</li> <li>Within last</li> <li>Except las</li> <li>Today</li> <li>Current we</li> <li>Current me</li> <li>Within the</li> <li>07/31/2</li> </ul>	t 1 eek onth	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√ hour(s)</li> </ul>	~	Activiti	25	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

Date &	Location	Malware Name	Action	Status
4/10/201	C:\Userc\	Generic Infector 4 Refresh	Ignore	Success
4/10/201	C:\Use	Show advanced filter	Ask	Success
4/10/201	C:\Use	Export Today	Detect	Success
4/10/201	C:\U5e	Current week Current month	Reverse	Success
4/10/201	C:\Use	Entire period	Quarantine	Success

#### To configure Advanced Filters for VirusScope events

Having chosen a **preset time**, you can further refine which events are shown by using the following additional parameters:

- Action Displays events according to the response (or action taken) by the VirusScope
- Location Displays only the events logged from a specific location
- Malware Name Displays only those events that reference a specific piece of malware
- Status Show events according to whether the logged action was successful or not. Status options are

COMODO Creating Trust Online\*

'Success' or 'Fail'.

#### **Configure advanced filters**

- Click the 'Advanced Filter' button on the title bar.
- · Select the filter you want then click 'Add' to apply the filter:

COMODO View L	ogs - Current week				?	-	
SHOW VirusScope Events	▼ Advance Filter	d Filter by Date and Time	Open log file	X Cleanup log file			
Date & Location	Malware Name	Action	Status	Alert	Act		
COMODO Advance	d Filter					?	×
ADVANCED FILTER Action Action	Add						
Location Malware Name							
Status							
				APPLY		CANCE	

There are four categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

i. **Action**: The 'Action' option allows you to filter logs based on the actions taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

COMODO Creating Trust Online\*

COMODO Advanced Filter		1	Y X
ADVANCED FILTER Action	+ Add		
Action Equal			$\otimes$
Quarantine	Remove	Ignore	-
Detect	Ask	Restore	
Block	Reverse	Add to trusted files	
Restore from Quarantine	Delete from Quarantine		
		APPLY CAN	ICEL

- a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b. Now select the check boxes of the specific filter parameters to refine your search. The parameter available are:
  - · Quarantine: Displays events at which the user chose to quarantine a file
  - · Remove: Displays events at which the user chose to delete the detected threat
  - · Ignore: Displays events at which the user chose to ignore the detected threat
  - · Detect: Displays events involving only the detection of malware
  - Ask: Displays events where an alert was shown to the user so they could choose an action against a
    piece of detected malware
  - Restore: Displays events at which guarantined applications were restored
  - Block: Displays event where suspicious applications were blocked
  - · Reverse: Displays events where VirusScope reversed potentially malicious actions
  - Add to trusted files: Displays events in which the user changed the file rating to 'Trusted'

For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

- · Restore from Quarantine: Displays events in which files were restored from quarantine
- Delete from Quarantine: Displays events in which files were deleted from quarantine
- ii. Location: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.

COMODO Creating Trust Online\*

COMODO Advanced Filter		?	×
ADVANCED FILTER Add			
Location Contains C:\Program Files\			$\otimes$
APPLY	c		L

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and type 'C:/Program Files/' in the text field, then all events with 'C:/Program Files/' in the 'Location' field will be shown. If you choose 'Does Not Contain' and type 'C:/Program Files/', then all events that do not have 'C:/Program Files/' in the 'Location' field will be shown.

iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.

сомодо	Advanced Filter				?	×
ADVANCED FILTER Malware Name	•	+ Add				
Malware Name	Contains Contains Does Not Contain	•	cuckoo		(	$\otimes$
				APPLY	CANCEL	

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Malware Name' field will be displayed. If you choose the 'Does Not Contain' option from the drop-down and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Malware Name' field will be displayed.

iv. Status: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter		? ×
ADVANCED FILTER Status	+ Add	
Status Equal • Equal Not Equal	Success Failure	$\otimes$
	APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
- Success: Displays events where the actions against the detected threat were successful. For example, the malware was successfully quarantined.
- Failure: Displays events where the intended actions against the detected threat were not successful. For example, the malware was not disinfected.

**Note:** Multiple filters can be added in the 'Advanced Filter' pane. After adding a filter, select the next filter type and click 'Add'. You can remove filters by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the VirusScope log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

## 5.4.3. Firewall Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- · Select 'Firewall Events' from the 'Show' drop-down
- Comodo Client Security records all actions taken by the firewall.
- Firewall events are created for various reasons. Reasons include when a process attempts a connection that breaks a **firewall rule**, or when there is a change in firewall settings.

#### View Firewall Logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Firewall Events' from the 'Show' drop-down:

HOW Firewall Events	۲	<b>⊤</b> Advanced Filter	Filter b and 1	y Date	pen log file	X Cleanup log file	<b>E</b> xport	C) Refresh
Date Application	Action	Direction	Protocol	Sour	Source	Destin	Destinati	Alert
4/10/ 🥹 C:\Program	Asked	Out	ТСР	127.0	49711	127.0.0.1	49710	Related alert
4/10/ 🥹 C:\Program	Blocked	Out	ТСР	127.0	49709	127.0.0.1	49708	
4/10/ 🥹 C:\Program	Asked	Out	ТСР	127.0	49709	127.0.0.1	49708	Related alert
4/10/ 💽 C:\Program	Asked	Out	ТСР	10.0.2	49702	91.212	80	Related alert
4/10/ 🥹 C:\Program	Asked	Out	ТСР	127.0	49689	127.0.0.1	49688	Related alert
4/10/ 🥥 C:\Program	Asked	Out	ТСР	10.0.2	49685	92.242	80	Related alert

- Date & Time When the event occurred.
- Application The name of the program or process that caused the event.
- Action How the firewall reacted to the connection attempt. For example, whether the attempt was allowed, blocked o r an alert displayed.
- Direction Whether the connection attempt was inbound or outbound.
- **Protocol** The connection method that the application attempted to use. This is usually TCP/IP, UDP or ICMP, which are the most heavily used networking protocols.
- **Source IP** The address of the host from which the connection attempt was made. For outbound connections, this is usually the IP address of your computer. For inbound connections, it is usually the IP address of the external server.
- Source Port The port number that the source host used to make the connection attempt
- **Destination IP** The address of the host to which the connection attempt was made. For inbound connections, this is usually the IP address of your computer.
- Destination Port The port number on the destination host which the source tried to connect to.
- Alert Click 'Related Alert' to view the notification generated by the event

**Note**: Firewall alerts are only shown if 'Do not show pop up alerts' is disabled in 'Settings' > 'Firewall' > 'Firewall' Settings'.

See General Firewall Settings for more details.

- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order

COMODO Creating Trust Online\*

### 5.4.3.1. Filter Firewall Logs

Filters allow you to view a specific sub-set of logs.

The following types of filters are available:

- Preset Time Filters
- Advanced Filters

Preset Time Filters:

• Click 'Filter by Date and Time' to view logs for a specific time period:

сом	DDO View Lo	gs - Currer	nt week				?	—		$\times$
SHOW Firewall E	vents	v	<b>⊤</b> Advanced Filter	Filter by Date and Time	Gen log file	X Cleanup log file		<b>e</b> port	C) Refres	h
Date	Application	Action	Direction	<ul> <li>(No filterin</li> <li>Within last</li> <li>Except last</li> <li>Today</li> <li>Current weight</li> <li>Current minimum</li> <li>Within the</li> <li>07/31/2</li> </ul>	t 1 t 1 eek onth period of	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√ hour(s)</li> </ul>	v v	stinati	Alert	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

Date	Application		Action	Direct	ion	Protocol	
11/21/	Window	/s O	Allow	In	1	UDP	10
11/21/	Wir	Refres Show	sh advanced	filter		UDP	10
		Expor	t				
	/	Today	/				
	(	Curre	nt week				
		Curre	nt month	)			
		Entire	period				

COMODO Creating Trust Online\*

### **Advanced Filters**

Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for 'Firewall' logs and their meanings:

- Action Displays events according to the response (or action taken) by the firewall
- Application Displays only the events propagated by a specific application
- · Destination IP Displays only the events with a specific target IP address
- Destination Port Displays only events that involved a specific target port number
- Direction Displays only the events of Inbound or Outbound nature
- Protocol Displays only events that involved a specific protocol
- · Source IP address Displays only the events that originated from a specific IP address
- Source Port Displays only events that involved a specific source port number

#### Configure advanced filters for firewall events

- · Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply the filter:

COMODO View Logs - C						? -	-
	current week			_	_		
SHOW	( 〒						
Firewall Events	Advance     Filter	d Filter b	y Date Time	)pen log file			
Date Application Act	tion Direction	Protocol	Sour	Source	Destin	Destinati	
		7.00	107.0	40744	107.0.0.1		
4/10/ 🥮 C:\Program Asl	ked Dut	TCP	127.0	49711	127.0.0.1		
COMODO Advanced Filter	-					?	×
ADVANCED FILTER	+						
Action	Add						
Action							
Application							
Destination IP							
Destination Port							
Direction							
Protocol							
Source IP							
Source Port							
				_			
					APPLY	CANC	EL

There are 8 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in

COMODO

the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. Action: Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

COMODO Advanced Filter		? ×
ADVANCED FILTER Action	+ Add	
Action Equal	Blocked Asked	$\otimes$
	APPLY	CANCEL

You should now choose the actions by which you want to filter the logs:

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
- Blocked: Displays events where CCS prevented the connection
- Allowed: Displays events where the connection was allowed to proceed
- Asked: Displays events where an alert was shown to the user so they could choose whether or not to allow the connection
- ii. Application: Selecting the 'Application' option displays a drop-down box and text entry field.

COMODO Advanced Filter	?	2	×
ADVANCED FILTER Add			
Application Contains		$\otimes$	
APPLY	CAN	CEL	

COMODO Creating Trust Online\*

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box.
- b. Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' from and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you select 'Does Not Contain' and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

iii. Destination IP: Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.

COMODO Advanced Filter				?	×
ADVANCED FILTER Destination IP	<b>∔</b> Add				
Destination IP Equal	<ul><li>▼</li></ul>	2.168.111.11	IPv4 IPv6		$\otimes$
			APPLY	CANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Select 'IPv4' or 'IPv6' from the drop-down box.
- c. Enter the IP address of the destination server or host, to filter the events that involve the connection attempts from/to that destination server or host.

For example, if you choose 'Contains' option from the drop-down, select IPv4 and enter 192.168.111.11 in the text field, then all events containing the entry '192.168.111.11' in the 'Destination IP' column will be displayed.

iv. Destination Port: Selecting the 'Destination Port' option displays a drop-down box and text entry field.

COMODO Creating Trust Online\*

сомодо	Advanced Filter	? ×
ADVANCED FILTER Destination Port	+ Add	
Destination Port	Equal   Equal  Greater Than  Greater Than Or Equal  Less Than  Less Than Or Equal  Not Equal	
		APPLY CANCEL

- a. Select any one of the option the drop-down:
- Equal
- Greater than
- Greater than or Equal
- Less than
- Less than or Equal
- Not Equal
- b. Now enter the destination port number in the text entry field.

For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

v. **Direction:** Selecting the 'Direction' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

сомор	Advanced Filte	r				?	×
ADVANCED FILTE Direction		•	<b>∔</b> Add				
Ec	qual qual ot Equal	•	🗹 In	D Out			$\otimes$
					APPLY	CANCE	iL

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the check box of the specific filter parameters to refine your search. The parameter available

COMODO Creating Trust Online\*

are:

- In: Displays a list of events involving inbound connection attempts
- Out: Displays a list of events involving outbound connection attempts

For example, if you choose 'Equal' option from the drop-down and select the 'In' checkbox, then all inbound connection attempts will be displayed.

i. **Protocol:** Selecting the 'Protocol' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

сомо	DO Advance	ed Filter				? ×
ADVANCED F	FILTER	•	<b>∔</b> Add			
Protocol	Equal Equal Not Equal	•	TCP IPv4 PUP ICMPv6	UDP IGMP IDP ND	☐ ICMP ☐ GGP ☐ IPv6	$\otimes$
					APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
  - TCP
  - UDP
  - ICMP
  - IPV4
  - IGMP
  - GGP
  - PUP
  - IDP
  - IPV6
  - ICMPV6
  - ND

For example, if you choose 'Equal' option from the drop-down and select the 'TCP' checkbox, then all connection attempts involving TCP protocol will be displayed.

vii. Source IP: Selecting the 'Source IP' option displays two drop-down boxes and a set specific filter parameters that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter		?	×
ADVANCED FILTER Source IP	+ Add		
Source IP Equal	<ul> <li>▼ 192.168.111.22</li> <li>IPv4</li> <li>IPv4</li> <li>IPv6</li> <li>IPv6</li> </ul>		$\otimes$
	APPLY	CANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Select 'IPv4' or 'IPv6' from the drop-down box.
- a. Enter the IP address of the source server or host, to filter the events that involve the connection attempts from/to that source server or host system.

For example, if you choose 'Contains' then select IPv4 and enter 192.168.111.22 in the text field, then all events containing the entry '192.168.111.11' in the 'Source IP' column will be displayed.

viii. **Source Port:** Selecting the 'Status' option displays a drop-down box and a set specific filter parameters that can be selected or deselected.

бомо	O Advanced Filter		? ×
DVANCED FILT ource Port	ER	<b>∔</b> Add	
Source Port	Equal Equal Greater Than Greater Than Or Equ Less Than Less Than Or Equal Not Equal	▼         8080           al	
		А	PPLY CANCEL

- a. Select any one of the following option the drop-down box.
  - Equal
  - Greater than
  - Greater than or Equal
  - Less than
  - Less than or Equal

COMODO Creating Trust Online\*

#### Not Equal

b. Now enter the source port number in the text entry field.

For example, if you choose 'Equal' and enter 8080 in the text field, then all events containing the entry '8080' in the 'Source Port' column will be displayed.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

## 5.4.4. HIPS Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'HIPS Events' from the 'Show' drop-down
- HIPS events are generated for various security reasons. These include changes in HIPS settings, when an application attempts to access restricted areas, or when an action contravenes your HIPS rulesets.

#### View 'HIPS' Logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'HIPS Events' from the 'Show' drop-down:

•	<b>⊤</b> Advanced Filter	Filter by Date and Time	)pen log file	X Cleanup log file	Export	🗘 Refresh
Application		Action	Target		Alert	
☆ C:\Bistone\Hote	l Management	Direct Keyboar				
C:\Users\giri1\A	ppData\Local\	Terminate Proc	🗋 C:\l	Jsers\ \App[	Data\	
C:\Bistone\Hote	l Management	Direct Keyboar				
C:\Users\giri1\A	ppData\Local\	Terminate Proc	📄 C:\l	Jsers\ \App[	Data\	
C:\Users\giri1\A	ppData\Local\	Terminate Proc	🗋 C:\l	Jsers\ \App[	Data∖	
ۏ C:\Program File	s (x86)\Mozilla	. Terminate Proc	📄 C:\F	Program Files (x8	36)\	
C:\Bistone\Hote	l Management	Direct Keyboar				
C:\Users\giri1\A	ppData\Local\	Terminate Proc	📄 C:\l	Jsers\ \App[	Data\	
C:\Windows\Sys	stem32\Open	Direct Keyboar				
	Application C:\Bistone\Hote C:\Users\giri1\A C:\Bistone\Hote C:\Users\giri1\A C:\Users\giri1\A C:\Users\giri1\A C:\Users\giri1\A C:\Users\giri1\A C:\Bistone\Hote C:\Users\giri1\A	Advanced Filter  Application  C:\Bistone\Hotel Management  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Bistone\Hotel Management  C:\Bistone\Hotel Management  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\  C:\Users\giri1\AppData\Local\	Advanced       Filter by Date and Time         Application       Action         Action       Direct Keyboar         C:\Bistone\Hotel Management       Direct Keyboar         C:\Users\giri1\AppData\Local\       Terminate Proce         C:\Users\giri1\AppData\Local\       Terminate Proce	Advanced       Filter by Date and Time       Open log file         Application       Action       Target	Advanced Filter       Filter by Date and Time       Open log file       Cleanup log file         Application       Action       Target         C:\Bistone\Hotel Management       Direct Keyboar       C:\Users\giri1\AppData\Local\       Terminate Proc       C:\Users\ \Appl         C:\Users\giri1\AppData\Local\       Terminate Proc       C:\Users\ \Appl	Advanced Filter by Date Open log file Cleanup log Export     Application Action Target Alert     Application Action Target Alert     C:\Bistone\Hotel Management Direct Keyboar C:\Users\ \AppData\     C:\Users\giri1\AppData\Local\ Terminate Proc C:\Users\ \AppData\

- Date & Time When the event occurred.
- Application The name of the program or process that caused the event.
- · Action The activity of the application and how HIPS handled it
  - If the action was allowed to proceed then this column will show the result of that action.
  - Click the 'Related Alert' link to see the notification that was shown at the time.
  - This column will state 'Block File' if the action was not allowed.
- **Target** Location of the file, COM interface or registry key accessed by the process.
- Alert Click 'Related Alert' to view the notification generated by the event

**Note**: Alerts are only shown if 'Do not pop-up alerts' is disabled in 'Settings' > 'HIPS Configuration > 'HIPS Settings'. See **HIPS Settings** for more details.

- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- · Refresh Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order

## 5.4.4.1. Filter HIPS Logs

Filters allow you to view a specific sub-set of logs:

- Preset Time Filters
- Advanced Filters

Preset Time Filters:

• Click 'Filter by Date and Time' to view logs for a specific time period:

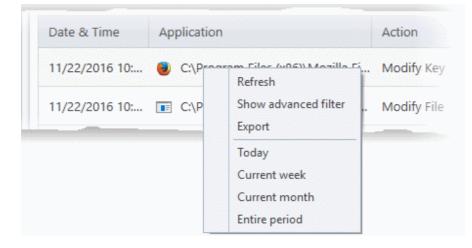
COMODO View Logs - Curren	t week				?	-		$\times$
SHOW HIPS Events	<b>⊤</b> Advanced Filter	5 Filter by Date and Time	Copen log file	X Cleanup log file	Export		C) Refres	h
Date & Time Application		<ul> <li>(No filtering</li> <li>Within last</li> <li>Except last</li> <li>Today</li> <li>Current we</li> <li>Current mode</li> <li>Within the point</li> <li>07/31/2</li> </ul>	1 t 1 eek onth period of	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√ hour(s)</li> </ul>		Alert		

- **No filtering** Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.



- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.



#### **Advanced Filters**

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. Following are available filters for HIPS logs and their meanings:

- Application Displays only the events propagated by a specific application
- Action Displays events according to the response (or action taken) by HIPS
- Target Displays only the events that involved a specified target application

#### Configure advanced filters for HIPS events

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply the filter:

COMODO Creating Trust Online\*

COMODO View Logs - Current week	? —
SHOW HIPS Events	Open log file Cleanup log Export
Date & Application Action	Target
4/11/201 COMODO\COMODO Inte Direct Disk Access	<b>\??\ide#cdromvbox_cd-r</b>
COMODO Advanced Filter	? ×
ADVANCED FILTER Application Action Target	APPLY CANCEL

There are 3 categories of filter you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following options are available in the 'Advanced Filter' drop-down:

i. Application: The 'Application' option displays a drop-down field and text entry field.

COMODO Advanced	Filter	? ×
ADVANCED FILTER Application	+ Add	
Application Contains Contains Does Not Co	▼ cuckoo ntain	×
		APPLY CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you choose 'Does Not Contain' from the drop-down and enter the phrase 'cuckoo', then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

COMODO Creating Trust Online\*

ii. Action: Selecting the 'Action' option displays a drop down menu and a set of filter parameters that can be selected or deselected.

COMODO Advanced Filter			?	×
ADVANCED FILTER Action	+ Add			
Action Equal			$\otimes$	
Scanned online and found malicious	Access memory	Create process		
Terminate process	Modify key	Modify file		
Direct memory access	Direct disk access	Direct keyboard access		=
Direct monitor access	Load driver	Send message		
Instal Hook	Access COM interface	Execute image		
DNS/RPC client access	Change HIPS mode	Shellcode injection		
Block file	Suspicious	Hook		
Alert suppressed	Scanned and found safe			Ŧ
		APPLY	CANCEL	

- c. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- d. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Scanned online and found malicious
  - Access memory
  - Create process
  - Terminate process
  - Modify key
  - Modify file
  - Direct memory access
  - Direct disk access
  - Direct keyboard access
  - Direct monitor access
  - Load driver
  - Send message
  - Install Hook
  - Access COM interface
  - Execute image
  - DNS/RPC client access
  - Change HIPS Mode
  - Shellcode injection
  - Block file
  - Suspicious
  - Hook

COMODO Creating Trust Online\*

- Alert Suppressed
- Scanned and found safe

For example, if you choose 'Equal' and select 'Create process', only events involving the creation of a process by applications will be displayed. If you choose 'Not Equal' and select 'Modify Key', then all events that do not have the entry 'Modify key' in the 'Actions' column will be displayed. You can select more than one action from this interface, as required.

iii. Target: Selecting the 'Target' option displays a drop-down menu and text entry field.

COMODO Advanced Filter			?	×
ADVANCED FILTER Target	<b>∔</b> Add			
Target Contains 🔻	svhost.exe			$\otimes$
		APPLY	CANCE	ĒL

a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'svchost.exe' in the text field, then all events containing the entry 'svchost.exe' in the 'Target' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'svchost.exe', then all events that do not have the entry 'svchost.exe' in the 'Target' column will be displayed.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'HIPS' log viewer. Only those HIPS entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

## 5.4.5. Containment Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- · Click the 'Show' drop-down at top-left
- Select 'Containment Events' from the menu
- CCS records all actions taken by the containment module. Events that are recorded include:
  - · When you manually run an application in the container
  - When an an auto-containment rule runs an application in the container

#### View Containment Logs

• Click 'Tasks' on the CCS home screen

COMODO Creating Trust Online\*

Click 'Advanced Tasks' > 'View Logs'

- Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Containment Events' from the 'Show' drop-down:

но <mark>w</mark> Containment Ev	vents 🔻	<b>⊤</b> Advanced Filter	i Filter by D and Tim		ı file Cle	anup log file	<b>E</b> xport	🗘 Refresh	
Date & Time	Application	Rating	Action	Containe	Alert	Parent	Parent	Pare	
6/12/2019 10	C:\Program Files\C	Trusted	Run Vir	Virtual Des					
6/12/2019 10	C:\Windows\Syste	Trusted	Run Vir	Contained		<u>bitsadmi</u>	4152	E3381	
6/12/2019 10	C:\Old Man Apps\	Unrecogni	Run Vir	User		virtkiosk	5064	0E68	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O
6/12/2019 10	C:\Windows\Syste	Trusted	Run Vir	Containme		cmdvirth	812	84D6	
6/12/2019 10	C:\Windows\Syste	Trusted	Run Vir	Containme		<u>cmdvirth</u>	812	84D6	
6/12/2019 10	C:\Windows\Syste	Trusted	Run Vir	Containme		<u>cmdvirth</u>	812	84D6	
6/12/2019 10	C:\Windows\Syste	Trusted	Run Vir	Containme		<u>cmdvirth</u>	812	84D6	The second se
6/12/2019 10	C:\Program Files\C	Trusted	Run Vir	Containme		services	620	E2CA	
6/12/2019 10	C:\Program Files\C	Trusted	Run Vir	Virtual Des		explorer	4348	F5D0	

- Date & Time When the event occurred.
- · Application The installation path of the application that was run in the container
- **Rating** The reputation of the contained application. The trust rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Unrecognized files are run in the container until such time as they can be classified as 'Trusted' or 'Malicious'.
- Action How the malware was handled by CCS. This is also the restriction level imposed on the application by the container.
- Contained by The CCS service, policy or user that placed the application in the container.
- · Alert Click 'Related Alert' to view the notification generated by the event

**Note**: Containment alerts are shown when an installer, or unknown application requires admin/elevated privileges to run.

The alerts are only shown if 'Do not show privilege elevation alerts' is disabled in 'Settings' > 'Containment' > 'Containment Settings'.

See Containment Settings for more details.

- Parent Process The program which spawned the contained process.
  - Click the name of the parent process to view the hierarchical order of processes

ne\Hotel Mana	Unrecognized	Run Virtu	Contained Pr	. <u>exe</u> 336	E9482.
\giri1\AppDat	Unrecognized	Run Virtu	$\sim$		
сомо	DO Parent P	rocesses Tree	Details	?	×
Application				PID	
🔻 💷 winlog	on.exe			620	
🔻 匪 use	rinit.exe			4664	
🚽 🔽 🐂 e	explorer.exe			4232	
- 6	BiHMS.exe			336	
4	CompressDB	exe		7792	

- Parent Process ID The unique identifier that points to the process
- Parent process hash The SHA1 hash value of the program which spawned the contained process.
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- Open log file Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order.

### 5.4.5.1. Filter Containment Logs

You can create custom event log views according to your preferences. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

**Preset Time Filters:** 

• Click 'Filter by Date and Time' to view logs for a specific time period:

Creating Trust Online\*

COMODO View Logs - Curren	t week				?	_		×
SHOW Containment Events	<b>▼</b> Advanced Filter	Filter by Date and Time	Copen log file	X Cleanup log file	Expo		t) Refres	;h
Date & Time Application	Ra	<ul> <li>(No filterin</li> <li>Within las</li> <li>Except las</li> <li>Today</li> <li>Current w</li> <li>Current m</li> <li>Within the</li> <li>07/31/</li> </ul>	t 1 st 1 eek onth e period of	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√ hour(s)</li> </ul>	•	Alert	t	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- **Except last** Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

Date & Time	Application	▼ Ra	ting
11/22/2016 12:	C:\VTRoot	Refresh	ogni
11/22/2016 12:	C:\sample_	Show advanced filter Export	ogni
		Today	
		Current week	
		Current month	
		Entire period	

### **Advanced Filters**

Having chosen a time range, you can further refine events with the following filters:

- Application Show events propagated by a specific application
- Rating Show events which concern files that have a specific trust-rating
- Action Show events where a specific action was applied to the file by CCS
- Contained by Show events where the file was contained by a specific module or user

COMODO Creating Trust Online\*

- Parent process Show files contained based on its source process(es)
- Parent Process ID Show events created by a process ID
- **Parent process hash** -Show events where items was contained based on its source process(es) specified by hash value(s) of executable file(s) associated with the source process(es)

#### Configure filters for containment events

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply the filter:

COMODO View Logs - Today							?	- 0	ı ×
SHOW Containment Events	Advanced Filter	E Filter by Date and Time	<b>fin</b> Open log file	<b>X</b> Cleanup log file	Export	C) Refresh			
Date & Time Application	Piting	Action C	ontaine Al	ert Parent P	rocess	Parent Process ID	Parent proce	ess hash	
	l Filter						?		×
ADVANCED FILTER		+							
Application		Add							
Application	<u> </u>								
Rating									
Action									
Contained by									
Parent Process									
Parent Process ID									
Parent process hash									
						APPLY		CANCEL	

There are seven categories of filter you can add. Each of these categories can be further refined by selecting specific parameters, or by typing a filter string in the field provided. You can add and configure any number of filters.

i. Application: Allows you to filter the entries based on name of the contained item. The 'Application' option displays a drop-down field and text entry field.

сомод	O Advanced Filter			? ×
ADVANCED FILT Application	TER	+ Add		
Application	Contains Contains Does Not Contain	•		$\otimes$
			APPLY	CANCEL

COMODO Creating Trust Online\*

- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'pcflank' in the text field, then all events containing the entry 'pcflank' in the 'Application' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'pcflank', then all events that do not have the entry 'pcflank' in the 'Application' column will be displayed.

- c. Repeat the process to add more application filters
- ii. **Rating**: Allows you to filter the entries based on file reputation of the contained item. Selecting the 'Rating' option displays a drop-down menu and set of specific filter parameters that can be selected or deselected.

сомо	DDO Advanced Filter			? ×
ADVANCEI Rating	O FILTER	+ Add		
Rating	Equal Equal Not Equal	▼ □ None ☑ Trusted	Unrecognized	$\otimes$
			APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - None
  - Unrecognized
  - Trusted
  - Malicious

For example, if you choose 'Equal' and select the 'Unrecognized' file rating, only the containment events involving applications that are categorized as 'Unrecognized' will be displayed. If you choose 'Not Equal' and choose 'Malicious' file rating, then all events that do not have the entry 'Malicious' in the 'Rating' column will be displayed. You can select more than one file rating from this interface, as required.

- c. Repeat the process to add more filters based on file rating
- iii. Action: Allows you to filter the entries based on containment level imposed on the item. The 'Action' option displays a drop-down menu and a set of specific filter parameters that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter			? ×
ADVANCED FILTER Action	+ Add		
Action Equal  Equal Not Equal	Run Restricted     Blocked	☑ Run Virtually □ Ignored	$\otimes$
		APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the restriction level(s) applied by the container to the applications, either automatically of as chosen by the user from the alert. The options available are:
  - Run Restricted
  - Run Virtually
  - Blocked
  - Ignored

For example, if you choose 'Equal' from the drop-down and select 'Run Virtually', only the events of applications that are run inside the container will be displayed. If you choose 'Not Equal' and select 'Blocked', then all events that do not have the entry 'Blocked' in the 'Action' column will be displayed. You can select more than one checkbox as required.

- c. Repeat the process to add more filters based on the action
- iv. Contained by: Allows you to filter the entries based on CCS service or policy was responsible for running the item inside the containment. Selecting the 'Contained by' option displays a drop-down menu and a set of specific filter parameters that can be selected or deselected.

COMODO Advanced Filter		?	×
ADVANCED FILTER Contained by	Add		
Contained by Contains	•		$\otimes$
Containment Policy	User	Contained Process	
		APPLY CAN	CEL

a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your

COMODO Creating Trust Online\*

selected choice.

- b. To refine your search, select the source(s) by which the applications were contained. The options available are:
  - Containment Policy
  - User
  - Contained Process
  - Containment Service

For example, if you choose 'Contains' and select the 'User' checkbox, then only events involving applications that were manually run inside the container will be displayed. If you choose 'Does Not Contain' and select the 'Containment Policy' checkbox, then all events that do not have the entry 'Containment Policy' in the 'Contained by' column will be displayed. You can select more than one checkbox options from this interface, as required.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- c. Repeat the process to add more filters based on the CCS service/policy
- v. **Parent process:** Allows you to filter the entries based on the process(es) that launched the contained items. Selecting the 'Parent Process' option displays a drop-down field and text entry field.

сомодо	Advanced Filter					?		×
ADVANCED FILTER		+						
Parent Process	•	Add						
Parent Process	Contains Contains Does Not Contain							$\otimes$
				APPI	.Y	(	ANCEL	

- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the name of the application associated with the process, that launched contained item as the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'RuntimeBroker.exe' in the text field, then all events containing the entry 'RuntimeBroker.exe' in the 'Parent Process' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'RuntimeBroker.exe', then all events that do not have the entry 'RuntimeBroker.exe' in the 'Parent Process' column will be displayed.

- c. Repeat the process to add more filters based on the parent process(es).
- vi. Parent Process ID: Allows you to filter the entries based on the process(es) ID that launched the contained

COMODO Creating Trust Online\*

items. Selecting the 'Parent Process ID' option displays a drop-down field and text entry field.

соморо	Advanced Filter				?	×
ADVANCED FILTER Parent Process ID		+ Add				
Parent Process	Does Not Contain Contains Does Not Contain	0				$\otimes$
				APPLY	(	

- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the name of the application associated with the process, that launched contained item as the search criteria for filtering the logs in the text field.
   For example, if you choose 'Contains' and enter the phrase '2612' in the text field, then all events containing the entry '2612' in the 'Parent Process ID' column will be displayed. If you choose 'Does Not Contain' and enter the phrase '2612', then all events that do not have the entry '2612' in the 'Parent Process ID' column will be displayed.
- c. Repeat the process to add more filters based on the parent process(es).
- vii. **Parent process hash**: Allows you to filter the entries based on the parent process(es) by entering their SHA1 hash values .Selecting the 'Parent process hash' option displays a drop-down field and text entry field.

COMODO Advanced Filter				?	×
ADVANCED FILTER Parent process hash	<b>∔</b> Add				
Parent process hash Equal Not Equal					$\otimes$
			APPLY	CANCE	L

- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the SHA1 hash value of the executable file associated with the process, that launched contained item as the search criteria.
- c. Repeat the process to add more filters based on the parent process(es).
- Click 'Apply' for the filters to be applied to the 'Containment' log viewer. Only those 'Contained' entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

COMODO

## 5.4.6. Device Control Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- · Select 'Device Control Events' from the 'Show' drop-down
- CCS records all events related to external devices. External devices include USB, optical, and storage drives plugged into your computer.

Events logged include:

- Files copied, deleted and moved
- Device enabled/disabled ('Log detected devices' must be enabled)

See 'Advanced Settings > Device Control Settings' for more help to configure device control.

Admins can also configure this option in an Endpoint Manager profile. For example, if you want to allow unfettered access to certain devices you can (i) disable device control entirely (ii) remove the device class from the list of controlled types, or (iii) add specific devices to exclusions.

#### View 'Device Control' Logs

- Click 'Tasks' on the CCS screen
- Click 'Advanced Tasks' > 'View Logs'
  - · Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Device Control Events' from the 'Show' drop-down:

	v Logs - Today			?	- 0	>
SHOW Device Control Events	₹ Advan Filte	ced Filter by Date Onen log File Cleanup log	Export Refresh			
Date	Name	Identifier	Class	State		
8/2/2017 3:37:08 PM	USB Input Device	USB\VID_0627&PID_0001\42	745A17A0-74D3-11D0-B6FE-0.	. Enabled		
8/2/2017 3:37:08 PM	CD-ROM Drive	IDE\CDROMQEMU_QEMU_DVD-ROM	4D36E965-E325-11CE-BFC1-0	Enabled		
8/2/2017 3:32:20 PM	USB Input Device	US8\VID_0627&PID_0001\42	745A17A0-74D3-11D0-B6FE-0.	. Disabled		
8/2/2017 3:32:20 PM	CD-ROM Drive	IDE\CDROMQEMU_QEMU_DVD-ROM	4D36E965-E325-11CE-BFC1-0	Disabled		

- **Date** When the event occurred.
- Name The type of device associated with the event.
- · Identifier The identification string of the device
- **Class** The GUID (Globally Unique Identifier) string of the category of the device as defined by the Windows operating system.
- State Whether the device was allowed or blocked.
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log

COMODO Creating Trust Online\*

- Refresh Reload the current list and show the latest logs
- · Click any column header to sort the entries in ascending \ descending order

### 5.4.6.1. Filter 'Device Control' Logs

Filters allow you to view a specific sub-set of logs. The following types of filter are available:

- Preset Time Filters
- Advanced Filters

### **Preset Time Filters**

• Click 'Filter by Date and Time' to view logs for a specific time period:

COMODO View Logs - Today					? —	
SHOW Device Control Events	<b>⊤</b> Advanced Filter	Filter by Date and Time	Gen log file	X Cleanup log file	Export	C) Refresh
Date Name	Id	<ul> <li>(No filterin</li> <li>Within last</li> <li>Except last</li> <li>Today</li> <li>Current we</li> <li>Current m</li> <li>Within the</li> <li>07/31/2</li> </ul>	t 1 t 1 eek onth period of	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√31/2017 ▼</li> </ul>		te

- **No filtering** Display every event logged since Comodo Client Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Display all logged events for today.
- **Current Week** All events logged during this week. The current week is calculated as the previous Sunday to the next Saturday.
- Current Month Display all events logged from the 1st of this month.
- Custom Filter Select specific 'To' and 'From' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.

COMODO Creating Trust Online\*

	Name	Identifier	
72017 3:3 <b>7:08 PM</b>	USB Input Dev	Refresh	ID_0001\42
/2017 3:37:08 PM	CD-ROM Driv	Show advanced filter Export	J_QEMU_DVD-F
//2017 3:3 <b>2:20 PM</b>	USB Input Dev	Today	- I <b>D_00</b> 01\42
/2017 3:32:20 PM	CD-ROM Driv	Current week Current month	J_QEMU_DVD-F
		Entire period	

### **Advanced Filters**

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want and click 'Add' to apply it:

соморо	View Logs - Toda	у				?	_		×
SHOW		Ŧ	<b>1</b>	-	×			Ð	
Device Control Ev	vents 🔻	Advance Filter	d Filter by Date and Time	Open log file	Cleanup log file	Ехро	rt	Refres	h
Date	Name		Identifier		Class		State		
								-	
СОМОДО	Advanced Filter				_			?	×
ADVANCED FILTER Name		<b>∔</b> Add							
Name Identifier	<u> </u>								
Class State									
									_
					АРР	LY		CANCEL	

- There are 4 types of filter you can add. Each of these can be further refined by selecting or deselecting parameters, or by typing a filter string as criteria.
- You can add and configure any number of filters in the 'Advanced Filter' dialog.
- · Click 'Apply' after adding the filter(s) to view the filtered results

The following filters are available:

Name: Filter the entries based on the type of the device.

COMODO Creating Trust Online\*

сомо	Advanced Filter			?	×
ADVANCE Name	D FILTER	+ Add			
Name	Contains Contains Does Not Contain	Sandisk			$\otimes$
			APPLY	CANCE	iL

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your filter criteria.
- b) Enter the type of the device in full or part as your filter criteria in the text field.

For example, if you choose 'Contains' and type 'USB Input Device' in the text field, you will see logs related to USB input devices like keyboards, mice and finger print scanners.

Identifier: Filter entries based on the device ID of the external device.

• Select 'Identifier' from the drop-down and click 'Add'

сомоі	OO Advanced Filter				? ×
ADVANCED F	ILTER	<b>₽</b> Add			
Identifier	Contains Contains Does Not Contain	USBTOR	DISk		$\otimes$
				APPLY	CANCEL

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your filter criteria.
- b) Enter the device ID of the device in full or part as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'USB\VID\_0627&PID\_0001', in the text field only those log entries related to external devices whose device ID contains the string will be displayed.

Class: Filter the entries based on the GUID of the device:

COMODO Creating Trust Online\*

сом	<b>DDO</b> Advanced Filter			? ×
ADVANCE Class	ed filter	<b>∔</b> Add		
Class	Contains Contains Does Not Contain	4D36E967		$\otimes$
			APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your filter criteria.
- b. Enter a Device Class ID (GUID) in part or full as your search criteria

For example, if you select 'Contains' option from the drop-down field and enter '4D36E967', then all events containing the entry '4D36E967' in the 'Class' field will be displayed..

State: Filter events based on whether the device connection attempt was allowed or blocked	State:	Filter	events	based	on	whether	the	device	connection	attempt	t was	allowed	or blocke	d.
--	--------	--------	--------	-------	----	---------	-----	--------	------------	---------	-------	---------	-----------	----

сом	ODO Advanced Filter			?	×
ADVANC	ED FILTER	+ Add			
State	Equal Equal Not Equal	Enabled	Disabled		$\otimes$
			APPLY	CANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' inverts your search criteria.
- b. Now select the state to refine your search. The parameters available are:
  - Enabled
  - Disabled

**Note**: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' to view the filtered results.
- Remove all filters and click 'Apply' to view the full list again.

## 5.4.7. Autorun Event Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- · Click the 'Show' drop-down at top-left

COMODO Creating Trust Online\*

- Select 'Autorun Events' from the menu
- Autorun logs show events where unexpected changes were attempted on Windows services, auto-start entries and scheduled tasks.

#### Background:

- CCS monitors changes to registry items related to Windows Services, Autorun entries and scheduled tasks.
- You can define the response CCS should take against unrecognized autoruns in 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'. See Miscellaneous Settings for more details.
- You can also define the response to unknown autoruns found by an antivirus scan. See **configure scan options** for more help on this.

#### View 'Autoruns Events' logs interface

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - · Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Autoruns Events' from the 'Show' drop-down:

ном	1	-	📩 🖬	🗶 Cleanup log		<i>t</i> 9	
Autoruns Events		<ul> <li>Advanced Filter</li> <li>Filter and</li> </ul>	∙by Date Open log d Time ⊿	file file	Export	Refres	sh
Date & Time	Туре	Location	Modifier	Action	Detecte	Status	•
4/16/2019 9:43	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/16/2019 9:43	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 1:52	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 1:52	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 1:52	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 1:52	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 1:52	Auto Runs	C:\ProgramData\Com	C:\Users\giri1\	Ignore	Monitor	Success	
4/12/2019 11:2	Window Servi	C:\Users\giri1\AppDa	C:\Windows\Sy	Ignore	Monitor	Success	
4/12/2019 11:2	Auto Runs	C:\Suspicious\AntiTes	C:\Suspicious\	Ignore	Monitor	Success	

- Date & Time When the event occurred.
- Type Whether the detected item is an autorun entry, Windows service, or scheduled task.
- Location The installation path of the affected item, or the location of the new item
- Modifier The location of the application that made the change.
- Action How CCS responded to the event.

COMODO Creating Trust Online\*

- Status Whether the action taken was a success or failure
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- Open log file Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs
- · Click any column header to sort the entries in ascending \ descending order

### 5.4.7.1. Filter Autorun Events Logs

Filters allow you to view a specific sub-set of logs. The following types of filters are available:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters**

• Click 'Filter by Date and Time' to display logs for a specific time period:

HQW Autoruns Events	<b>▼</b> Advanced Filter	Filter by Date and Time	Gen log file	X Cleanup log file	Export	€) Refresh
Date & Alert Type Description	Advice	<ul> <li>(No fliterin</li> <li>Within las</li> <li>Except las</li> <li>Today</li> <li>Current w</li> <li>Current m</li> <li>Within the</li> <li>07/31/</li> </ul>	t 1 st 1 eek onth	<ul> <li>▲ hour(s)</li> <li>▲ hour(s)</li> <li>√31/2017 ▼</li> </ul>		Event

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged from 12:00 am today to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period:

COMODO Creating Trust Online\*

Date &	Alert Type	Description	Advice	Answered	
4/11/201	Antivi	Refresh	:\Suspicious fi	4/11/2017	Disinfec
4/11/201	Antivi	Show advanced filter Export	:\Suspicious fi	4/11/2017	Skip on
		Today Current week			
		Current month Entire period			

### Configure advanced filters for autorun logs

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want and click 'Add' to apply it:

COMODO Advanced Setting	gs					?	-		×
COMODO View Logs - Tod	ay					?	-		×
SHOW Autoruns Events	Advanced Filter	Filter by Date and Time	Gen log	Clean	¥ up log ile	Expo		C) Refresh	
Date & Time Type	Location	Modifier		Action		Detected	Ву	Status	
COMODO Advanced Filter								?	×
ADVANCED FILTER Type Location Modifier Action Detected By Status	+ Add								
					AP	PLY		CANCE	

- Click the 'Add' button to create a custom filter
- There are 6 categories of filter you can add. Each of these can be further refined by selecting or deselecting parameters, or by typing a filter string in the field provided.
- You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following are available:

**Type**: Allows you to filter entries based on the launched tasks. Selecting the 'Type' option displays a drop down box and a set of specific task types that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter		,	? ×
ADVANCED FILTER Type	+ Add		
Type Equal	<ul> <li>Windows service</li> <li>Scheduled task</li> </ul>	Autostart entry	$\otimes$
		APPLY	CANCEL

- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Windows Service
  - Autostart entry
  - Scheduled task

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

**Location**: Filter file list changes according to their CCS code. You can view file list changes in the 'Location' column of the log viewer. Selecting the 'Location' option will display drop-down and text entry fields.

COMODO Creating Trust Online\*

COMODO Advanced Filter	?	Х
ADVANCED FILTER + Location Add		
Location Contains C:/Program Files((x86)\Cuckoo Files\cuckoo.exe		$\otimes$
Does Not Contain		
APPLY	CANCE	:L

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Enter the location or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe in the text field, then only log entries with the same value in the 'Path' column will be displayed.

**Modifier**: Filter log entries based on the file or user that launched the event. Selecting the 'Modifier' option will display drop-down and text entry fields.

COMODO Advanced Filter	? ×
ADVANCED FILTER Add	
Modifier       Contains         Contains       Does Not Contain	
APP	CANCEL

a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your

COMODO Creating Trust Online\*

#### selected choice.

b. Enter the location or a part of it as your filter criteria in the text field.

For example if you choose 'Contains' and enter 'C:/Users/tester/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/UnknownAppUI3.exe' in the text field, then only log entries with the same value in the 'Path' column will be displayed.

**Action**: The 'Action' option allows you to filter logs based on the actions taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

COMODO Advanced Filter			?	×
ADVANCED FILTER	<b>+</b> Add			
Action Equal	☐ Ignore ☐ Terminate and Disable	<ul> <li>Terminate</li> <li>Quarantine and Disable</li> </ul>	8	9
		APPLY	CANCEL	

- c. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- d. Now select the check boxes of the specific filter parameters to refine your search. The parameter available are:
  - Ignore CCS does not take any action
  - Terminate CCS stops the process / service
  - Terminate and Disable Auto-run processes will be stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
  - Quarantine and Disable Auto-run processes will be quarantined and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.

**Detected By**: The 'Detected By' option allows you to filter logs based on the item that detects or identifies the threat or malware. To filter logs by CCS detected by, select from the drop down box and then choose the detection method.

COMODO Advanced Filter		? ×
ADVANCED FILTER Detected By	+ Add	
Detected By Equal	Autoruns monitor	Antivirus Scan
		APPLY CANCEL

COMODO Creating Trust Online\*

- c) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- d) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Autorun monitor
  - Antivirus Scan

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

**Status**: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.

COMODO Advanced Filter		? ×
ADVANCED FILTER Status	+ Add	
Status Equal Equal Not Equal	Success Failure	$\otimes$
	APPLY	CANCEL

- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
- Success: Displays events where the actions against the detected threat were successful. For example, the
  malware was successfully quarantined.
- Failure: Displays events where the intended actions against the detected threat were not successful. For example, the malware was not disinfected.

**Note:** Multiple filters can be added in the 'Advanced Filter' pane. After adding a filter, select the next filter type and click 'Add'. You can remove filters by clicking the 'X' button at the top right of the filter pane.

• Click 'Apply' for the filters to be applied to the VirusScope log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

## 5.4.8. Alert Logs

Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

COMODO Creating Trust Online\*

- Click the 'Show' drop-down at top-left
- Select 'Alerts' from the menu
- Alert logs are a record of all threat notifications generated by CCS, and also record the user's response to the alert.

### **View Alert Logs**

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Alerts' from the 'Show' drop-down

			₹	ĊŤ	F		×	E		
HOW Alerts	_	<b>▼</b>	dvanced Filter	by Date d Time	Open lo	-	anup log file	Export	<del>ري</del> Refres	
Date &	Alert Ty	Description	Advice	Answ	ered	Answer	Option	Treat as	Event	1
4/24/20	HIPS alert	smartscreen.ex	smartscreen.ex.	. 4/24/	2019	Treat as		Allowed	Related	
4/24/20	HIPS alert	smartscreen.ex	smartscreen.ex.		Show	Show			Related	
4/24/20	Antivirus	.Unclassified M	C:\Suspicious\p	4/24/	2019	Skip once			Related	
4/24/20	Antivirus	.Unclassified M	C:\Suspicious\p			Show			Related	
4/24/20	Antivirus	Backdoor.Win3	C:\Suspicious\p	4/24/	2019	Skip once			Related	
4/24/20	Antivirus	Backdoor.Win3	C:\Suspicious\p			Show			Related	
4/24/20	Antivirus	Malware@#27s	C:\Suspicious\e	4/24/	2019	Disinfect			Related	
4/24/20	Antivirus	Malware@#27s	C:\Suspicious\e			Show			Related	
4/24/20	Antivirus	Malware@#27s	C:\Users\giri1\	4/24/	2019	Skip once			Related	
										•

- Date & Time When the event occurred.
- Alert Type The security module that generated the alert. Alert types include antivirus, firewall, HIPS, containment, VirusScope and secure shopping.
- Description Name of the file or event that caused the alert.
- Advice -The recommendation, or informational text in the alert. This text is intended to help users decide to respond to the threat.
- Answered Whether or not the alert was answered by the user. You will see the date and time of the
  response if an answer was provided.
- Answer The user's response to the alert. For example, 'Allow', 'Block', 'Disinfect', 'Skip'.
- Option Additional settings chosen by the user at the alert. For example, 'Remember My Answer'.
- **Treat As** Whether or not the user applied a specific ruleset to the file at the alert. The ruleset tells CCS the restriction level to apply to the file in future. Example rulesets include 'Treat as a safe application, or 'Treat as an installer'.
- Event Click 'Related Event' to view more details about the incident that triggered the alert.
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

COMODO Creating Trust Online\*

- Open log file Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Refresh Reload the current list and show the latest logs

Click any column header to sort the entries in ascending / descending order.

#### 5.4.8.1. Filter 'Alerts' Logs

Filters allow you to view a specific sub-set of logs. The following types of filters are available:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters**

• Click 'Filter by Date and Time' to view logs for a specific time period:

COMODO View Logs - Today					?	_		×
SHOW Alerts	<b>⊤</b> Advanced Filter	G Filter by Date and Time	Copen log file	X Cleanup log file	Exp		रू Refresi	h
Date & Alert Type Description	Advice	<ul> <li>(No filterin</li> <li>Within las</li> <li>Except las</li> <li>Today</li> <li>Current w</li> <li>Current m</li> <li>Within the 07/31/</li> </ul>	t 1 st 1 reek nonth e period of	<ul> <li>hour(s)</li> <li>hour(s)</li> </ul>	*	at as	Event	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

COMODO

Date &	Alert Type	Description	Advice	Answered	
4/11/201	Antivi	Refresh	:\Suspicious fi	4/11/2017	Disinfec
4/11/201	Antivi	Show advanced filter Export	:\Suspicious fi	4/11/2017	Skip on
		Today Current week			
		Current month Entire period			

#### **Advanced Filters**

You can further refine which events are displayed according to specific filters. The following filters are available:

- Advice: Displays only alerts that match the advice entered.
- Answer: Displays only alerts that were answered by the user.
- **Answered:** Displays only alerts that were answered at a specific date and time.
- Description: Displays only alerts that match the description entered
- **Option**: Displays only alerts where the user selected an additional option at the alert. Addition options include 'Remember my answer'.
- **Treat As:** Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.
- Alert Type: Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope).

#### Configure Advanced Filters for Alerts Displayed

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply it:

COMODO Creating Trust Online\*

сомо	DO View	Logs - Today	$\frown$				?	
SHOW Alerts			<b>▼</b> Advanced Filter	ilter by Date and Time	<sub>o file</sub> Clean	¥ iup log ile		
Date &	Alert Type	Description	Advice	Answered	Answer	Option	Treat	
4/11/201	Antivirus	Virus.Win32.Par	. D:\Suspicio	us fi 4/11/2017	Disinfect			
сомод	O Advanced	l Filter					?	×
ADVANCED FIL Advice Advice	TER	Add						
Answer Answered								
Description Option Treat as								
Alert Type								
					APPLY		CANCEL	

There are 7 categories of filter you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following options available in the 'Add' drop down menu:

i. Advice: Filter alerts based on the recommendations given by CCS in the alert. Selecting the 'Advice' option will display drop-down and text entry fields.

COMODO Creating Trust Online\*

COMODO Advanced Filter	? ×
ADVANCED FILTER     +       Advice     Add	
Advice Contains You can safely allow this request	$\otimes$
Does Not Contain	
APPL	Y CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' and enter the phrase 'you can safely allow this request' in the text field, then only entries containing 'you can safely allow this request' in the 'Advice' column will be displayed.

i. **Answer**: Allows you to filter alerts based on what action the user selected at the alert. Selecting the 'Answer' option displays a drop-down box and a set of answers that can be selected or deselected.

COMODO Creating Trust Online\*

COMODO Advanced Filter			?	×
ADVANCED FILTER Answer	+ Add			
Answer Equal 🔻				$\otimes$
Unknown	Allow	Deny		
Treat as	Disinfect	Quarantine		
Quarantine and reverse	Skip once	Add to exclusions		
Add to trusted files	False positive	Skip		
Terminate	🔲 Keep inside the Container	Run outside the Container		
Deny and Terminate	Deny, Terminate and Reverse	Containment		
🔲 Run Unlimited	🔲 Run inside the Container	Blocked		
		APPLY	CANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the responses to refine your search. The options available are:
  - Unknown
  - Allow
  - Deny
  - Treat as
  - Disinfect
  - Quarantine
  - Quarantine and reserve
  - Skip once
  - Add to exclusions
  - Add to trusted files
  - False positive
  - Skip
  - Terminate
  - Keep inside the Container
  - Run outside the Container
  - Deny and Terminate
  - Deny, Terminate and Reverse
  - Containment
  - Visit with Secure Browser
  - Run Unlimited
  - Run inside the Container
  - Blocked

For example, if you choose 'Equal' from the drop-down and select the 'Add to exclusions' checkbox, only the alerts where you answered 'Ignore' > 'Ignore and Add to exclusions' will be displayed.

Creating Trust Online\*

iii. **Answered**: The' Answered' option enables you to filter logs based on the date you answered the alerts. Selecting the 'Answered' option displays a drop-down box and date entry field.

COMODO Advanced Filter		? X
ADVANCED FILTER	+	
Answered <b>•</b>	Add	
		$\otimes$
Answered Equal 🔻	07/31/2017 🔻	
	<ul> <li>✓ July 2017</li> </ul>	
	Sun Mon Tue Wed Thu Fri Sat	
	25 26 27 28 29 30 1 2 3 4 5 6 7 8	
	9 10 11 12 13 14 15	
	16 17 18 19 20 21 22	
	23 24 25 26 27 28 29	
	<b>30 31</b> 1 2 3 4 5	
	Today: 7/31/2017	
	APPLY	CANCEL

- a. Select any one of the following option the drop-down.
  - Equal
  - Not Equal

b. Select the required date from the drop-down calendar.

For example, if you select 'Equal' and select '07/31/2017', only alerts answered on 07/31/2017 will be displayed.

iv. **Description**: The 'Description' option enables you to filter logs based on the description of the attempt displayed in the alert. Selecting the 'Description' option displays a drop-down field and text entry fields.

COMODO Creating Trust Online\*

COMODO Advanced Filter	?	×
ADVANCED FILTER		
Description   Add		
Description Contains Connect to the intranet		$\otimes$
Does Not Contain		
APPLY		

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you select 'Contains' from the drop-down and enter 'connect to the Internet', only the log entries of Firewall alerts that contain the phrase 'connect to the Internet' in the description, will be displayed.

v. **Option**: Displays only alerts where the user selected an additional options like 'Remember my answer', 'Submit as False Positive' from the alert.

сомо	Advanced Filter			?	×
ADVANCED Option	♥ FILTER	+ Add			
Option	Equal ▼ Equal Not Equal	<ul><li>Remember</li><li>Submit</li></ul>	<ul><li>Restore point</li><li>Trusted publisher</li></ul>		$\otimes$
			APPLY	CANCE	

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Remember
  - Restore point
  - Submit

COMODO Creating Trust Online\*

#### Trusted publisher

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

vi. **Treat As**: Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.

COMODO Advanced Filter	? ×
ADVANCED FILTER Treat As Add	
Treat As Contains Installer	$\otimes$
Does Not Contain	
APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu
- b. Enter the text or word as your filter criteria

For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

vii. Alert Type: The 'Type' option enables you to filter the entries based on the component of CCS that has triggered the alert. Selecting the 'Type' option displays a drop-down menu and set of specific alert types that can be selected or deselected.

Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope).

COMODO Creating Trust Online\*

COMODO Advanced Filter			? ×
ADVANCED FILTER	+		
Alert Type	Add		
			$\otimes$
Alert Type Equal •			_
Antivirus Alert	Firewall Alert	HIPS alert	
Containment alert	VirusScope Alert	Network alert	
		APPLY CAN	NCEL

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Antivirus Alert
  - Firewall Alert
  - HIPS alert
  - Containment alert
  - VirusScope Alert
  - Network alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of Antivirus alerts will be displayed.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Alerts' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

#### 5.4.9. CCS Tasks Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Click the 'Show' drop-down at top-left
- Select 'Tasks' from the menu
- A task log is a record of a CCS operation such as a database update or a virus scan.

• The task log area shows all tasks run, their completion status and other details.

#### View task logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Tasks' from the 'Show' drop-down

HOW	▼           Advanced           Filter	Filter by Date and Time	Dpen log file	K Cleanup log	Export	C) Refresh	
Date & Ti Type	Parameter		ompleted	file	de li	nfo	Additiona
5/31/2019 Antivirus s	can (Be Full Scan						
5/31/2019 Antivirus u	ipdate (	5/	31/2019 11:21:04	AM	C	Old database 30947	New datab
5/31/2019 Antivirus s	can (Co Rating Scan	5/	31/2019 11:19:23	AM	S	canned 1808	Found 0
5/31/2019 Antivirus s	can (Be Rating Scan						
5/31/2019 Antivirus u	ipdate (						
5/31/2019 Virtual De	sktop Se	5/	31/2019 11:06:08	AM 0x8	3000400		
5/31/2019 Virtual De	sktop Se	5/	31/2019 11:06:08	AM 0x8	3000400		
5/31/2019 Virtual De	sktop Se	5/	31/2019 11:06:08	AM 0x8	3000400		
5/31/2019 Virtual De	sktop Se	5/	31/2019 11:06:08	AM 0x8	3000400		

- Date & Time When the event occurred.
- Type The task that was performed. For example, 'Antivirus scan', or 'Database update'.
- Parameter:
  - The sub-type of the operation. For example, 'Quick Scan' is a sub-type of 'Antivirus scan'. OR
  - The target of the operation. For example, 'C:\Program Files' is the target area scanned.
- Completed The time that the operation finished
- **Code** Error code generated by Windows for CCS tasks that were not successful. No code is shown if the task finished successfully.
- Info and additional info Shows further details about the task. For update tasks, these fields show the old and new version numbers. For scan tasks, they show the number of items scanned and the number of viruses found.
- Open log file Browse to and view a saved log file.
- Cleanup log file Delete the selected event log
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- · Refresh Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order.

COMODO Creating Trust Online\*

#### 5.4.9.1. Filter 'Tasks' Logs

Filters allow you to view a specific sub-set of logs. The following types of filters are available:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters**

• Click 'Filter by Date and Time' to display logs for a specific time period:

сомо	DO View Logs	- Curren	t week				? —	n x
SHOW Tasks		٠	<b>⊤</b> Advanced Filter	Tilter by Date and Time	🖬 Open log file	X Cleanup log file	Export	Q Refresh
Date &	Туре	Param	eter	(No filtering)	-			Additio,
8/1/2017	Antivirus scan	Quick	Scan	<ul> <li>Within las</li> <li>Except las</li> </ul>		+ hour(s)		
8/1/2017	Antivirus update			Today			base 2	New data
8/1/2017	Antivirus update			Ourrent w			base 2	New data
7/31/201	Antivirus update			<ul> <li>O Current m</li> <li>Within the</li> </ul>			base 2	New data
7/31/201	Antivirus update			08/01/	2017 🔫 - 08	/01/2017	base 2	New data

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since
  installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

Creating Trust Online\*

e	Parameter	Complet	ed	Code	Info
tivirus scan	Quick Scan				
tivirus up <mark>date</mark>		8/1/2017	2:35:30 AM Refresh		Old databas
tivirus update		8/1/:	Show advance	d filter	Old databas
tivirus update		7/31	Export Today		Old databas
tivirus update		7/31	Current week		Old databas
tivirus update		7/3	Entire period		Old databas
virus update		7/31/201	17 2:4 <del>3.89</del> AM		Old databe

#### **Advanced Filters**

You can further refine which events are displayed according to specific filters. The following additional filters are available:

- Code Filters tasks based on specified error code
- Completed Displays only tasks completed on the specified date.
- **Parameter** Displays only tasks that include the selected parameter. A 'parameter' is a sub-type of the main task type. For example, 'Quick Scan' and 'Rating Scan' are both parameters of the main task type 'Antivirus Scan'.
- **Type** Displays only tasks of a certain type. Tasks that you can filter for include antivirus updates, antivirus scans, log clearing, warranty activation and more.

#### **Configure Advanced Filters for Tasks logs**

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply it:

COMODO Creating Trust Online\*

SHOW Tasks Advanced Filter by Date and Time Open log file Cleanup log file Cleanup log file Cleanup log file Code Info 4/11/201 Antivirus scan C \Promar Files\Mozi 4/11/2017 5:27:38 AM Scanned 0 COMODO Advanced Filter ? × Add Code Completed Parameter Type	COMODO View Logs	- Today			? —
4/11/201 Antivirus scan C\Protram Files\Mozi 4/11/2017 5:27:38 AM Scanned O  COMODO Advanced Filter  Advanced Filter  Add  Code  Code  Completed  Parameter  Code  Completed  Completed Co			liter by Date		
COMODO Advanced Filter ? X ADVANCED FILTER Code Code Code Completed Parameter	Date & Type	Parameter	Completed	Code Info	
ADVANCED FILTER Code Code Completed Parameter	4/11/201 Antivirus scan	C:\Program Files\Mozi	4/11/2017 5:27:38 AM		
	ADVANCED FILTER Code Code Completed Parameter	+			? ×

i. **Code**: Filter incomplete tasks according to their error code generated by Windows. You can view task codes in the 'Code' column of the log viewer. Selecting the 'Code' option will display drop-down and text entry fields.

COMODO Advanced Filter	?	×
ADVANCED FILTER Code Add		
Code Equal Equal Not Equal		$\otimes$
Not Equal		
APPLY C/	ANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Enter the code or a part of it as your filter criteria in the text field.

COMODO Creating Trust Online\*

For example, if you have select 'Equal' and entered '0x80004004' in the text field, then only entries containing the value '0x80004004' in the 'Code' column will be displayed.

i. **Completed**: Lets you filter logs based on the completion dates of the Tasks. Selecting the 'Completed' option displays drop-down box and date entry field.

COMODO Advanced Filter		? ×
ADVANCED FILTER	F Contraction of the second	
Completed	dd	
Completed Equal	08/01/2017 *	$\otimes$
	<ul> <li>▲ August 2017 ▶</li> </ul>	
	Sun Mon Tue Wed Thu Fri Sat	
	30 31 1 2 3 4 5	
	6 7 8 9 10 11 12	
	13 14 15 16 17 18 19 20 21 22 23 24 25 26	
	27 28 29 30 31 1 2	
	3 4 5 6 7 8 9	
	Today: 8/1/2017	
	· · · · · · · · · · · · · · · · · · ·	
	APPLY C	ANCEL

- a. Select any one of the following option the drop-down box.
- Equal
- Not Equal
- b. Select the required date from the date picker.

For example, if you choose 'Equal' and select '08/01/2017', only the logs of tasks completed on 08/01/2017' will be displayed.

iii. Parameter: The 'Parameter' option lets you filter entries based on the 'Parameter' column of the log viewer. This includes descriptions such as 'Quick Scan' and 'Rating Scan'. Selecting the 'Parameter' option displays drop-down and text entry fields.

COMODO Creating Trust Online\*

COMODO Advanced Filter	? ×
ADVANCED FILTER + Parameter Add	
Parameter • Add	
Parameter Contains Quick Scan Contains	$\otimes$
Does Not Contain	
	cuucti
APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Quick Scan' in the text field, then only the entries of 'Antivirus Scan Tasks' with the scan parameter 'Quick Scan' will be displayed.

iv. **Type**: Allows you to filter entries based on type of 'Tasks' launched. Selecting the 'Type' option displays a drop down box and a set of specific task types that can be selected or deselected.

COMODO Advanced Filter			? >	×
ADVANCED FILTER Type	+ Add			
Type Equal 🔻			$\otimes$	
Antivirus update	Antivirus scan	Log Clearing		
Product upgrade	🔲 Binary update	File Rating DB Update		
				1
		APPLY	CANCEL	Í

COMODO

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Antivirus update
  - Antivirus scan
  - Log Clearing
  - Product upgrade
  - Binary update
  - File Rating DB Upgrade

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

#### 5.4.10. File List Changes Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- · Click the 'Show' drop-down at top-left
- Select 'File List Changes' from the menu
- The 'File List' is an inventory of executable files and applications discovered on your computer. The list also shows the file vendor, the date the file was discovered, and the file's trust rating.
- You can view the file list in CCS at 'Settings' > 'File Rating' > 'File List'. See File List for help on this area.
- File list change logs are a record of any modifications to these files. Logged actions include adding a new file, removing a file, or changing the trust rating of a file.

#### View the 'File List Changes' Logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'File List Changes' from the 'Show' drop-down

COMODO Creating Trust Online\*

HOW File List Chan	ges 🗸 Ad	<b>⊤</b> Ivanced Filter	Tilter by Date and Time	🗖 Open log file	Cleanup log file	Export	🗘 Refresh
▲ Date &	Path	Modifier	Action	Property	Old Rating	New Ratin	g
4/24/2019	C:\Suspicious\vt.exe	COMODO	Added	COMOD		Unrecogni	zed
4/24/2019	C:\Suspicious\vt.exe	COMODO	Added	COMOD		Unrecogni	zed
4/24/2019	C:\Users\giri1\Downloads\U	COMODO	) Changed	COMOD	Unrecognized	Malicious	
4/24/2019	C:\Program Files (x86)\Goog	COMODO	Added	COMOD		Trusted	
4/24/2019	C:\Windows\Temp\CR_10F5	COMODO	Added	COMOD		Trusted	
4/24/2019	C:\Program Files (x86)\Goog	COMODO	Added	COMOD		Trusted	
4/24/2019	C:\Suspicious\8200755cbed	COMODO	Added	COMOD		Malicious	
4/24/2019	C:\Suspicious\poison1\smb	COMODO	Added	COMOD		Malicious	
4/24/2019	C:\Suspicious\poison2\smb	COMODO	Added	COMOD		Malicious	

- Date & Time When the event occurred.
- Path The location or the SHA 1 hash value of the file that was changed.
- Modifier The service or user that made the change.
- Action Whether the file was added, removed, or assigned a new rating
- Property Whether the current trust rating was assigned by Comodo, an administrator, or a user.
- Old Rating The trust rating of the file before the change.
  - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.
- New Rating The trust rating of the file after the change.
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log.
- Refresh Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

#### 5.4.10.1. Filter 'File List Changes' Logs

Filters allow you to view a specific sub-set of logs. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters**

Creating Trust Online

• Click 'Filter by Date and Time' to display logs for a specific time period:

COMODO View Logs - Current	t week				?	_		×
SHOW File List Changes	<b>⊤</b> Advanced Filter	Filter by Date and Time	Gen log file	X Cleanup log file	Exp		t) Refres	:h
Date & Path	Modifier	🔘 (No filterin				New	(Rating	
8/1/2017 C:\Program Files\COMODO	D\ COMOD	<ul> <li>Within las</li> <li>Except las</li> </ul>		+ hour(s)		Trus	ted	
8/1/2017 C:\Program Files\COMODO	D\ COMOD	Today				Trus	ted	
8/1/2017 C:\Program Files\COMODO	D\ COMOD					Trus	ted	
8/1/2017 C:\Program Files\COMODO	D\ COMOD	<ul> <li>Current m</li> <li>Within the</li> </ul>				Trus	ted	
8/1/2017 C:\Program Files\COMODO	D\ COMOD	08/01/	2017 - 08	/01/2017 •		Trus	ted	

- No filtering Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

Date &	Path	Modifier	Action	
4/11/20	C:\ProgramData\Comodo\C	. COMODO	Changed	COMOD.
4/11/20	D:\Su Show advanced filt	er DMODO	Added	COMOD.
4/11/20	D:\Su Today	DMODO	Added	COMOD.
4/11/20	C:\Pro Current week	DMODO	Added	COMOD.
4/11/20	C:\WI Entire period	моро	Added	COMOD.
4/11/20	D:\COMODO\COMODO Int	COMODO	Added	

#### **Advanced Filters**

You can further refine which events are displayed according to specific filters. The following additional filters are available:

COMODO Creating Trust Online\*

- Location Displays only change logs based on entered file location.
- Modifier Displays logs based on who assigned the rating (user, admin, or Comodo).
- Action Displays only change logs for selected actions such as (Added, Removed or Changed).
- **Property** Displays only change logs based on file rating done by such as (Administrator, User, and Comodo rating).
- Old Rating Displays only change logs based on the old file rating.
- New Rating Displays only change logs based on the new file rating.

#### Configure advanced filters for File List Changes logs

- Click the 'Advanced Filter' button on the title bar.
- Select the filter you want then click 'Add' to apply it:

COMODO View Logs - Today	? —
SHOW File List Changes	Export
Date & Path Modifier Action Property Old Rating	
4/11/20 C:\ProgramData\Comodo\C COMODO Changed COMOD	
COMODO Advanced Filter	? ×
ADVANCED FILTER Location Location Modifier Action Property Old Rating New Rating	
APPLY	CANCEL

i. Location: Filter file list changes according to their CCS code. You can view file list changes in the 'Location' column of the log viewer. Selecting the 'Location' option will display drop-down and text entry fields.

COMODO Creating Trust Online\*

COMODO Advanced Filter	?	Х	
ADVANCED FILTER     +       Location     Add			
Location Contains C:/Program Files((x86)\Cuckoo Files\cuckoo.exe		$\otimes$	
Does Not Contain			
APPLY C	ANCE	L	

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Enter the location or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe in the text field, then only log entries with the same value in the 'Path' column will be displayed.

ii. **Modifier**: The 'Modifier' option enables you to filter the log entries based on who did the file list changes. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

COMODO Advanced Filter	?	×
ADVANCED FILTER + Add		
Modifier Equal User Comodo		$\otimes$
APPLY	CANCEI	

COMODO Creating Trust Online\*

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - User
  - Comodo
  - Administrator

For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs changes done by the user will be displayed.

Action: The 'Action' option allows you to filter log entries based on the 'Action' column of the log viewer. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

COMODO Advanced Filter			?	×
ADVANCED FILTER Action	+ Add			
Action Equal 🔻	Added	Changed		$\otimes$
		APPLY	CANCEL	

a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Added
- Changed
- Removed

For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of files that were removed from the file list will be displayed.

iv. **Property**: Allows you to filter log entries based on the file rating. Selecting the 'Property' option displays a drop-down box and a set of specific filter parameters.

COMODO Creating Trust Online\*

COMODO Advanced Filter		?	×
ADVANCED FILTER Property	+ Add		
Property Contains 💌	<ul> <li>Administrator Rating</li> <li>User Rating</li> <li>Comodo Rating</li> </ul>	(	S
	APPLY	CANCEL	

- a. Select 'Contains' or 'Does Not Contain' option from the drop down. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Administrator Rating
  - User Rating
  - Comodo Rating

For example, if you select 'Equal' from the drop-down and select 'User Rating' checkbox, only the logs of files that were rated by the user will be displayed.

v. **Old Rating**: Allows you to filter log entries based on old file rating before it's rating was changed. Selecting the 'Old Value' option displays a drop-down and a set of specific filter parameters.

COMODO Advanced Filter		?	×
ADVANCED FILTER Location	+ Add		
Old Rating Contains	Unrecognized     Trusted     Malicious		$\otimes$
	APPLY	CANCEL	

a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Unrecognized
- Trusted

#### Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'Old Value' column will be displayed.

vi. New Rating: Allows you to filter log entries based on new file rating before it's rating was changed.

сомор	O Advanced Filter		? ×
ADVANCED FILT	ER T	<b>∔</b> Add	
New Rating	Contains Contains Does Not Contain	Unrecognized Trusted     Malicious	$\otimes$
		APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - Unrecognized
  - Trusted
  - Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'New Value' column will be displayed.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'File List Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

#### 5.4.11. Vendor List Changes Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Click the 'Show' drop-down at top-left
- Select 'Vendor List Changes' from the menu
- CCS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CCS
  allows unknown files which are digitally signed by one of these trusted vendors to run. Click 'Settings' > 'File
  Rating' > 'Vendor List' to view the list.
- · You can also add new vendors, and change the rating of existing vendors. Admin / User ratings supersede

COMODO Creating Trust Online\*

#### the Comodo rating.

- The files published by these vendors are rated depending on the current rating assigned to the vendor
- Any changes to vendors in the list are logged in 'Vendor List Changes'.

#### View 'Vendors List Changes' Logs

- Click 'Tasks' on the CCS home screen
  - Click 'Advanced Tasks' > 'View Logs'
    - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Vendor List Changes' from the 'Show' drop-down

ном		₹	ī		×	∍	Ð
Vendor List	Changes 🗸 Ad	lvanced Filter	Filter by Date and Time 4	Open log file <sup>Cle</sup>	anup log file	Export	Refres
Date &	Vendor	Modifier	Action	Property	Old Rating	N	ew Rating
4/23/201	LAVASOFT SOFTWARE CANA	COMODO	Added	COMOD		U	nrecognized
4/16/201	Valeriy Sokolov	COMODO	Changed	COMOD	Unrecognized	d U	nrecognized
4/16/201	Digital Wave Ltd	COMODO	Changed	COMOD	Unrecognized	d U	nrecognized
4/16/201	Digital Wave Ltd	COMODO	Added	COMOD		U	nrecognized
4/16/201	Valeriy Sokolov	соморо	Added	COMOD		U	nrecognized
4/12/201	VideolQ	User	Changed	User rating	Unrecognized	d Tr	usted
4/12/201	VideoLAN	User	Changed	User rating	Trusted	U	nrecognized
4/12/201	VideolQ	User	Changed	User rating	Trusted	U	nrecognized
4/11/201	Threatstar B.V.	COMODO	Added	COMOD		U	nrecognized

- Date & Time When the change event occurred.
- Vendor The name of the software publisher
- Modifier Who made the change (User or Comodo).
- · Action Whether the vendor was added, removed, or assigned a new rating
- Property Whether the current rating was assigned by Comodo, an admin, or a user.
- Old Rating The trust rating of the vendor before the change.
  - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.
- New Rating The trust rating of the vendor after the change.
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log.

COMODO Creating Trust Online\*

• Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

#### 5.4.11.1. Filter 'Vendor List Changes' Logs

Filters allow you to view a specific sub-set of logs. The following types of filters are available:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters**

• Click 'Filter by Date and Time' to view logs for a specific time period:

сомо	DO View Logs - Entire	period	~			? —
SHOW <mark>Vendor List</mark>	Changes 🔹	<b>⊤</b> Advanced Filter	Filter by Date and Time	Copen log file	X Cleanup log file	Export
Date &	Vendor	Modifier	(No filterin			New
4/23/201	LAVASOFT SOFTWARE CA	NA COMOD	<ul> <li>Within last</li> <li>Except last</li> </ul>		+ hour(s)	Vnred
4/16/201	Valeriy Sokolov	COMOD	🔿 Today			Unre
			O Current w	eek		
			O Current m	onth		
			O Within the	period of		
			04/24/2	2019 👻 - 04	/24/2019 🔻	

- **No filtering** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Display all logged events for today.
- **Current Week** All events logged during this week. The current week is calculated as the previous Sunday to the next Saturday.
- **Current Month** Display all events logged from the 1<sup>st</sup> of this month.
- Custom Filter Select specific 'To' and 'From' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.

COMODO Creating Trust Online\*

HOW Vendor List Cha	anges	۲		<b>▼</b> vanced Filter	Filter by Date and Time	Dpen lo	g file CI	¥ eanup log file	
Date & Ve	endor			Modifier	Action	1	Property	Old Rating	
4/23/201 LA	VASOFT	SOFTWARE CA	NA	COMODO	Added	(	COMOD		
4/16/201 Va	aleri	Refresh Show advanced Export	filter	OMODO	) Changed	(	COMOD	Unrecogniz	
		Today		-					
		Current week ၂	հղ						
		Current month Entire period							

#### **Advanced Filters**

- Click the 'Advanced Filter' button in the title bar OR right-click inside the log viewer module and choose 'Advanced Filter'
- Select the filter you want and click 'Add' to apply it:

COMODO View Logs - Entire peri	od				?	
SHOW Vendor List Changes	<b>⊤</b> Advanc Filter	ilter by Date and Time	Dpen log file	<b>≭</b> Cleanup log file	Export	
Date & Vendor	Modifier	Action	Property	Old Rating	)	
4/23/201 LAVASOFT SOFTWARE CANA	. COMODO	Added	COMOD.			
4/16/201. Valeriv Sokolov	COMODO	Changed	COMOD.	Unrecoan		
					?	×
ADVANCED FILTER Property Vendor Modifier Action Property Old Rating New Rating	+ Add					
			APPLY		CANCEL	

COMODO Creating Trust Online\*

- There are 6 categories of filters that you can add. Each of these can be further refined by selecting or deselecting parameters, or by typing a filter string as criteria.
- You can add and configure any number of filters in the 'Advanced Filter' dialog.
- · Click 'Apply' after adding the filter(s) to view the filtered results

The following filters are available:

Vendor: Filter the entries based on the name of the software publisher.

Select 'Vendor' from the drop-down and click 'Add'

COMODO Advanced Filter	?	×
ADVANCED FILTER Vendor Add		
Vendor Contains		$\otimes$
APPLY	CANCE	L

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Not Equal' will invert filter criteria.
- b) Enter the name of the vendor in full or part as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered "Digital", in the text field only those log entries related to the vendors who has contain "Digital" as a part in their name will be displayed.

Modifier - Filter the entries based on who made the changes in the 'Vendor List', whether the User or Comodo.

Select 'Modifier' from the drop-down and click 'Add'

COMODO Advanced Filter	? ×
ADVANCED FILTER Add	
Modifier Equal	$\otimes$
APPLY	CANCEL

a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

User

COMODO Creating Trust Online\*

#### Comodo

Action - Filter the entries based on the change made to the Vendor List, whether you want to view events related to addition of vendors, removal of vendors and / or changes to the vendor trust ratings.

Select 'Action' from the drop-down and click 'Add'

COMODO Advanced Filter			? ×
ADVANCED FILTER Action	<b>∔</b> Add		
Modifier Equal	User	Comodo	$\otimes$
Action Equal 💌	Added	Changed	$\otimes$
		APPLY	CANCEL

- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
- Added
- Changed
- Removed

**Property** - Filter entries based on who assigned the trust rating to the vendor. For example you might want to only view vendors whose rating was set by Comodo.

Select 'Property' from the drop-down and click 'Add'

COMODO Creating Trust Online\*

COMODO Advanced Filter			?	×
ADVANCED FILTER Property	<b>∔</b> Add			
Property Contains		ninistrator Rating 🗌 User Rating nodo Rating		$\otimes$
		APPLY	CANCE	L

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
- Administrator rating
- User rating
- Comodo rating

**Old Rating** - Filter entries related to vendors that had a specific trust rating before the change. For example you might want to only view vendors whose trust rating was 'Unrecognized' before the change.

• Select 'Old Rating' from the drop-down and click 'Add'

COMODO Advanced Filter	?	×
ADVANCED FILTER Old Rating Add		
Property Contains   Administrator Rating User Rating  Comodo Rating		$\otimes$
Old Rating Contains		$\otimes$
APPLY C	ANCEL	

COMODO

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the rating to refine your search. The parameters available are:
- Trusted
- Unrecognized
- Malicious

**New Rating** - Filter entries related to vendors that have a specific trust rating after the change. For example you might want to view only the log entries related to vendors whose trust rating is changed to 'Trusted'.

Select 'New Rating' from the drop-down and click 'Add'

COMODO Advanced Filter				? >	<
ADVANCED FILTER New Rating	<b>∔</b> Add				
New Rating Contains	•	Unrecognized Malicious	Trusted	$\otimes$	
			APPLY	CANCEL	

- a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the rating to refine your search. The parameters available are:
- Trusted
- Unrecognized
- Malicious

**Note**: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' to view the filtered results.
- Remove all filters and click 'Apply' to view the full list again.

#### 5.4.12. Configuration Changes

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Configuration Changes' from the 'Show' drop-down
- Configuration change logs are a record of changes to CCS settings

#### View configuration change logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
  - Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Configuration Changes' from the 'Show' drop-down

Creating Trust Online\*

Configuration Changes Filter and Time Open log file file Export Kerresh	SHOW		<b>⊤</b> Advance	ed Filter b			🗶 Cleanup log		•	Ð	
R11/201Firewall: ModeOption CAdministAllowed ApplicationSafe ModeDisabled8/1/201Firewall: Predefined pChangedAdministAllowed Application <object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministFtp Client<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministBlocked Application<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministBlocked Application<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministOutgoing Only<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministWeb Browser<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministEmail Client<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministSystem<object tlags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: ApplicationChangedAdministSystem<object device<="" td=""><object device<="" td="">8/1/201Firewall: ApplicationChangedAdministSystem<object device<="" td=""><object device<="" td=""></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object>	Configurati	on Changes				Open log file		Ex	port	Refres	h
B/1/201Firewall: Predefined pChangedAdministAllowed Application <object flags="&lt;/th"><object flags="&lt;/th">B/1/201Firewall: Predefined pChangedAdministFtp Client<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministBlocked Application<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministBlocked Application<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministOutgoing Only<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministWeb Browser<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministEmail Client<object flags="&lt;/td"><object flags="&lt;/td">B/1/201Firewall: Predefined pChangedAdministSystem<object plags="&lt;/td"><object plags="&lt;/td">B/1/201Firewall: ApplicationChangedAdministSystem<object device<="" td=""><object device<="" td="">B/1/201Firewall: ApplicationChangedAdministSystem<object device<="" td=""><object device<="" td=""></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object></object>	Date &	Component	Action	Modifier	Name		Old Setting	)	New Se	etting	ć
8/1/201Firewall: Predefined pChangedAdministFtp Client <object flags="&lt;/th"><object flags="&lt;/th">8/1/201Firewall: Predefined pChangedAdministBlocked Application<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministDutgoing Only<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministWeb Browser<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministWeb Browser<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: Predefined pChangedAdministEmail Client<object flags="&lt;/td"><object flags="&lt;/td">8/1/201Firewall: ApplicationChangedAdministSystem<object device<="" td=""><object plags="&lt;/td"></object></object></object></object></object></object></object></object></object></object></object></object></object></object>	8/1/201	Firewall: Mode	Option C	Administ			Safe Mode		Disable	ed	
8/1/201       Firewall: Predefined p       Changed       Administ       Blocked Application <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Outgoing Only       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Outgoing Only       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Web Browser       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Email Client       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Application       Changed       Administ       System       <object device<="" td=""> <object device<="" td=""></object></object></object></object></object></object></object></object></object></object></object></object>	8/1/201	Firewall: Predefined p	Changed	Administ	Allowe	d Application	<object fla<="" td=""><td>igs=</td><td><objec< td=""><td>t Flags=</td><td></td></objec<></td></object>	igs=	<objec< td=""><td>t Flags=</td><td></td></objec<>	t Flags=	
8/1/201       Firewall: Predefined p       Changed       Administ       Outgoing Only <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Web Browser       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Email Client       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Email Client       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Application       Changed       Administ       System       <object device<="" td=""> <object device<="" td=""></object></object></object></object></object></object></object></object></object></object>	8/1/201	Firewall: Predefined p	Changed	Administ	Ftp Cli	ent	<object fla<="" td=""><td>igs=</td><td><object< td=""><td>t Flags=</td><td></td></object<></td></object>	igs=	<object< td=""><td>t Flags=</td><td></td></object<>	t Flags=	
8/1/201       Firewall: Predefined p       Changed       Administ       Web Browser <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Predefined p       Changed       Administ       Email Client       <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Application       Changed       Administ       System       <object device<="" td=""> <object device<="" td=""></object></object></object></object></object></object>	8/1/201	Firewall: Predefined p	Changed	Administ	Blocke	d Application	<object fla<="" td=""><td>igs=</td><td><object< td=""><td>t Flags=</td><td></td></object<></td></object>	igs=	<object< td=""><td>t Flags=</td><td></td></object<>	t Flags=	
8/1/201       Firewall: Predefined p       Changed       Administ       Email Client <object flags="&lt;/td"> <object flags="&lt;/td">         8/1/201       Firewall: Application       Changed       Administ       System       <object device<="" td=""> <object device<="" td=""></object></object></object></object>	8/1/201	Firewall: Predefined p	Changed	Administ	Outgo	ing Only	<object fla<="" td=""><td>igs=</td><td><objec< td=""><td>t Flags=</td><td></td></objec<></td></object>	igs=	<objec< td=""><td>t Flags=</td><td></td></objec<>	t Flags=	
8/1/201       Firewall: Application       Changed       Administ       System <object device<="" td=""> <object device<="" td=""></object></object>	8/1/201	Firewall: Predefined p	Changed	Administ	Web B	rowser	<object fla<="" td=""><td>igs=</td><td><object< td=""><td>t Flags=</td><td></td></object<></td></object>	igs=	<object< td=""><td>t Flags=</td><td></td></object<>	t Flags=	
	8/1/201	Firewall: Predefined p	Changed	Administ	Email	Client	<object fla<="" td=""><td>igs=</td><td><objec< td=""><td>t Flags=</td><td></td></objec<></td></object>	igs=	<objec< td=""><td>t Flags=</td><td></td></objec<>	t Flags=	
8/1/201 Firewall: Application Added Administ COMODO Client - Se <object device<="" td=""><td>8/1/201</td><td>Firewall: Application</td><td>Changed</td><td>Administ</td><td>System</td><td>n</td><td><object de<="" td=""><td>vice</td><td><object< td=""><td>t Device</td><td></td></object<></td></object></td></object>	8/1/201	Firewall: Application	Changed	Administ	System	n	<object de<="" td=""><td>vice</td><td><object< td=""><td>t Device</td><td></td></object<></td></object>	vice	<object< td=""><td>t Device</td><td></td></object<>	t Device	
	8/1/201	Firewall: Application	Added	Administ	COMO	DO Client - Se			<object< td=""><td>t Device</td><td></td></object<>	t Device	

- **Date & Time** When the configuration change was done.
- Component The CCS interface that was modified.
- Action Short description of the change made to the CCS component. For example, if a setting was changed, or an exclusion was created.
- **Modifier** The service or user that made the change. Possible modifiers include 'User', 'Antivirus Alert', 'Auto-Learn', 'Firewall Alert', 'HIPS Alert', 'Containment Alert', 'Scheduler' and 'Comodo'.
- Name The item featured in the modification. This will vary depending on the component.
- **Old Setting** The value before the configuration change.
- New Setting The value after the configuration change.
  - Pace your mouse over an entry in the 'Old Value' or 'New Value' column to view the full setting string
- Export Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** Browse to and view a saved log file.
- Cleanup log file Delete the selected event log.
- **Refresh** Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

#### 5.4.12.1. Filter 'Configuration Changes' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

#### Preset Time Filters

COMODO Creating Trust Online\*

#### Advanced Filters

#### **Preset Time Filters**

• Click 'Filter by Date and Time' to display logs for a specific time period:

COMODO View Logs - Curr	ent week			?	_		$\times$
SHOW Configuration Changes	<b>⊤</b> Advance Filter		Filter by Date and Time     Image: Clean up log Open log file     Clean up log file		port	र् Refres	h
Date & Component	Action	Мо	(No filtering)		New S	etting	^
7/31/20 Files Group	Changed	Adr	Within last     1		<object< td=""><td>ct Name</td><td></td></object<>	ct Name	
8/1/201 Files Group	Changed	Adr	─ Today		<object< td=""><td>ct Name</td><td></td></object<>	ct Name	
8/1/201 Files Group	Changed	Adr	Current week		<object< td=""><td>ct Name</td><td></td></object<>	ct Name	
7/31/20 Files Group	Changed	Adr	<ul> <li>Current month</li> <li>Within the period of</li> </ul>		<object< td=""><td>ct Name</td><td></td></object<>	ct Name	
8/1/201 HIPS Predefined Policy	Removed	Adr	08/01/2017 💌 - 08/01/2017 💌	]			

- **No filtering** Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.

nent	Action	Modifier	Name	▼ Old Setting	N
roup	Changed	Adm	Refresh	<object name<="" td=""><td>&lt;0</td></object>	<0
roup	Changed	Adm	Show advanced filter Export	<object name<="" td=""><td>&lt;0</td></object>	<0
roup	Changed	Adm	Today	<object name<="" td=""><td>&lt;0</td></object>	<0
roup	Changed	Adm	Current week Current month	<object name<="" td=""><td>&lt;0</td></object>	<0
redefined Policy	Removed	Adm	Entire period	<object flags="&lt;/td"><td></td></object>	
redefined Policy	Changed	Administ.	Windows System App	<object flags="&lt;/td"><td>&lt;:</td></object>	<:

#### **Advanced Filters**

You can further refine which events are displayed according to specific filters. The following additional filters are available:

COMODO Creating Trust Online\*

- Action: Displays only logs for the selected action(s). Example actions are add, remove and change of rules.
- **Modifier:** Filters logs based on the source of the change. Example sources include the user making a change at an alert, auto-learning, the scheduler, Comodo, Administrator and so on.
- Name: Filters logs based on the name of the object.
- Component: Filters logs according to changes in selected CCS components and settings

#### **Configure Advanced Filters for Configuration Changes logs**

1. Click the 'Advanced Filter' button from the title bar or right-click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu.

The Advanced Filter' interface for 'Configuration Changes' logs will open:

2. Select a filter from the 'Advanced Filter' drop-down and click 'Add'.

сомо	DO View Logs - Toda	у			?
SHOW Configurati	on Changes	Advanced Filter	Compen log file	X Cleanup log file	
Date &	Component	Action Modifier Name		Old Setting	
4/11/20	Elevation Alerts: Defa	Option C User		Run in the Co	
сомог	<b>DO</b> Advanced Filter				? ×
ADVANCED FI		+ Add			
Action Modifier Name					
Component					
			AP	PPLY	CANCEL

i. Action: Allows you to filter log entries based on the actions executed. These include a change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

#### COMODO Creating Trust Online\*

COMODO Advanced Filter			?	×
ADVANCED FILTER Action	+ Add			
Action Equal Equal Not Equal	<ul> <li>Added</li> <li>Removed</li> </ul>	<ul><li>Changed</li><li>Option changed</li></ul>	(	$\otimes$
		APPLY	CANCEL	

- a. Select 'Equal' or 'Not Equal' option from drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
  - Added
  - Changed
  - Removed
  - Option changed

For example, if you choose 'Equal' from the drop-down and select 'Added' checkbox, only logs entries with the value 'Added' under 'Action' column will be displayed.

ii. **Modifier**: Allows you to filter log entries based on the entity that is responsible for the configuration change. It can be the user or the response given to an alert. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.

COMODO Advanced Filter			? ×
ADVANCED FILTER Modifier	+ Add		
Modifier Equal Equal User Not Equal	Auto learn	Antivirus Alert	⊗
Firewall Alert	HIPS alert	Containment alert	
Scheduler	Comodo	Administrator	
		APPLY C	ANCEL

COMODO Creating Trust Online\*

- a. Select 'Equal' or 'Not Equal' option from drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
  - User
  - Auto learn
  - Antivirus Alert
  - Firewall Alert
  - HIPS alert
  - Containment alert
  - Scheduler
  - Comodo
  - Administrator

For example, if you have chosen 'Equal' in the drop-down and selected 'Antivirus Alert ' checkbox, then, only logs entries related to the configuration changes effected by responses to 'Antivirus Alerts' will be displayed.

iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.

COMODO Advanced Filter		? ×
ADVANCED FILTER Name	+ Add	
Name Contains V Contains Does Not Contain	Surfer.exe	$\otimes$
Does Not Contain		
	APPLY	CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from drop-down. 'Does Not Contain' will invert your selected choice.
- b. Enter the name of the change, partly or fully as filter criteria in the text box.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.

iv. **Component:** Allows you to filter log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays drop down and the objects of CCS configuration.

Creating Trust Online\*

COMODO Advanced Filter			?	х
ADVANCED FILTER	+			
Component	Add			
Component Equal			$\otimes$	* 
Not Equal	Firewall: Auto rules for safe applications	E Firewall: Alert timeout		
Firewall: ICS computer	Firewall: TCP request alerts	E Firewall: UDP request alerts		
Firewall: ICMP request alerts	Firewall: Loopback alerts	Firewall: Protect ARP		
Firewall: Block ARP	Firewall: Block fragmented packets	E Firewall: Analyze protocol		
Firewall: Monitor non TCP/IP protocols	E Firewall: Predefined policy	E Firewall: Application policy		
Firewall: Global policy	Firewall: Network zone	Firewall: Blocked zone		
Firewall: Disable logging	Firewall: Alert Frequency	Firewall: Auto Detect Networks		Ŧ
		APPLY C	ANCEL	

- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll down the window to see all the objects.

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode' checkbox, only the log entries related to the change of Firewall mode will be displayed.

**Note:** More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- To clear filters, open the 'Advanced Filter' pane and remove each filter by clicking the 'X' button at the top
  right of each filter pane then click 'Apply'.

#### 5.4.13. Virtual Desktop Event Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Click 'Show' > 'Virtual Desktop Events'
- CCS records all events from the virtual desktop. Events that are recorded include:
  - Launch and close of the virtual desktop
  - Pause, resume, and terminate of a virtual desktop session
  - · Switching between the virtual desktop and the host desktop

#### View virtual desktop event logs

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'

COMODO

- · Alternatively, right-click on the CCS tray icon and select 'View Logs'
- Select 'Virtual Desktop Events' from the 'Show' drop-down:

HOW /irtual Desktop Events	₹ Advan Filte	iced Filter by Date	Open log file	X Cleanup log file	Export	🗘 Refresh
Date & Time	Action		Status			
7/8/2019 2:36:31 PM	Virtual Desktop Termir	nated	Success			
7/8/2019 2:24:36 PM	Session Terminated		Success	(Last Session D	uration: 00:03:27)	
7/8/2019 2:24:35 PM	Switched to Host		Success			
7/8/2019 2:24:34 PM	Switched to Virtual De	sktop	Success			
7/8/2019 2:21:44 PM	Session continued		Success			
7/8/2019 2:18:21 PM	Session Paused		Success			
7/8/2019 2:18:20 PM	Switched to Virtual De	sktop	Success			
7/8/2019 2:17:43 PM	Session Started		Success			
7/8/2019 2:17:39 PM	Switched to Virtual De	sktop	Success			

- Date & Time When the event occurred
- Action The operation executed
- Status Whether the action taken was a success or failure
- · Click any column header to sort the entries in ascending \ descending order

#### 5.4.13.1. Filter Virtual Desktop Event Logs

Filters allow you to view a specific sub-set of logs.

You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

#### **Preset Time Filters:**

• Click 'Filter by Date and Time' to view logs for a specific time period:

COMODO Creating Trust Online\*

	w Logs - Entire	period				? —
SHOW Virtual Desktop Events	•	<b>⊤</b> Advanced Filter	Filter by Date and Time	Copen log file	X Cleanup log file	Export
▼ Date & Time	Action		(No filterin)	g)	Tenerated	
7/8/2019 2:36:31 PM	Virtual Deskt	op Terminated	<ul> <li>Within last</li> </ul>	t <u>1</u>	thour(s)	·
170/2013 200031111	Thread Desite	op leinnatea	<ul> <li>Except las</li> </ul>	it 1	hour(s)	¥
7/8/2019 2:24:36 PM	Session Term	inated	🔿 Today			n <mark>: 00:03:</mark> 20
			O Current we	eek		State of the second
			O Current m	onth		
			O Within the	period of		
			07/08/2	2019 👻 - 07	/08/2019	

- **No filtering** Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- Within last Show all logs from a certain point in the past until the present time.
- Except last Exclude all logs from a certain point in the past until the present time.
- Today Show all events logged today, from 12:00 am to the current time.
- Current Week Show all events logged from the previous Sunday to today.
- Current Month Display all events logged from 1st of the current month to today.
- Within the period of Show logs between a custom date range.
- You can also right-click inside the log viewer module and choose the time period.

COMODO Vie	w Logs - Entire period				? —
SHOW Virtual Desktop Events	▼           Advanced           Filter	Tilter by Date and Time	Gen log file	X Cleanup log file	Export
▼ Date & Time	Action		Status		
7/8/2019 2:36:31 PM	Virtual Deskton Terminated Refresh		Success		
7/8/2019 2:24:36 PM	Show advanced filter		Success	(Last Session D	uration: 00:03
7/8/2019 2:24:35 PM	Export Today		Success		
	Current week				
	Current month Entire period				

Having chosen a **preset time filter**, you can further refine which events are shown by using the following additional parameters:

- Action Filter events by the virtual desktop activity
- Status Filter events by whether the operation was successful or not. Status options are 'Success' or 'Failure'.

COMODO Creating Trust Online\*

#### Configure advanced filters for antivirus events

- Click the 'Advanced Filter' button on the title bar.
  - Alternatively, right-click inside the log viewer module and select 'Show advanced filter'
- Select the filter you want then click 'Add' to apply the filter:

7/8/2019 2:36:31 PM     Virtual Desktop Terminated     Success	COMODO Vie	w Logs - Entire period			? —
7/8/2019 2:36:31 PM     Virtual Desktop Terminated     Success       7/8/2019 2:24:36 PM     Session Terminated     Success (Last Session Duration of the session Duration Duration of the session Duration Dur		Advanced Filing	er by Date Onen log file		
7/8/2019 2:24:36 PM Session Terminated Success (Last Session Duration 2) COMODO Advanced Filter ? □ × ADVANCED FILTER Status Action	▼ Date & Time	Action	Status		
COMODO Advanced Filter ? C × ADVANCED FILTER Status Action	7/8/2019 2:36:31 PM	Virtual Desktop Terminated	Success		
ADVANCED FILTER Status Action	7/8/2019 2:24:36 PM	Session Terminated	Success	(Last Session D	
	Status				
			APPLY		CANCEL

There are two categories of filters you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

- i. Action: The 'Action' option allows you to filter logs based on the virtual desktop activity
  - Select 'Action' from the drop-down then click 'Add':

COMODO Creating Trust Online\*

COMODO Advanced Filter		?		
ADVANCED FILTER	+ Add			
Action Equal	<ul> <li>Virtual Desktop Launched</li> <li>Session Started</li> <li>Session Continued</li> <li>Switched to Host</li> </ul>	<ul> <li>Virtual Desktop Terminated</li> <li>Session Paused</li> <li>Session Terminated</li> <li>Switched to Virtual Desktop</li> </ul>	$\otimes$	
		APPLY CA	NCEL	

You should now choose the actions by which you want to filter the logs:

- a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
  - Virtual Desktop Launched Shows the events at which the virtual desktop was started. This
    includes manual start and auto-launch of the virtual desktop when a specific user user logs-on
    to the computer.
  - Virtual Desktop Terminated Shows the events at which the virtual desktop was closed.
  - Session Started Shows the events at which a user started the virtual desktop by accepting to the disclaimer
  - Session Paused Shows the events at which a user suspended the virtual desktop
  - · Session Continued Shows the events at which a pauses session was resumed
  - · Session Terminated Shows the events at which a paused session was terminated
  - Switched to Host Shows the events at which a user paused the virtual desktop and moved to the real desktop
  - Switched to Virtual Desktop Shows the events at which a user re-opened to the virtual desktop from the real desktop
- ii. Status: The 'Status' option allows you to filter the log entries based on the success or failure of the action.
  - Select 'Status' from the drop-down then click 'Add':

COMODO Creating Trust Online\*

COMODO Advanced Filter		?	o x
ADVANCED FILTER Status	+ Add		
Action Equal 🔻	<ul> <li>Virtual Desktop Launched</li> <li>Session Started</li> <li>Session Continued</li> <li>Switched to Host</li> </ul>	<ul> <li>Virtual Desktop Terminated</li> <li>Session Paused</li> <li>Session Terminated</li> <li>Switched to Virtual Desktop</li> </ul>	$\otimes$
Status Equal 🔹	Success	☑ Failure	$\otimes$
		APPLY CAI	NCEL

- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
- Success: Displays events in which the virtual desktop actions were successfully executed (for example, a
  paused session was successfully resumed)
- Failure: Displays events at which the actions failed (for example, the user entered a wrong PIN and could not resume a paused session)

**Note**: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

Click 'Apply' for the filters to be applied to the 'Virtual Desktop Events' log viewer. Only those entries
selected based on your set filter criteria will be displayed in the log viewer.

COMODO Creating Trust Online\*

#### 5.5. Submit Files for Analysis to Comodo

- Click 'Tasks' > 'Advanced Tasks' > 'Submit Files'
- Files you submit from this interface are uploaded to Comodo's Valkyrie service for testing.
- Valkyrie is Comodo's file testing and verdicting system. It's purpose is to discover whether or not a file is malicious or safe to run.
- CCS rates files as either 'trusted', 'malicious' or 'unknown'.
- Files with no rating at all are automatically uploaded when they are executed, or if they are discovered by a rating scan.
  - Files that were awarded an unknown rating by admin, user or Comodo are not uploaded to Valkyrie.

Tip - You can also submit files to Valkyrie from the Quarantine and File List interfaces.

#### Upload files for analysis

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' then 'Submit Files'

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K HOME () SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	ADVANCED TASKS
Create Rescue Disk Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.	Clean Endpoint * Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager Open the task manager to view running security tasks in progress.	View Active Processes View the details of the processes active on this computer.
View Logs View a record of security events, activity and alerts.	Submit Files You can submit as many files as you wish to COM O for analysis.
	(?)
	? 🗆 ×
+ ¥ Add Remove	
Location	Q
Submit as False-Positive Submit to Valkyrie	SUBMIT CLOSE

• Click 'Add' at top right.

C	омоі	DO Sub	mit	?	×
	+ Add	X Remove			
	Files				Q
	Folders Running	Processes	Desktop\vir\rundll.exe		
		E:\Suspiciou	s file\eicar.com		

- There are three ways to select a file:
  - · Files Browse to the file or executable you want to add to the 'Submit Files' list.
  - Folders Browse to the folder you want to add. All files in the folder will be added to the 'Submit Files' list.
  - Running Processes Select a currently active process. The parent application of the process will be added to the 'Submit Files' list.
- Repeat the process to add more files
- Please note that 'Submit to Valkyrie' is pre-selected by default. You cannot change this setting.
- Click the 'Submit' button

The uploading process will commence. You can stop, pause/resume or send the submission process to background by clicking respective buttons.

COMODO Valkyrie Submit Files		?	—		×
C:\old man files\give_a_dog_a_bone.exe					
File Name	State				
C:\Program Files (x86)\Lantiv\Lantiv Timetabler 6.2.36\LanTime.exe	Ċu	pload	ling		
C:\Program Files (x86)\MB Free Astrology Birth Chart\MBFreeAstrologyBirthCh	Ö P	endin	g		
♀ <u>C:\Program Files (x86)\MyFreeWeather\MyWeather.exe</u>	Ö P	endin	g		
C:\Astrolog\Astrolog.exe	Ö P	endin	g		
<u>C:\Program Files\AgeCalculator.exe</u>	Ċ P	endin	g		
STOP    PAUSE	s	END	TO BACI	KGROUN	ID

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen shows the results:

Creating Trust Online\*

	/alkyrie Submit Files		?	—		×
100%	C:\Program Files\AgeCalculator.exe					
File Name		Sta	te			
C:\Program Files (x)	86)\Lantiv\Lantiv Timetabler 6.2.36\LanTime.exe	0	Uploa	ded		
C:\Program Files (x)	86)\MB Free Astrology Birth Chart\MBFreeAstrologyBirthCh	0	Alread	y submit	ted	
G:\Program Files (x	86)\MyFreeWeather\MyWeather.exe	0	Alread	y submit	ted	
C:\Astrolog\Astrolo	og.exe	0	Alread	y submit	ted	
C:\Program Files\A	geCalculator.exe	0	Alread	y submit	ted	
× CLOSE			SEND	TO BAC	KGROUN	ID

- Uploaded The file was accepted for review by our research labs. The file's signature was not among the list of files waiting to be tested.
- **Already submitted** The file has already been uploaded by another CCS user and is queued for testing. This means the file was not uploaded from your machine.

Comodo will analyze all submitted files. If the file is found to be trustworthy it will be added to the Comodo safe list (white-listed). Conversely, if it is found to be malicious then it will be added to the virus database (black-listed).

Click 'Settings' > 'File List' > 'Submitted Files' to view all files uploaded to our labs. See **Submitted Files** for more details.

#### 5.6. View Active Process List

- Click 'Tasks' > 'Advanced Tasks' > 'View Active Processes'
- The active process list shows all processes started by applications currently running on your system.
- CCS can identify the parent application of a process to detect when a non-trusted application is trying to spawn a trusted application. CCS can then deny access rights to the trusted application.
- This deep level of inspection protects you against malware that tries to use trusted software to launch an attack.
- The interface also lets you run an online lookup on the parent application. Here, you can check its trust rating on the latest cloud databases. You can also submit an application to Comodo for analysis.

#### View the active process list

- Click 'Tasks' > 'Advanced Tasks'
- Click the 'View Active Processes' tile:

COMODO Creating Trust Online\*

Secure All systems		and running	ADVANCED TASKS		
ENERAL IASKS FIREWALL IAS	INS CONT		ADVANCED IASKS	_	
Create Rescue Disk Create a bootable CD clean up heavily infect	or USB Flash	Drive to	Clean End Run COMO persistent	DOO Cleaning Essent	ials tool to cle
Open Task Manage Open the task manage tasks in progress.	er to view rur	$\sum$	computer. 介 <sub>国</sub> Submit Fi	ls of the processes	
		1			
OMODO Active Pro	ocesses List	K		? -	- 🗆
OMODO Active Pro	PID	Company	User Name	? - Restriction	- 🗆 Rating
		Company Microsoft Wi	User Name UMFD-1		
Application	PID			Restriction	Rating
Application fontdrvhost.exe	PID 776	Microsoft Wi	UMFD-1	Restriction Disabled	Rating Trusted
Application  fontdrvhost.exe  dwm.exe	PID 776 968	Microsoft Wi Microsoft Wi	UMFD-1 DWM-1	Restriction Disabled Disabled	Rating Trusted Trusted
Application   fontdrvhost.exe  dwm.exe  explorer.exe	PID 776 968 4232	Microsoft Wi Microsoft Wi Microsoft Wi	UMFD-1 DWM-1 John	Restriction Disabled Disabled Disabled	Rating Trusted Trusted Trusted
Application   fontdrvhost.exe  dwm.exe  explorer.exe  MSASCuiL.exe	PID 776 968 4232 6584	Microsoft Wi Microsoft Wi Microsoft Wi	UMFD-1 DWM-1 John John	Restriction Disabled Disabled Disabled Disabled Disabled	Rating Trusted Trusted Trusted Trusted
Application	PID 776 968 4232 6584 336	Microsoft Wi Microsoft Wi Microsoft Wi	UMFD-1 DWM-1 John John	Restriction Disabled Disabled Disabled Disabled Disabled Disabled Eully Virtu	Rating Trusted Trusted Trusted Trusted Unknown

- Application The name of the parent executable of the process.
- **PID** The unique process identifier.
- Company The vendor who created the software
- User Name The user account under which the program is run
- Restriction The security limitations placed on the program by the CCS containment module.
- Rating The trust level of the program as per the local file list ('Settings' > 'File Rating' > File List')
- Right-click on any process to open the context sensitive menu:

😡 MyWeather.exe	3784	John	Disabled	Trusted
A BiHMS.exe	Show Full Path	·	Fully Virtu	Unknown
🌀 🗏 chrome.exe	Show Contained Only Show COMODO Processes Ru	inning Inside the Container	Disabled	Trusted
	Add to Trusted Files Online Lookup Submit Submit to Valkyrie Jump to Folder			
	Show Activities			

- Show Full Path View the install location of the parent program
- Show Contained Only Hides all processes except those running in the container.
- Show COMODO Processes Running Inside the Container Hide all processes except Comodo processes running in the container.
- Add to Trusted Files Assign 'Trusted' status to the executable that started the process. This allows the file to run as normal in future. You can view trusted files in the CCS 'File List' ('Settings' > 'File Rating' > 'File List').
- **Online Lookup** Search for the executable in Comodo's global blacklist and whitelist. The results will tell you if the file is clean, malicious or unknown.
- **Submit to Valkyrie** Uploads the parent executable to Comodo Valkyrie for analysis. Valkyrie is Comodo's file testing and verdicting system that analyzes the submitted files with a range of static and dynamic tests to determine the file's trust rating. The files are added to the Comodo safe list (white-listed) or to the database of virus signatures (blacklisted) depending on the results.
- Jump to Folder Opens the folder containing the executable.
- Show Activities Shows all actions by processes of the application. This option is available only for contained applications and if VirusScope is enabled ('Settings' > 'Advanced Protection > 'VirusScope').
- Click the 'More' button to open Comodo KillSwitch an advanced system monitor that lets you quickly identify and terminate any unsafe processes on your system.

📧 🗆 services.exe	612	Microsoft Wi	SYSTEM	Disabled	Trusted	
						~
				MORE	CLOSE	

If KillSwitch is not yet installed, clicking this button will prompt you to download the application. See **Identify and Kill Unsafe Running Processes** for more details.

#### View 'Active Processes' list of contained applications

Click the shortcut on the widget to view processes by applications inside the container. These applications include:

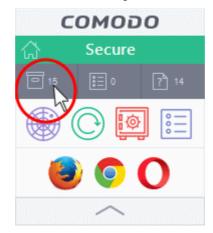
- Auto-Containment Applications that are made to run in the container by a containment rule. See 'Auto-Containment Rules' for more details on defining auto-containment rules.
- Run Virtual Applications that were manually run in containment. See 'Run an Application in Containment' for more details.

COMODO Creating Trust Online\*

- Applications that are run inside the containment using the context sensitive menu Click here for more details.
- Running browsers inside the containment from the widget Click here for more details.
- Programs that are added manually See 'Auto-Containment Rules' for more details.

#### View active processes from contained applications

• Click the first box in the second row in the CCS Widget.



The Active Processes List (Contained Only) screen appears:

Application	PID	Company	User Name	Restriction	Rating
O opera.exe	6480	Opera Softw	John	Fully Virtu	Unknown
🦻 🗏 firefox.exe	7988	Mozilla Corp	John	Fully Virtu	Trusted
🍯 firefox.exe	3324	Mozilla Corp	John	Fully Virtu	Trusted
🍯 firefox.exe	6692	Mozilla Corp	John	Fully Virtu	Trusted
🍯 firefox.exe	5088	Mozilla Corp	John	Fully Virtu	Trusted
🍯 firefox.exe	7612	Mozilla Corp	John	Fully Virtu	Trusted
dllhost.exe	7924	Microsoft Wi	John	Fully Virtu	Trusted
🏠 BiHMS.exe	6344		John	Fully Virtu	Unknown

COMODO Creating Trust Online\*

# 6.CCS Advanced Settings

- Click 'Settings' at the top-left of the CCS home screen
- The settings area lets you configure every aspect of the operation, behavior and appearance of Comodo Client Security.
  - General settings Specify top-level preferences regarding the interface, updates and event logs.
  - **Security settings** Configure each CCS security module. Modules include antivirus, firewall, filerating and containment.

HOME () SETTING	·)					
Secure   All sys		and running				
OMODO Advanc	ed Settings		?	-		×
General Settings User Interface	User	Interface				
Updates	Language:	English (United States) - By COMODO	•			
Logging	Show me	ssages from COMODO Message Center				
Configuration	Show not	ification messages				
Antivirus	Show des	ktop widget				
Firewall	Show info	ormation messages when tasks are minimized/se	ent to back	ground		
HIPS	Play soun	d when an alert is shown				
Containment	Show notific	ation messages				
File Rating						
Advanced Protection						
		ок		C/	NCEL	

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See **'Password Protection'** for more details.

Click the following links for help with specific settings:

- General Settings Configure the appearance and behavior of the application
  - Customize User Interface
  - Configure Virus database Updates
  - Log Settings
  - Manage CCS Configurations
- Antivirus Settings

•

Real-time Scanner Settings

COMODO Creating Trust Online\*

- Scan Profiles
- Firewall Settings
  - General Firewall Settings
  - Application Rules
  - Global Rules
  - Firewall Rule Sets
  - Network Zones
  - Port Sets
- HIPS Settings
  - General HIPS Settings
  - Active HIPS Rules
  - HIPS Rule Sets
  - Protected Objects HIPS
  - HIPS Groups
- Containment Settings
  - Containment Settings
  - Auto-Containment Rules
  - Protected Objects Containment
  - Virtual Desktop Settings
  - Containment An Overview
  - Unknown Files: The Scanning Process
- File Ratings
  - File Rating Settings
  - File Groups
  - File List
  - Submitted Files
  - Vendor List
- Advanced Protection
  - VirusScope Settings
  - Scan Exclusions
  - Device Control Settings
  - Script Analysis Settings
  - Miscellaneous

#### 6.1. General Settings

- Click 'Settings' > 'General Settings'
- The general settings area lets you customize the appearance and overall behavior of Comodo Client Security.
- You can configure the interface language, notifications, automatic updates, logging, and more.

#### **Configure General CCS Settings**

- Click 'Settings' on the CCS home screen
- Click 'General Settings' on the left:

COMODO Creating Trust Online\*

COMODO Advanced	Settings	?	-		×
<ul> <li>Advanced</li> <li>General Settings</li> <li>User Interface</li> <li>Updates</li> <li>Logging</li> <li>Configuration</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> </ul>	Settings User Interface Language: English (United States) - By COMODO Show messages from COMODO Message Center Show notification messages Show desktop widget Show information messages when tasks are minimized/sent Play sound when an alert is shown Show notification messages	•	ground		×
<ul> <li>Advanced Protection</li> </ul>	οκ			ANCEL	

General settings is broken down into the following areas:

- User Interface
- Updates
- Logging
- Configuration

COMODO Creating Trust Online\*

#### 6.1.1. Customize User Interface

- Click 'Settings' > 'General Settings' > 'User Interface'
- The user interface tab lets you choose your preferred language, and customize the look and feel of the application.

COMODO Advance	ed Settings ? - D X
- General Settings	User Interface
User Interface	
Updates	Language: English (United States) - By COMODO
Logging	Show messages from COMODO Message Center
Configuration	Show notification messages
✓ Antivirus	Show desktop widget
✓ Firewall	□ Show information messages when tasks are minimized/sent to background
✓ HIPS	Play sound when an alert is shown
✓ Containment	Show notification messages
✓ File Rating	
✓ Advanced Protection	
	OK CANCEL

• Language Settings - Comodo Client Security is available in many different languages. Switch languages by clicking the 'Language' drop-down menu: (*Default = English (United States)*).

COMODO Creating Trust Online\*

	ed Settings		? — 🗆 X
<ul> <li>General Settings</li> <li>User Interface</li> </ul>	User I	nterface	
Updates	Language:	English (United States) - By COMODO English (United States) - By COMODO	-
Logging	Show mess	- الحربية By Community	
Configuration	Show notif	Български - Бу Соттипіту	
<ul> <li>Antivirus</li> </ul>	Show desk	中文(简体) - By COMODO 正體中文 - By Community	
✓ Firewall	Show infor	Hrvatski (Croatian) - By Community	ground
✓ HIPS	Play sound	Čeština - By Community Dansk - By Community	
<ul> <li>Containment</li> </ul>	Show notificat	Nederlands - By Community Eesti keel - By Community	
<ul> <li>File Rating</li> </ul>		Français - By Community Deutsch - By Community	
<ul> <li>Advanced Protection</li> </ul>		Ελληνικά - By Community Magyar - By Community	
		Italiano - By Community	
		日本語 - By Community	
		By Community - فارسی	
		Polski - By Community	
		Română - By COMODO	
		Русский - Ву СОМОДО	
		Српски - By Community	
		Español - By Community	
		Svenska - By Community	CANCEL
		Türkçe - By COMODO	CANCEL
		Українська – By Community	
		Tiếng Việt - By Community	Lucalitité)

 Show messages from COMODO Message Center - Message center messages keep you abreast of Comodo news and special offers. If enabled, the messages will periodically appear as small pop-ups. (Default = Disabled)



 Show notification messages - CCS system notices appear in the bottom right-hand corner of your screen (just above the tray icons). They inform you about any actions that CCS is taking, and any CCS status updates. (*Default = Disabled*)

Note - To view these messages, you also need to allow notifications from Comodo in Windows:

- Click the 'Show notification messages' link
- This opens the Windows 'Notifications and Actions' page
- Enable 'Get notifications from apps and other senders'
- Enable 'Comodo Client Security' in the senders list

COMODO Creating Trust Online\*

COMODO Advance	Settings ?
- General Settings	
User Interface	
Updates	Language: English (United States) - By COMODO
Logging	Show messages from COMODO Message Center
Configuration	Show notification messages
<ul> <li>Antivirus</li> </ul>	Show desktop widget
✓ Firewall	Show information messages when tasks are minimized/sent to backgrou
HIPS	Play sound when an alert is shown
<ul> <li>Containment</li> </ul>	Show notification messages
ettings	✓ - □ >
යි Home	Notifications & actions
Find a setting	occasionally when I sign in to highlight what's new and suggested
ystem	On On
- Display	Get tips, tricks, and suggestions as you use Windows On
₽ Display	Get notifications from apps and other senders
li) Sound	On
Notifications & actions	
) Focus assist	Get notifications from these senders
り Power & sleep	Select a sender to see more settings. Some senders might also have their own notification settings. If so, open the sender to change
	them.
→ Battery	COMODO Client - Security On
⊐ Storage	On: Banners, Sounds

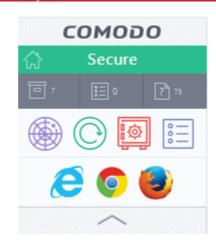
**Show desktop widget** - The desktop widget shows your overall security status, outgoing and incoming traffic, and any background tasks.

The widget also contains shortcuts to open CCS, to open the task manager, to open your browsers, and to visit social network sites.

Select this checkbox if you want the widget on your desktop. (Default = Disabled)

Tip: You can also enable or disable the widget by right-clicking on the CCS system icon.

COMODO Creating Trust Online\*



See The Widget for more details.

•

Show information messages when tasks are minimized/sent to background - CCS can show messages which explain what happens when you minimize or move a task:

COMODO Minimize Window X	COMODO Send To Background X
What is a Minimized Task? A task which doesn't consume as much resources as an active task.	What is a Background Task? A task which runs in the background without interfering with your normal PC activities.
Minimize Window action, where available, makes the task such as scanning or updating continue running with a lower priority compared to other programs. These tasks are going to take longer to complete but be less resource intensive.	Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.
Restoring the window to foreground will restore the previous priority back as well.	Please use Task Manager in order to access them later.
Do not show this message again OK	Do not show this message again OK

Disable this setting if you don't want to view these messages (*Default = Disabled*).

- Play sound when an alert is shown CCS plays a chime when it shows a security alert. (*Default = Disabled*).
- Click 'OK' for your settings to take effect

Note: In a managed network, CCS settings are governed by Endpoint Manager.

#### 6.1.1. Configure Virus Database Updates

- Click 'Settings' > 'General Settings' > 'Updates'
- This area lets you configure CCS program and database updates:

COMODO Creating Trust Online\*

	ed Settings	? – 🗆 X
- General Settings User Interface	O Updates	
Updates	Check for database updates every	1 🔹 hour(s) 🔻
Logging	Options	
Configuration	Do not check for updates if I am using these connection	tions
✓ Antivirus	Do not check for updates if running on battery	
✓ HIPS	Check for updates during Windows Automatic Mainte	enance
✓ Containment	Send requests to COMODO online services only if inte	ernet connection is present
✓ File Rating	Proxy and Host Settings	
✓ Advanced Protection		
		OK CANCEL

- Check for database updates every... Set how frequently CCS should check for application updates. Updates are downloaded from Comodo servers by default, but you can also set up a proxy to handle them if required. Select the interval in hours / days. (*Default and recommended* = every 1 hour)
- Do not check updates if am using these connections CCS will not check for updates if you are using specific internet connections. For example, you may not wish to check for updates when using a wireless connection you know is slow or insecure. (*Default = Disabled*)
  - Enable 'Do not check updates if am using these connections'.
  - Click the 'these connections' link.
  - Select the connection over which you do not want to check for updates.
  - Click 'OK'.

COMODO Creating Trust Online\*

) Advanced	l Settings	?	-		×
	O Updates				
	Check for database updates every	1 🔹	hour(s)	•	
	Options				
0	Do not check for updates if I am using <u>these connections</u>	>			
	<ul> <li>Do not cneck for updates if running on battery</li> <li>Check for updates during Windows Automatic Maintenance</li> </ul>				
	COMODO Connections	' [	x c		
	Connection Names				
	Ethernet				
	Ethernet 2				
	Ethernet 3				
	ок	CAN			

- **Do not check for updates if running on battery** CCS will not download updates if it detects your computer is on battery power. This is intended to extend battery lifetime on laptops. (*Default = Disabled*).
- Check for updates during Windows Automatic Maintenance Allow CCS to receive updates when Windows is updating itself (*Default = Disabled*).
- Send requests to COMODO online services only if internet connection is present By default, CCS automatically connects to Comodo servers for updates and essential services such as FLS, Endpoint Manager, and Valkyrie. This setting lets you disable these connection requests if you are not connected to the internet.

This is how CCS will proceed if you enable or disable this setting:

- Enabled + No internet connection CCS will not make requests to Comodo online services. A failure
  message is shown if you attempt a manual lookup, submit or update.
- Enabled + Connected to internet CCS makes requests to Comodo online services.
- Disabled + Connected to internet CCS makes requests to Comodo online services.
- **Disabled + No internet connection** CCS will make requests to Comodo online services, but will not be able to connect. An error message is shown.

#### (Default = Disabled)

- Proxy and Host Settings Specify the host from which this computer should collect updates.
  - By default, CCS downloads updates direct from Comodo servers. Alternatively, admins can download updates to a local server first.

COMODO Creating Trust Online\*

- Individual endpoints can then fetch updates from this local server instead of from Comodo servers. This helps save bandwidth and accelerates updates when a large number of endpoints are involved.
- The 'Proxy and Host Settings' area lets you point CCS at such a proxy/staging server.

Note: You need to install the 'ESM Update Mirror' utility to download updates to the local server. • Download the setup file from

- Download the setup file from https://drive.google.com/file/d/0B4qKr5xfENWBS0FOUHM2VDFQMnc/view.
- Run the setup file on a Windows server and follow the wizard to install the application
- Ensure that the service has started:
  - 'Run' > Enter 'services.msc' > locate 'Apache2.2'
  - Click the 'Start' link on the left if the service is not running

#### Configure updates via local update server

• Click 'Proxy and Host Settings' at the bottom of the updates interface:

сомодо Creating Trust Online<sup>4</sup>

O Advanced	Settings	? – 🗆 ×
	O Updates	
	Check for database updates every	hour(s) ▼
	Options	
	Do not check for updates if I am using <u>these connections</u>	
	Do not check for updates if running on battery	
	Check for updates during Windows Automatic Maintenance	
	Send requests to COMODO online services only if internet con	nection is present
	Proxy and Host Settings	
	COMODO Proxy and Host Settings ?	
	Use proxy	
	Host:	
	Port: 0	
	Use authentication	
	Login:	
	Password:	
	+ 🖌 🗶 t +	
	Add Edit Remove Move Up Move Down	
	Servers Servers	Status
	http://download.comodo.com	
	ок	CANCEL
	Click the 'Add' button	1.

Click the 'Add' button

COMODO Creating Trust Online\*

COMODO Proxy and Host Settings	?		×
Use proxy			
Host:			
Port: 0			
Use authentication			
Login:			
Password:			
+     *     t     +       Add     Edit     Remove     Move Up     Move Down	n		
Servers		Status	
tttps://download.comodo.com/			
COMODO Edit property Add a new host		?	×
ОК	c	ANCEL	

- Enter the IP address or hostname of the server (with 'http://' prefix)
- Repeat the process to add more local update servers

Creating Trust Online\*

COMODO Proxy and Host Settings	?		×
Use proxy			
Host:			
Port: 0			
Use authentication			
Login:			
Password:			
Image: Add     Image: Constraint of the second	'n		
Servers		Status	
https://download.comodo.com/			
http://10.100.11.11			
http://10.100.11.12			
ОК		CANCEL	

- Use the 'Move Up' and 'Move Down' buttons to choose the order in which servers should be consulted. CCS will download from the first server that contains new updates.
- · Use the status switches to activate or deactivate individual servers
- Click 'OK' for your settings to take effect.

#### 6.1.2. Log Settings

- Click 'Settings' > 'General Settings' > 'Logging'
- Comodo Client Security keeps detailed records of all antivirus, firewall, HIPS, containment, device control, VirusScope and autorun events.
- Logs are also created for 'Alerts Displayed', 'Tasks Launched', 'File List' changes, 'Vendor list changes' and 'CCS Configuration Changes'.
- Log settings let you specify the storage location, the maximum size of log files, and how CCS should react if the maximum file size is exceeded.

Note: You can view the logs themselves at 'Tasks' > 'Advanced Tasks' > 'View Logs'.

COMODO Creating Trust Online\*

#### **Configure log settings**

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Logging':

COMODO Advance	ed Settings ? — $\Box$ X
<ul> <li>General Settings</li> <li>User Interface</li> </ul>	Cogging
Updates	Logging options allow you to manage recording of critical events like malware events, firewall events, etc.
Logging	☑ Write to local log database (COMODO format)
Configuration	Write to syslog server
✓ Antivirus	Host Port 514
✓ Firewall	Write to remote server (JSON format)
✓ HIPS	Host O
✓ Containment	Token
✓ File Rating	□ Write to log file (CEF format)
✓ Advanced Protection	Path Browse
	☑ Write to Windows Event Log
	Log File Management
	When log file reaches 100 MB
	Keep on updating it removing the oldest records
	O Move it to the specified folder
	User Statistics
	Send anonymous program usage statistics to COMODO
	When this option is enabled, usage statistics (e.g. crashes, errors, clicks, etc.) about the product will be sent to COMODO anonymously. This information will be used by our engineers to improve the product's quality and is subject to COMODO's privacy policy.
	OK CANCEL

#### Logging

- Write to local log database (COMODO format) Enable or disable logs in Comodo format (*Default = Enabled*)
- Write to Syslog Server (CEF Format) CCS forwards the logs to an external Syslog server integrated with Endpoint Manager (EM). Enter the IP/hostname and port of the Syslog server in fields provided. (Default = Disabled).
- Write to remote server (JSON format) CCS forwards the logs over https to a server integrated with Endpoint Manager. (*Default = Disabled*).
  - Host Enter the IP address or the host name of the server
  - Port The port through which the server listens to the CCS logs
  - **Token** Enter the client authentication token so CCS can connect and forward logs to the server. The token is generated when you configure the HTTP Event Collector (HEC) on the server.
  - See https://docs.splunk.com/Documentation/Splunk/7.2.6/Data/UsetheHTTPEventCollector

COMODO Creating Trust Online\*

if you need help to setup the event collector and generate a token.

- Enter the IP/hostname and port of the server in fields provided. Enter the security token to access the remote server in the field provided.
- Write to Log file (CEF) Format CCS stores the logs at a specific local or network location. Click 'Browse' to select the storage location (Default = Disabled).
- Write to Windows Event Logs CCS logs are appended to 'Windows Event' logs . (Default = Enabled)
  - Type 'Event Viewer' in Windows search to view Windows logs

#### Log File Management

- Specify what should happen when the log file reaches a certain size. You can choose keep the older logs or discard them.
  - When log file reaches Enter the maximum size of a log file in MB. (Default = 100MB)
  - Keep on updating it removing the oldest records When a log file reaches the max. size, CCS will delete the earliest log entries to make room for the new entries. (Default = Enabled)
  - Move it to the specified folder When a log file reaches the max. size, CCS starts a new log file and moves the old one to a folder of your choice. (Default = Disabled)
    - Select the option and click 'the specified folder' to choose the storage folder:

☑ Write to Windows E	vent Log		
Log File Managem When log file reaches	100 MB		
<ul> <li>Keep on updating i</li> <li>Move it to the spectrum</li> <li>User Statistics</li> </ul>	t removing the oldest records		
	Pick a Directory	×	
	<ul> <li>Federal Bank Statements</li> <li>Old Man Apps</li> <li>old man files</li> <li>PerfLogs</li> <li>Program Files</li> <li>Program Files (x86)</li> <li>ProgramData</li> </ul>	•	
	ОК	Cancel	

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

COMODO Creating Trust Online\*

☑ Write to Windows Event Log	
Log File Management	
When log file reaches 100 MB	
○ Keep on updating it removing the oldest records	
Move it to <u>C:\CCS Logs</u>	
User Statistics	

#### **User Statistics**

- Send anonymous program usage statistics to Comodo Comodo collects usage details so we can analyze how our users interact with CCS. This real-world data allows us to create product improvements which reflect the needs of our users. If you enable this option, CCS will periodically send usage data to Comodo servers through a secure, encrypted channel. Your privacy is not affected because the data is anonymized. Disable this option if you don't want to send usage details to Comodo. (Default = Enabled)
- Click 'OK' for your changes to take effect

#### 6.1.3. Manage CCS Configurations

- Click 'Settings' > 'General Settings' > 'Configuration'
- CCS lets you export your current security settings as a profile. You can then import the profile on another computer with CCS installed, and avoid having to configure everything again.
- Exporting your settings is a great time-saver if:
  - You are a network admin who wants to implement a standard configuration on multiple computers.
  - You need to uninstall and re-install CCS or Windows, and want to quickly implement your old settings.

**Note**: Any changes you make over time are automatically saved in the 'Active' profile. If you want to export your current settings then export the 'Active' profile.

- The configurations area lets you switch your currently active profile and import/export profiles.
- Access the configuration settings interface
- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'

COMODO Creating Trust Online\*

COMODO Advanced	Settings				?	-		×
- General Settings	in con	figuration						
User Interface	Jegg Con	ilguration						
Updates	This section	lets you imp	ort, export a	nd switch (	configura	itions.		
Logging	•	₽	~	×				
Configuration	Import	Export	Activate	Remove				
✓ Antivirus	Configurati	ons			Status			
✓ Firewall	соморо с	lient - Securi	ty		Active			
✓ HIPS	COMODO	lient - Securi	ty Managed					
✓ Containment								
✓ File Rating								
✓ Advanced Protection								
				ОК		CA	NCEL	

The configurations interface shows all Comodo and user-defined profiles. The 'Active' profile is the one that is currently in effect on your computer. The following sections explain more about:

Comodo Preset Configurations

#### • Importing/Exporting and Managing Personal Configurations

#### 6.1.3.1. Comodo Preset Configurations

- Comodo preset configurations implement strong security settings on your endpoints.
- CCS ships with two preset configurations 'Comodo Client Security' and 'Comodo Client Security' Managed'.
  - · 'Comodo Client Security Managed' is applied to managed endpoints by default.
  - Comodo Client Security' is applied to unmanaged endpoints
- Reminder the 'Active' profile is, in effect, your current CCS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time.

**Comodo Client Security Managed -** The default configuration for computers managed by Endpoint Manager. Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- VirusScope is enabled.
- Realtime scan is enabled.
- Traffic filtering (Firewall) is enabled in Safe mode.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Advanced Protection is tuned to prevent infection of the system.
- Alert message notification is disabled.

COMODO Creating Trust Online\*

• VirusScope alerts are disabled

**Comodo Client Security** - The default configuration on standalone (unmanaged) computers. Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- VirusScope is disabled.
- Realtime scan is enabled.
- Traffic filtering (Firewall) is enabled in Safe mode.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Advanced Protection is tuned to prevent infection of the system.
- Alert message notification is enabled.
- VirusScope alerts are disabled

If you wish to switch to Comodo Client - Security option, you can select the option from the 'Configuration' panel.

#### 6.1.3.2. Personal Configurations

- Click 'Settings' > 'General Settings' > 'Configuration'
- · You can import, export, activate and manage your custom CCS configurations
- Exported Configuration profiles have the file extension .cfgx.
- See the following sections for more information:
  - Export a stored configuration to a file
  - Import a saved configuration from a file
  - Select a different active configuration setting
  - Delete a inactive configuration profile

#### Export a stored configuration to a file

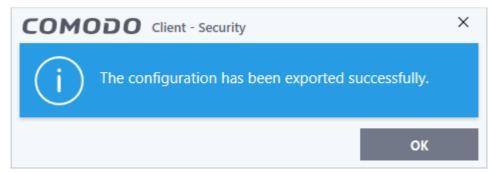
- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Configuration'
- Select a configuration profile then click 'Export'
- You will be given the chance to save any unsaved config. changes before exporting:

COMODO Creating Trust Online\*

COMODO Advance	d Settings	? – 🗆 ×
- General Settings User Interface	Configuration	nd switch configurations.
Updates Logging Configuration	Import	Remove
<ul> <li>✓ Antivirus</li> <li>✓ Firewall</li> </ul>	Configurations COMODO Client - Security	Status Active
✓ HIPS	COMODO Client - Security Managed	
Containment	<b>ODO</b> Client - Security Would you like to save your changes configuration before exporting it?	× s to the current
	YES NO	CANCEL

- Next, browse to the location where you want to save the configuration file.
- Create a name for the profile. For example, 'My CCS Settings', or 'CCS Highest Security Settings'
- Click 'Save':

A confirmation dialog will appear if the export is successful:



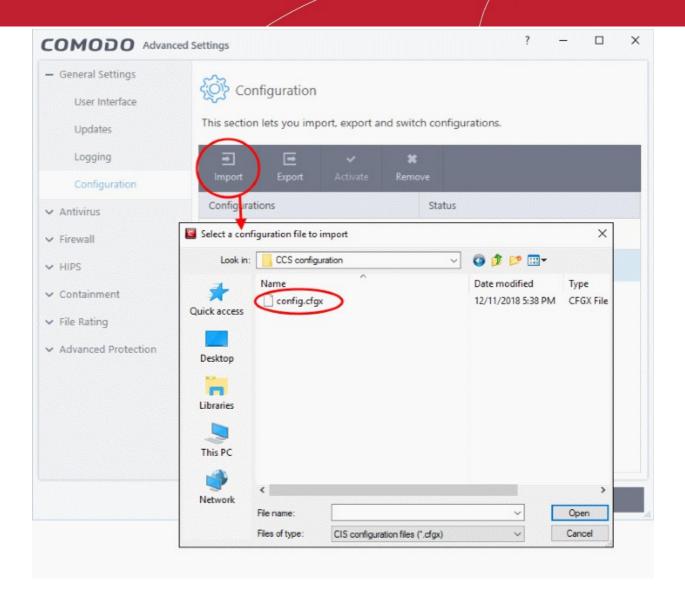
#### Import a saved configuration from a file

- You can import a CCS configuration from a previously saved file
- · Note After importing, you must activate the profile for it to take effect

#### Import a profile

- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'
- Click the 'Import' button:

COMODO

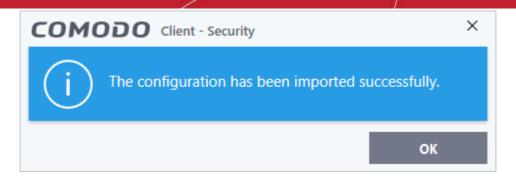


- Navigate to the location of the saved profile and click 'Open'. Configuration files have a .cfgx extension.
- Enter a name for the profile you wish to import and click 'OK'.

COMODO Import As		? )	×
Enter a name for this configuration: My_CCS_modified_profile			]
	ок	CANCEL	

The following message is shown after a successful import:

COMODO Creating Trust Online\*



Activate the profile - Select the profile you just imported and click the 'Activate' button:

COMODO Advance	d Settings					? ·	-		×
<ul> <li>General Settings</li> <li>User Interface</li> <li>Updates</li> </ul>	U	figuration lets you imp		nd switch config	urations.				
Logging	€	⊡	~	×					
Configuration	Import	Export	Activate	Remove					
✓ Antivirus	Configurati	ons		Status					
✓ Firewall	COMODO	Client - Securi	ity						
✓ HIPS	COMODO	Client - Securi	ity Managed	Active					
✓ Containment	My_CCS_mo	odified_profile	e						
✓ File Rating									
✓ Advanced Protection									
					ОК		CAN	CEL	

#### Select and implement a different configuration profile

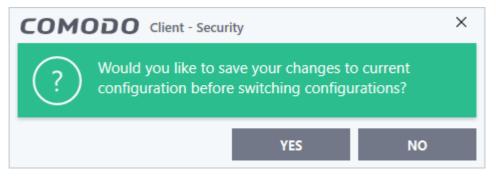
You can change the active configuration profile at any time.

- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'
- Choose the profile you want to enable and click the 'Activate' button:

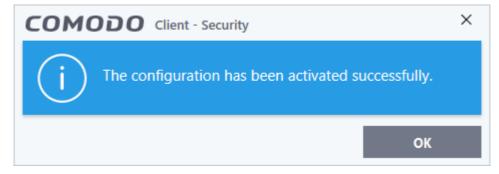
Creating Trust Online

COMODO Advance	d Settings	?	-		×
<ul> <li>General Settings</li> <li>User Interface</li> <li>Updates</li> </ul>	Configuration This section lets you import, export and switch configurations.				
Logging	= = ~ ×				
Configuration	Import Export Activate Remove				
✓ Antivirus	Configurations Status				
✓ Firewall	COMODO Client - Security				
✓ HIPS	COMODO Client - Security Managed Active				
✓ Containment	My_CCS_modified_profile				
✓ File Rating					
✓ Advanced Protection					
	ок		c	ANCEL	

You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.



2. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.



COMODO Creating Trust Online\*

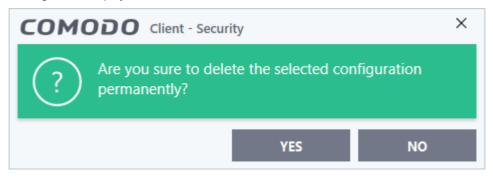
#### Delete an inactive configuration profile

You can remove any unwanted configuration profiles from the list. You cannot delete the currently active profile.

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Configuration'
- Choose the configuration profile you want to delete then click the 'Remove' button

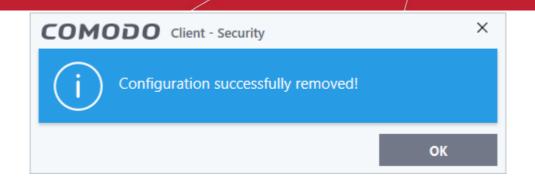
COMODO Advanced	d Settings	?	-		×
<ul> <li>General Settings</li> <li>User Interface</li> <li>Updates</li> </ul>	Configuration This section lets you import, export and switch configurations				
Logging Configuration	Import Export Activate Remove				
✓ Antivirus	Configurations Status				
✓ Firewall	COMODO Client - Security				
✓ HIPS	COMODO Client - Security Managed Active				
✓ Containment	My_CCS_modified_profile				
✓ File Rating					
<ul> <li>Advanced Protection</li> </ul>					
	ОК		C	ANCEL	

A confirmation dialog will be displayed.



3. Click 'Yes'. The configuration profile will be deleted from your computer.

COMODO Creating Trust Online\*



#### 6.2. Antivirus Configuration

Click 'Settings' > 'Antivirus'

The 'Antivirus' settings area lets you configure:

- The behavior of the real-time antivirus monitor
- · Scan profiles for on-demand and scheduled scans

<ul> <li>General Settings</li> </ul>			
— Antivirus	Realtime Scan		^
<ul> <li>Antivirus</li> <li>Realtime Scan</li> <li>Scans</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	<ul> <li>Enable Realtime Scan (Recommended)         <ul> <li>This option enables virus scanning when your computer is before they enter your system.</li> </ul> </li> <li>Enable scanning optimizations (Recommended)         Use this option to activate the performance improving te scanning.</li> <li>Do not show auto-scan alerts Ignore          <ul> <li>Use this option to scan removable media such as USB stilletc.</li> </ul> </li> <li>Detection         <ul> <li>Scan computer memory after the computer starts</li> <li>Do not show antivirus alerts Quarantine Threats              <ul> <li>Set new on-screen alert timeout to</li> <li>Set new maximum file size limit to</li> </ul> </li> </ul></li></ul>	cchnologies for realtime cks, CDs, DVDs, external HDDs,	
	Set new maximum script size limit to	4 MB	~

The following sections explain about:

- Real-time Scan Settings
- Custom Scan Profiles

COMODO Creating Trust Online\*

### 6.2.1. Real-time Scanner Settings

- Click 'Settings' > 'Antivirus' > 'Realtime Scan'
- The real-time scanner automatically checks for viruses whenever you open or move a file. It also monitors background activity for malicious processes.
- The real-time scanner also scans:
  - System memory on system startup
  - Any plugged-in removable storage devices
- You can specify that CCS does not show you alerts when it finds a threat, but automatically deals with the threat. You can choose to automatically quarantine or delete threats if you disable alerts.
- We strongly recommend you leave the real-time scanner enabled at all times.

#### Configure real-time scans

- Click 'Settings' at the top of the CCS home screen
- Click 'Antivirus' > 'Realtime Scan' on the left

COMODO Advance	d Settings	? – 🗆 X
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Realtime Scan	
Realtime Scan         Scans <ul> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	<ul> <li>☑ Enable Realtime Scan (Recommended) This option enables virus scanning when your computer is used and prevents threats before they enters ☑ Enable scanning optimizations (Recommended) Use this option to activate the performance improving technologies for realtime scanning. ☑ Do not show auto-scan alerts [Ignore ♥] Use this option to scan removable media such as USB sticks, CDs, DVDs, external HDDs, etc. Detection ③ Scan computer memory after the computer starts ④ Do not show antivirus alerts Quarantine Threats ♥ ○ Decompress and scan archive files of extension(s): *_exe, *_jar ○ Set new on-screen alert timeout to ③ Set new maximum file size limit to ④ Use heuristics scanning ☑ Use heuristics scanning of files on network ☑ Use Windows Antimalware Scan Interface (AMSI) technology □ Use cloud services while scanning via AMSI (Cloud Lookup should be enabled in File Rating section)</li></ul>	0 secs MB MB
		OK CANCEL

- Enable Realtime Scan Activate or deactivate real-time scanning. The real-time scanner continually
  monitors your computer for malicious activity and protects you from threats as soon as they occur. Comodo
  strongly recommends you keep this option enabled. (*Default=Enabled*)
- Enable scanning optimizations Will enable various techniques during a virus scan to reduce resource usage and speed-up the scan process. For example, antivirus scans will run in the background. (Default = Enabled)
- **Do not show auto-scan alerts** Select whether CCS alerts you when you plug a removable device into your computer (USB stick, portable HDD etc). The alert asks you whether you want to scan the device for viruses.

COMODO

- **Enabled** = Alerts are not shown. CCS will automatically take the action shown in the dropdown box next to the setting.
- **Disabled** = Alerts are shown when you plug a removable device into your computer. You can choose to scan the device, or skip the scan. An example alert is shown below:

сом	ODO Antivirus ?	
	We've just detected that new removable media device has been connected (D:\). We recommended to scan it.	
$\bigcirc$	<b>Scan</b> Scan the device to make sure it's not infected.	
(!)	<b>Ignore</b> Skip the scan. Note: malware undetected now may harm your and other computers later.	
🔳 Remem	ber my answer	

- Ignore The device is not scanned
- Scan The device is automatically scanned for viruses. The scan uses the settings in the 'Manual Scan' profile. If this is not available then the scan uses the settings in the 'Full Scan' profile.

### **Detection Settings**

- Scan computer memory after the computer starts The antivirus scans system memory immediately
  after your computer starts up. Disable to remove the scan from the list of Windows startup processes.
  (Default = Disabled)
- **Do not show antivirus alerts** Configure whether or not alerts are shown when CCS finds malware on your computer. (Default = Enabled ).

'Do not show antivirus alerts' will minimize disturbance but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CCS should automatically take:

- **Quarantine Threats** Prevents the threat from running and moves it to quarantine (*Default*). You can review quarantined files at 'Tasks' > 'Advanced Tasks' > 'View Quarantine'.
- Block Threats Prevents the threat from running then deletes it from your computer.

Note: If you deselect this option then the user is offered the choice to quarantine or block the threat at the alert.

 Decompress and scan archive files of extension(s) - Comodo Antivirus will scan all types of archive files. Archive file types include .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB files. You will be alerted to the presence of viruses in compressed files before you even open them. (Default = Enabled)

You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

• Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.

COMODO Creating Trust Online\*

COMODO Manage Extensions	?		×
<b>+ </b>			
Extensions Q File Size Limit	Status		
□ *.exe 4096 KB			
□ *.jar 1024 KB			
ОК	C/	ANCEL	

• To add a file type, click 'Add' at the top

Creating Trust Online\*

COMODO Manage Extensions	? 🗆	×
+ X Add Edit Remove		
Extensions Q File Size Limit	Status	
(☑) *.exe 4096 KB		
□ *.jar 1024 KB		
COMODO Edit property	? ×	
Set archive extension		
*.exe Set file size limit 4096 KB •		
ок	CANCEL	
OK	CANCEL	

- Enter the extension type you wish to scan and click 'OK'. Example extensions include .zip , .rar, .msi, .7z , .jar and .cab.
- Set the file size for the extension selected
- Repeat the process to add more extensions
- Click 'OK' in the 'Manage Extensions' dialog
- Set new on-screen alert timeout to Specify the length of time that virus alerts should stay on the screen.
   (Default = 120 seconds)
- Set new maximum file size limit to Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (*Default = 40 MB*)
- Set new maximum script size to Specify the largest script size that the antivirus should scan. CCS will not scan scripts bigger than the size specified here. (*Default = 4 MB*)
- Use heuristics scanning Enable or disable heuristic scans, and define the sensitivity of the scanner. (Default = Disabled)

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

If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will

decide a file is malware:

Low - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users.

- **Medium** Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.
- Enable realtime scanning of files on network Activate or deactivate automatic scans of files on network drives (Default = Disabled)
  - If enabled, the scanner will check all files you interact with on a network drive, even if you do not copy them to your local machine.
  - If disabled, network files are not checked unless you copy them to your local machine.
- Use Windows Anti-malware Scan Interface (AMSI) technology AMSI technology, developed by Microsoft allows 3rd party applications to request AV scans from the installed AV product on the machine. CCS is on the AMSI provider's list. This feature provides enhanced malware protection for users, their data and applications. (*Default = Enabled*)
  - Enabled CCS will scan on request from an AMSI enabled application.
  - Disabled CCS removes itself from the local AMSI providers list, and will not respond to scan requests from AMSI enabled apps.
- Use cloud services while scanning via AMSI This option is available if 'Use Windows Anti-malware Scan Interface (AMSI) technology' is enabled. (Default = Disabled)
  - Enabled CCS will check a file's trust rating on our cloud severs as part of the AMSI scan process.
    - Note Cloud Lookup must also be enabled in 'File Rating Settings'.

### 6.2.2. Scan Profiles

• Click 'Settings' > 'Antivirus' > 'Scans'

An antivirus scan profile is a collection of scanner settings that tell CCS:

- · What to scan (which files, folders or drives)
- When to scan (you can create a scan schedule)
- How to scan (you can configure the behavior of the scan engine)

CCS ships with two pre-defined scan profiles and allows you to create custom scan profiles.

- **Full Scan** Covers every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned if connected.
- Quick Scan Covers critical areas of your computer which are highly prone to infection and attack. 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 clean.

You cannot modify the areas scanned in a pre-defined profile, but you can edit the scan parameters. You can also create custom profiles and scan schedules.

#### Open the 'Scans' panel

- Click 'Settings' on the CCS home screen
- Click 'Antivirus' > 'Scans'

COMODO Creating Trust Online\*

<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> </ul>	Scar This page al		add, remove	e and edit sca	n profiles and scheduled sc	ans.
Scans	+	1	×			
<ul> <li>Firewall</li> </ul>	Add	Edit	Remove	Action	1-16	Chathan
✓ HIPS	Nar				Last Scan	Status
<ul> <li>Containment</li> </ul>	L Full	Scan		<u>Scan</u>	12/11/2018 5:44:22 PM	
✓ File Rating	Qui	ck Scan		Scan	12/11/2018 2:15:38 PM	
<ul> <li>Advanced Protection</li> </ul>	🗆 susp	picious		Scan	Never	
					ок	CANCEL

	Scan Profiles - Column Descriptions			
Column Header	Description			
Name	Name of the scan profile.			
Action	The activity that the profile is set to perform.			
	Click this link to manually run a scan according to the profile's parameters.			
Last Scan	Date and time of the most recent virus scan using this profile.			
Status	Enable or disable the profile.			
	'On' - Any scheduled scans configured in the profile will continue to run. In addition, you can manually run the scan at any time by clicking the 'Scan' link.			
	'Off' - Any scheduled scans configured in the profile will not run. You can still manually run the scan by clicking the 'Scan' link.			

Click the following links for more details about:

- Create a scan profile
- Run a custom scan

#### Create a custom profile

- Click 'Settings' on the top of the CCS home screen
- Click 'Antivirus' > 'Scans'
- Click 'Add' from the options at the top.

The profile configuration screen opens:

COMODO Creating Trust Online\*

сомо	DO Scan					?		×
Scan Name:	Old man do	ocuments						
Define items		d, scanning op	tions and run	ning schedule				
[] Add Files	Add Folder	🖾 Add Area	X Remove					
Pro	ofile							
					ОК	(	ANCEL	

• Type a name for the profile.

The next steps are to:

- Select the items to scan
- Configure scan options for the profile
- Configure a schedule for the scan

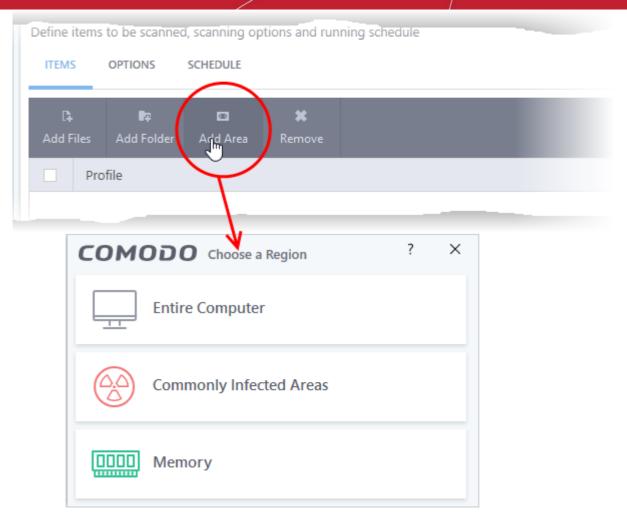
#### Select the items to scan

• Click 'Items' at the top of the 'Scans' interface.

The buttons along the top let you add three types of item to the scan. You can add any combination of items.

- Add Files Specify individual files to be scanned. Click the 'Add Files' button and navigate to the file you want to include in the scan. Repeat to add more files.
- Add Folder Specify entire folders to be scanned. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- Add Area Select pre-defined regions to be scanned. Regions include 'Full Computer', 'Commonly Infected Areas' and 'Memory'.

COMODO Creating Trust Online\*



• Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

### **Configure Scan Options**

• Click 'Options' at the top of the scan interface

COMODO Creating Trust Online\*

an Name:	
Define items	to be scanned, scanning options and running schedule
ITEMS	OPTIONS SCHEDULE
✓ Decomp	ress and scan compressed files
	n allows scanner to decompress archive files e.gzip, .rar, etc. during scanning
Use clou	d while scanning
This optic	n allows scanner to connect to cloud to query file ratings
Automat	ically clean threats Quarantine Threats 💌
When the	threats are identified, perform the selected action automatically
This optic	an results window on enables to view results of scans launched as per schedule or from the management portal, as well as e media scans.
☑ Use heur	istics scanning Low 🔻
Use the s	elected level of sensitivity while scanning heuristically
	ximum file size to 40 MB nning, if a file size is larger than specified, it is not scanned
Run this	
Priority of	f scanner determines how much of the computer resources are used among other tasks
🗹 Update v	virus database before running
This optic	on makes sure the database is updated before running the scan
Detect p	otentially unwanted applications
Potentiall download	y unwanted applications are programs that are unwanted despite the possibility that users consented to I them.
Apply th	is action to suspicious autorun processes Terminate and Disable 🔻
	ted action will be automatically applied if unrecognized Windows services, autostart entries or d tasks are detected.
	ime of a single file to 9 imin(s) e set time limit is reached, the file will be skipped and antivirus will proceed scanning other files.
	OK CANCEL

- **Use cloud while scanning** Improves scan accuracy by augmenting the local scan with an online look-up of Comodo's latest signature database. Cloud Scanning means CCS can detect the latest malware even if your virus database is out-dated. (*Default = Disabled*).
- Automatically clean threats Whether or not CCS should automatically remove any malware found by the scan.

archives (Default = Enabled) .

COMODO

- **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can select the action to be taken on them individually, or on all items at-once. See **Process Infected Files** for guidance on manually handling detected threats.
- **Enabled** = You can choose the automatic action to be taken against detected threats. The options are:
  - **Quarantine Threats** Infected items will be moved to Quarantine. You can review quarantined items later and remove them or restore them (in case of false positives). See **Manage Quarantined Items** for more details on managing quarantined items.
  - Disinfect Threats If a disinfection routine is available, the antivirus will remove the infection and keep the original, safe, file. If not, the item will be moved to 'Quarantine'. (*Default*)
- **Show scan result window** If selected, you will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.
- Use heuristics scanning Enable or disable heuristic scans, and define the sensitivity of the scanner. (Default = Enabled)

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

If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

• Low - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (Default)

- **Medium** Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.
- Limit maximum file size to Specify the largest file size that the antivirus should scan. CCS will
  not scan files bigger than the size specified here. (*Default = 40 MB*)
- Run this scan with Whether you want to set a priority for the scans with this profile
  - Enabled = You can set the priority. The available options are:
    - High
    - Normal
    - Low
    - Background.
  - Disabled = The scan will be run at the background (Default)
- **Update virus database before running** CCS checks for and downloads the latest virus signatures before starting every scan with this profile (*Default = Enabled*).
- Detect potentially unwanted applications The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility 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 your activity on the internet. (Default = Enabled).
- Apply this action to suspicious autorun processes Specify how CCS should handle unrecognized auto-run items, Windows services and scheduled tasks.
  - Ignore The item is allowed to run (Default)

COMODO Creating Trust Online\*

- Terminate CCS stops the process / service
- **Terminate and Disable** Auto-run processes will be stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- **Quarantine and Disable** Auto-run processes will be quarantined and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.

Note 1 - This setting monitors only registry records during the on-demand scan. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

See Miscellaneous Settings for more details

Note 2 - CCS ships with a list of applications for which script analysis will be performed to protect the registry records. You can manage the list of applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See 'Autorun Scans' in Script Analysis Settings for more details
- Limit scan time of a single file to Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

#### Schedule the scan

Click 'Schedule' at the top of the 'Scan' interface.

COMODO Scan	?		×
Scan Name:			
Define items to be scanned, scanning options and running schedule			
ITEMS OPTIONS SCHEDULE			
Frequency:			^
O not schedule this task			
O Every few hours			
O Every Day			
O Every Week			
O Every Month			
Additional Options			
Run only when computer is not running on battery			
Run only when computer is IDLE			
Turn off computer if no threats are found at the end of the scan			
Run during Windows Automatic Maintenance			~
c	ж	CANCEL	

You have the following options:

Do not schedule this task - The scan profile will be created but will not run automatically. The

COMODO

profile will be available for on-demand scans.

- Every few hours Run the scan at the intervals of the hours specified in 'Repeat scan every NN hour(s)'
- Every Day Run the scan every day at the time specified in the 'Start Time' field.
- Every Week Run the scan on the day(s) specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- Every Month Run the scan on the date(s) specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- Run only when computer is not running on battery The scan only runs when the computer is
  plugged into the power supply. This option is useful when you are using a laptop or other mobile
  device.
- Run only when computer is IDLE The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- Turn off computer if no threats are found at the end of the scan Will turn off your computer if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- Run during Windows Automatic Maintenance Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time *in addition* to the configured schedule.

The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See **Automatically Clean Threats**.

**Note**: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

• Click 'OK' to save the profile.

The profile will be available for deployment in future.

#### Run a custom scan as per a scan profile

- Click 'General Tasks' on the CCS home screen
- Click 'Scan' > 'Custom Scan'
- Click 'More Scan Options'

The 'Advanced Settings' interface will open at the 'Scans' panel:

Click 'Scan' beside the required scan profile.

COMODO Creating Trust Online\*

COMODO Advance	ed Settings		? -	- 🗆 X
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Realtime Scan</li> </ul>	Scans This page allows you to add, remov	ve and edit sc	an profiles and scheduled	scans.
Scans	+ 🖌 🗶			
✓ Firewall	Add Edit Remove			
V HIPS	Name	Action	Last Scan	Status
✓ Containment	Full Scan	<u>Scan</u>	Never	
✓ File Rating	Quick Scan	<u>Scan</u>	6/11/2019 11:52:59 AI	м 💽
✓ Advanced Protection	Shared Folder Scan	Scan	Never	
			ОК	CANCEL

The scan will start immediately. Results are displayed afterwards:

COMODO Creating Trust Online\*

	can		?	_		×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48					
THREAT(S) FOUND	SKIPPED FILES: 24					
Threat Name	Q	Action	Clean		•	^
🗏 Malware@ (#vigyao	klh7gw, #jgft8m0jxmvk, #3bqdlv583lryf, #2hr					
— 📄 C:\Share\Mah	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mah	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mah	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
– 🗋 C:\Share\Mal	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
— 📄 C:\Share\Mak	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	
C:\Share\Mah	ware-Samples-master\Malware-Samples-mast	🗸 Cle	an		•	J
Turn off this complete the second	puter if no threats are found at the end of the	scan				
CLOSE			APPLY	SELECTED		NS

The results window has two tabs:

- Threats Found: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See 'Process infected files' if you need help with these options.

**Note**: You will only see the drop-down menus if 'Automatically clean threats' is disabled for the selected scan profile in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

• **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

Creating Trust Online\*

	can			?	-	×
100%	TASK: Shared Folder Scan STATUS: Scan Finished ELAPSED TIME: 00:03:48					
THREAT(S) FOUND	: 8 🕜 SKIPPED FILES: 24					
Path						^
C:\Share\Firefox Setup	13.0.1.exe					
C:\Share\Firefox Setup	13.0.1.exe					
C:\Share\icedragonset	up.exe					
C:\Share\icedragonset	up.exe					
C:\Share\Firefox Setup	13.0.1.exe					
C:\Share\Paint.NET.3.5.	10.Install.exe					
C:\Share\Paint.NET.3.5.	10.Install.exe					
C:\Share\Paint.NET.3.5.	10.Install.exe					~
Turn off this complete	outer if no threats are found a	t the end of the	scan			
CLOSE				APPLY	SELECTED	NS

### 6.3. Firewall Configuration

- Click 'Settings' > 'Firewall'
- The firewall protects your computer against inbound and outbound threats.
- It checks that all network traffic in and out of your computer is legitimate, hides your computer ports against hackers, and blocks software from transmitting your personal data over the internet.
- The simple rules interface lets you specify exactly which applications can access the internet.
- You can choose to receive alerts if the firewall detects suspicious activity, or have the firewall autoimplement a specific action.

### Configure the 'Firewall' module

- Click 'Settings' on the CCS home screen
- Click 'Firewall' on the left:

COMODO Creating Trust Online\*

COMODO Advanced	Settings ? - 🗆 X
<ul><li>General Settings</li><li>Antivirus</li></ul>	Firewall Settings
<ul> <li>Antivirus</li> <li>Firewall</li> <li>Firewall Settings</li> <li>Application Rules</li> <li>Global Rules</li> <li>Global Rules</li> <li>Rulesets</li> <li>Network Zones</li> <li>Portsets</li> <li>Yortsets</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	<ul> <li>Enable Firewall (Recommended) Safe Mode  This option enables firewall which filters inbound and outbound traffic. </li> <li>Alert Settings Do not show popup alerts Allow Requests   </li> <li>Turn traffic animation effects on Create rules for safe applications Set alert frequency level Low   Set new on-screen alert timeout to 120 secs Advanced Filter IPv6 traffic Filter loopback traffic (e.g. 127.x.x.x. ::1) Block fragmented IP traffic Do protocol analysis</li></ul>
	<ul> <li>□ Enable anti-ARP spoofing</li> <li>☑ Detect disabled firewall driver in network adapter settings and Log only ▼</li> </ul>
	OK CANCEL

Firewall settings has the following sections:

- General Firewall Settings Settings that govern the overall behavior of the firewall.
- Application Rules Rules which control the network access rights of specific applications, or types of application.
- Global Rules Rules which apply to all traffic flowing in and out of your computer.
- Rule Sets Collections of rules that can be applied to internet capable applications like browsers and email/FTP clients.
- **Network Zones** A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** Predefined groups of regularly used ports that can be used and reused when creating traffic filtering rules.

#### Background note on rules:

Both application rules and global rules are consulted when the firewall decides whether to allow or block a connection:

Outgoing connections - Application rules are consulted first then global rules.

Incoming connections - Global rules are consulted first then application rules.

COMODO Creating Trust Online\*

### 6.3.1. General Firewall Settings

- Click 'Settings' > 'Firewall' > 'Firewall Settings'
- Firewall settings let you quickly configure the overall behavior of the firewall. Settings are divided into three main areas:
  - General Settings
  - Alert Settings
  - Advanced Settings

#### Configure the firewall settings

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

COMODO Advance	d Settings ? — 🗆 🗙
<ul><li>General Settings</li><li>Antivirus</li></ul>	Firewall Settings
— Firewall	Enable Firewall (Recommended)     Safe Mode
Firewall Settings	This option enables firewall which filters inbound and outbound traffic.
Application Rules	Alert Settings
Global Rules	Do not show popup alerts Allow Requests *
Rulesets	Turn traffic animation effects on
Network Zones	Create rules for safe applications
Portsets	Set alert frequency level
✓ HIPS	Set new on-screen alert timeout to 120 secs
✓ Containment	Advanced
✓ File Rating	□ Filter IPv6 traffic
<ul> <li>Advanced Protection</li> </ul>	Filter loopback traffic (e.g. 127.x.x.x, ::1)
	Block fragmented IP traffic
	Do protocol analysis
	Enable anti-ARP spoofing
	Detect disabled firewall driver in network adapter settings and Log only 🔻
	OK CANCEL

### **General Settings**

•

- Enable Firewall Activate or deactivate firewall protection. (Default and recommended = Enabled)
  - If enabled, you can also choose the security level from the drop-down menu:

COMODO

Firewall Settings	
Enable Firewall (Recommended)     Saf	e Mode 🔻
This option enables firewall which filte	Block All nd traffic.
Alert Settings	Custom Ruleset Safe Mode
☑ Do not show popup alerts Allow F	Training Mode
Turn traffic animation effects on	

The choices available are:

- Block All: The firewall stops all traffic in and out of your computer, regardless of any other settings or rules. The firewall does not attempt to learn the behavior of any application, and does not create traffic rules for any applications. This option prevents your computer from accessing any networks, including the internet.
- Custom Ruleset Mode: The firewall applies ONLY network traffic rules that you have created. New users
  may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the
  behavior of any applications. Nor does it automatically create network traffic rules for those applications.
  You will receive alerts every time there is a connection attempt by an application even for applications on
  the Comodo Safe list (unless, of course, you have specified rules and policies that instruct the firewall to
  trust the application's connection attempt).

If any application tries to make a outbound connection, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.

Safe Mode (Default): If Create rules for safe applications is enabled then the firewall automatically creates rules to allow traffic by applications certified as 'Safe' by Comodo. For new, unknown 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 deploys the predefined firewall ruleset 'Trusted Application' onto the application.

'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.

Training Mode: The firewall monitors network traffic and creates automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the correct network access rights.

### **Alert Settings**

 Do not show popup alerts - Whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do not show pop-up alerts' will minimize disturbances but at some loss of user awareness. (*Default = Enabled*)

If you choose this option then you have a choice of default responses that CCS should take - either 'Block Requests' or 'Allow Requests'.

COMODO Creating Trust Online\*

This option enables firewall wh	nich fil	ters inbound and	outbound tra	aff
Alert Settings				
Do not show popup alerts	Allow	v Requests 🔻		
Turn traffic animation effects	Ċ	Allow Requests Block Requests		
Create rules for safe application	ons		1	
Set alert frequency level	ow 🔻			

 Turn traffic animation effects on - By default, the Comodo Client Security's 'Shield' tray icon displays a small animation whenever traffic moves to or from your computer.

📌 🔨 🎦 🛱 🗘 ENG	09:30 29-04-2019
---------------	---------------------

If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the shield. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer.

- Clear this check box If you would rather not see this animation. (Default = Disabled)
- Create rules for safe applications Comodo Firewall trusts the applications if:
  - The application is on the Comodo safe list, a global white-list of trusted software.
  - The application has a 'Trusted' rating in the local file list. See File List if you need more details.
  - The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file. See Vendor List if you need more details.

By default, CCS does not automatically create 'allow' rules for safe applications. This helps to lower resource usage and simplifies the rules interface. It also reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CCS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **Application Rules** interface. The Advanced users can edit/modify the rules as they wish. (**Default = Disabled**)

Set alert frequency level - Configure the amount of alerts that the firewall generates. Please note that this does not affect your security level, which is determined by the actual rules you have in place (for example, in 'Application Rules' and 'Global Rules'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of suspicious behavior while not getting overwhelmed with alerts. (*Default =Disabled*)

Create rules for safe applica	tions
Set alert frequency level	Low 🔻
Set new on-screen alert tim	Very High High
Advanced	Medium
Filter IPv6 traffic	Low
☑ Filter loopback traffic (e.g. 1	Very Low 27.x.x.x, :: 1)

The options available are:

COMODO Creating Trust Online\*

- Very High: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.
- **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
- **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
- **Low:** 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.
- Very Low: The firewall shows only one alert for an application.

The alert frequency settings refer only to connection attempts by applications or from IP addresses that you do not trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

Set new on-screen alert time out to: How long a firewall alert remains on-screen if it is not answered. The default timeout is 120 seconds. You may adjust this setting to your own preference.

### **Advanced Settings**

Advanced detection settings help protect your computer against common types of denial of service (DoS) attack. 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.

Filter IP v6 traffic - If enabled, the firewall will filter IPv6 network traffic in addition to IPv4 traffic.(Default = Disabled)

**Background Note**: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available. This hard limit has already led to the development of 'work-around' solutions such as Network Address Translation (NAT), which enable multiple hosts on private networks to access the Internet using a single IP address.

IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- 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. Leaving this option enabled means the firewall will filter traffic sent through this channel. (*Default = Enabled*)
- 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

COMODO

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. (*Default = Disabled*)

- Do Protocol Analysis Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Enabling this option means Comodo Firewall checks that every packet conforms to that protocols standards. If not, then the packets are blocked. (*Default = Disabled*)
- Enable anti-ARP spoofing A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update your machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update your ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in your home network. Enabling this setting helps to block such requests protecting the ARP cache from potentially malicious updates. (*Default = Disabled*)
- Detect disabled firewall driver in network adapter settings The firewall will take action if it discovers its driver is not enabled.

Detect disabled firewall driver in network adapter settings and	Log	only 🔻
		Log only Re-enable driver

You can choose the following actions if this condition is met:

- Log only Creates an event log but does not notify the administrator.
- Re-enable Driver Attempts to turns the driver back on automatically.

### 6.3.2. Application Rules

- Click 'Settings' > 'Firewall' > 'Application Rules'
- Application rules let you manage network access rights for specific applications.
- Whenever an application makes a request for network access, CCS allows or denies the request based on the ruleset applied to the application.
- Firewall rulesets are made up of one or more application rules. Each rule outlines an application's permissions regarding a specific type of traffic.

COMODO Creating Trust Online\*

<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	The fo		lication Ru 19 firewall ap		es are active	on this comp	uter.		
Firewall Settings	+ Ade		۲. Edit	# Remove	<b>t</b> Move Up	<b>↓</b> Move Down	ନ Purge		
Global Rules		Арр	lication			Q	Treat as		Q r
The application's name is liste above the rules applied to it Rules applied to an application determines its network access rights	ed dire	Cay (1)	C:\Program	n Files\COMO n Files\Mozilla All Incoming	a Firefox\firefo	ox.exe N	Custom ame of the pre uleset	-defined	
✓ HIPS			🗉 System				Custom		
<ul> <li>Containment</li> </ul>			🗆 Comodo (	Client - Securi	ty		Outgoing Only		
Each ruleset is derived from at least one but usually a			- 🗸 Allow	All Outgoing	Requests				
combination of individually			Block	and Log All U	nmatching R	equests			
configurable rules					energenergenerge				222

- Application Programs or file groups for which a firewall ruleset has been created. In the case of file
  groups, all member applications will use the ruleset of the group.
  - Click '+' next to the name to view the rules which apply to the application/group.
- Treat as Name of the ruleset assigned to the application or group.

The controls above the table let you manage the rule sets:

	App	lication Ru	iles				
	The followin	g firewall ap	plication rule	es are active	on this comp	iter.	
(	+ Add	<b>"</b> Edit	🗶 Remove	<b>↑</b> Move Up	<b>↓</b> Move Down	ନ Purge	
	🗆 Арр	lication			Q Treat	15	۹ ^
		3 System			Custor	n	

- Add Add a new application/application group then create a ruleset for it.
- Edit Modify an application rule/ruleset.
- **Remove** Delete a selected rule.

- **Purge** Check that all applications mentioned in a ruleset are still installed at the paths specified. If not, the rule is removed from the list.
- **Move Up** and **Move Down** Rules are prioritized top-to-bottom, with those at the top having the higher priority. The 'Move Up' and 'Move Down' buttons let you change the priority of a selected rule.

### **Predefined rulesets**

- Although you could create a ruleset from the ground-up by configuring its individual rules, this practice would be time consuming if performed for every program on your system.
- For this reason, Comodo provide a selection of rulesets according to broad application category. For example, the 'Web Browser' ruleset is designed for applications like 'Internet Explorer', 'Firefox' and 'Chrome'.
- Each predefined ruleset optimizes security for a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets**.

### Create a firewall ruleset

- Step 1 Select the target application or group
- Step 2 Configure the rules

### Step 1 - Select the target application or group

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Application Rules'
- Click the 'Add' button

The 'Application Rule' interface appears:

COMODO Creating Trust Online\*

COMODO Advanced	Settings	? –
✓ General Settings	Application Rules	
<ul> <li>Antivirus</li> <li>Firewall</li> </ul>	The following firewall application rules are acti	ive on this computer.
Firewall Settings	+ 2 × 1	∔ O
Application Rules	Add Im Edit Remove Move U	Jp Move Down Purge
Global Rules	Application	Q Treat as
Rulesets	E C:\Program Files (x86)\COMODO\(	Comodo ITSM Custom
<b>COMODO</b> Αρ	plication Rule	? 🗆 🗙
Name:		Browse 🔻
O Use Ruleset:		Web Browser 💌
Use a Custom Rules	et	Copy from 🔻
∔     .       Add     Edit	Image: termImage: termRemoveMove UpMove Down	
Rules		Q
	ОК	CANCEL

#### Click the 'Browse' button beside the 'Name' field:

COMODO Application Rule	? 🗆 X	
Name:	<b>BLOWSOLL</b>	
O Use Ruleset:	Web File Groups Running Processes	•

There are three types of target you can add:

.

- File Groups Apply the ruleset to a predefined file group. All members of the group are covered by the rule. See File Groups if you need help with file groups.
- Files Apply the ruleset to a specific application.

na Trust Online

Running Processes - Apply the ruleset to an application by selecting its running process •

#### Add a File Group

A file group is category of files or folders. For example, 'Executables', 'Media Players', or 'Important Files/Folders'. See File Groups more help with them.

• Choose 'File Groups' from the 'Browse' drop-down.

? 🗆 ×	
Browser	
File Groups       Web       Files       Running Processes	Executables All Applications Windows Updater Applications
	Windows Management 3rd Party Protocol Drivers Metro Apps
	Email Clients
	File Archivers
	Temporary Files
	Shared Spaces
	File Downloaders
	Suspicious Locations
	Containment Folders
	Pseudo File Downloaders
	Windows System Applications
	Web Browsers
	Browser Plugins
	Startup Folders
	Management and Productivity Applications
	Media Players
	COMODO Client - Security
	COMODO Client - Security Manager
	ExceptionGroup
	Important Files/Folders
	Communication Client
	Exclusions for Purchase Dept Profile
	Openoffice
	COMODO Client Files/Folders
<ul> <li>Select a file group from the drop-down. The ruleset will apply</li> </ul>	to all executable files in the group

- Select a file group from the drop-down. The ruleset will apply to all executable files in the group.
  - . The next stage is Step 2 - Configure the rules for the selected file group.

### Add an individual File

Choose 'Files' from the 'Browse' drop-down: •

COMODO Creating Trust Online\*

Applicatio	on Rule	? 🗆 🗙	
me:		File Groups Files Running From	ese
G Open	ograms > Opera > 🗸 진		×
Organize ▼ New fold		Search Opera	
<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Docutres</li> <li>Doubt_files</li> <li>Music</li> <li>Share</li> <li>Suspicious</li> <li>ConeDrive</li> </ul>	Name 60.0.3255.124 Assets installation_status.json installer_prefs.json.backup launcher launcher.visualelementsmanifest pref_default_overrides Resources.pri server_tracking_data	Date modified         Type           6/12/2019 1:31 PM         File for           6/12/2019 1:31 PM         File for           6/12/2019 1:31 PM         File for           6/12/2019 1:31 PM         JSON           6/12/2019 1:31 PM         JSON           6/12/2019 1:31 PM         BACK           5/30/2019 1:31 PM         BACK           2/22/2019 11:10 SAM         Applie           2/22/2019 11:14 PM         XML I           6/12/2019 1:30 PM         File           2/22/2019 11:14 PM         PRI Fil           6/12/2019 1:31 PM         File	File File UP catio
> 💻 This PC 🗸	<		>
File n	aame: launcher 🗸 🗸	All Files (*.*) ✓ Open ▼ Cancel	

- Navigate to the file you want to add as target and click 'Open'. The rule will apply only to the specific application.
  - The next stage is **Step 2 Configure the rules** for the selected application.

Add a currently running application by choosing its process

• Choose 'Running Processes' from the 'Browse' drop-down.

COMODO Creating Trust Online\*

MODO Application Rule	Browse
e Ruleset:	Web Files Running
COMODO Browse for Processes	?
Application	PID
<ul> <li>explorer.exe</li> <li>MSASCuiL.exe</li> <li>cis.exe</li> </ul>	4044 6720 7560
<ul> <li>▲ G cis.exe</li> <li>▲ G OneDrive.exe</li> </ul>	8004 7000
<ul> <li>I svchost.exe</li> <li>I svchost.exe</li> <li>I svchost.exe</li> </ul>	2204 1380 2400
<ul> <li>MyWeather.exe</li> <li>Implication system</li> </ul>	6540 1972
<ul> <li>Image: svchost.exe</li> <li>Image: cmdprots.exe</li> <li>Image: GoogleCrashHandler.exe</li> </ul>	1760 2660 5808
<ul> <li>dasHost.exe</li> <li>cis.exe</li> </ul>	3904 7368
<ul> <li>▲ SoogleCrashHandler64.exe</li> <li>▲ O opera.exe</li> </ul>	6864 6880

- Select the target process and click 'OK'. The parent application of the process will be added as the target.
  - The next stage is to configure the rules for the selected application.

### Step 2 - Configure the rules in ruleset

There are two broad options for creating a ruleset - Use a Predefined Ruleset or Use a Custom Ruleset.

#### **Use Ruleset**

- A ruleset is a collection of rules designed to implement optimum security on a specific type of application. You can manage and create rulesets in 'Settings' > 'Firewall Configuration' > 'Firewall Rule Sets'.
- Comodo provides a range of curated rulesets for popular types of application. These include 'Web browser', 'FTP client' and 'Email client'.
- The example below shows us applying the 'Web Browser' ruleset to the Opera browser:

eating Trust Online

<b>COMODO</b> Application Rule ?								
Name: \Us	lame: \Users\John\AppData\Local\Programs\Opera\60.0.3255.124\opera.6							
Use Rules					Web	Browser Veb Browser		
O Use a Cu	stom Rulese	t				Email Client		
+ Add	<b>e</b> Edit	× Remove	t Move Up	<b>↓</b> Move Down		Ftp Client Allowed Application Blocked Application		
						Outgoing Only		

• Use a Custom Ruleset - Designed for more experienced users, 'Custom Ruleset' lets you fully configure all rules in the ruleset. You can create an entirely new ruleset, or use a predefined set as a starting point.

OMODO Application Rule	?	
ame: \Users\John\AppData\Local\Programs\Opera\60.0.3255.1	24\opera.exe Browse 🔻	
Use Ruleset:	Web Browser 🔻	
Use a Custom Ruleset	Copy from	
+ 💉 🗰 🖡 Add Edit Remove Move Up Move Down	Ruleset Another Application	Web Browser Email Client
Add Edit Remove Move Up Move Down	۹ ^	Ftp Client Allowed Application Blocked Application
Allow Access to Loopback Zone		Outgoing Only
Allow Outgoing HTTP Requests		
Allow Outgoing FTP Requests  Allow Outgoing FTP-PASV Requests		
Allow Outgoing DNS Requests	- 1	
ок		
	<b>V</b>	

ruleset to be created. Using this as a starting point, experienced users can add, re-order, modify and remove rules to suit to their applications.

- Select the 'Use custom ruleset' radio button
- Add Create individual rules for the set. See 'Add and Edit a Firewall Rule' for an overview of the process.
- Copy From Populate the list with the rules of a Predefined Firewall Rule. Edit/add/remove rules to

COMODO Creating Trust Online\*

create your custom ruleset.

#### **Understand Firewall Rules**

At their core, each firewall rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** that a packet of data must meet, and an **action** that is taken if those conditions are met.

As a packet filtering firewall, Comodo firewall analyzes the attributes of every packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding firewall rule, then the connection is automatically blocked until a rule is created.

If the packet of data meets these conditions
Allow ICP Out From IP 192.111.111.111 To MAC Any Where Source Port Is 25 A
then the firewall will take this action

The actual **conditions** (attributes)\* you see on a particular firewall rule are determined by the protocol chosen while **adding and editing a firewall rule**.

If you chose 'TCP', 'UDP' or 'TCP and 'UDP', then the rule has the form: Action |Protocol | Direction |Source Address | Destination Address | Source Port | Destination Port

If you chose 'ICMP', then the rule has the form: Action |Protocol | Direction | Source Address | Destination Address | ICMP Details

If you chose 'IP', then the rule has the form: Action | Protocol | Direction | Source Address | Destination Address | IP Details

- Action: The action the firewall takes when the conditions of the rule are met. The rule shows 'Allow', 'Block' or 'Ask'.\*\*
- **Protocol**: States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows '**TCP**', '**UDP**', '**TCP** or **UDP**', '**ICMP**' or '**IP**'
- Direction: States the direction of traffic that the data packet must be attempting to negotiate. The rule shows 'In', 'Out' or 'In/Out'
- Source Address: States the source address of the connection attempt. The rule shows 'From' followed by one of the following: IP , IP range, IP Mask , Network Zone, Host Name or Mac Address
- **Destination Address**: States the address of the connection attempt. The rule shows 'To' followed by one of the following: IP, IP range, IP Mask, Network Zone, Host Name or Mac Address
- **Source Port**: States the port(s) that the application must be attempting to send packets of data through. Shows 'Where Source Port Is' followed by one of the following: 'Any', 'Port #', 'Port Range' or 'Port Set'
- Destination Port: States the port(s) on the remote entity that the application must be attempting to send to. Shows 'Where Source Port Is' followed by one of the following: 'Any', 'Port #', 'Port Range' or 'Port Set'
- ICMP Details: States the ICMP message that must be detected to trigger the action. See Add and Edit a Firewall Rule for details of available messages that can be displayed.

• IP Details: States the type of IP protocol that must be detected to trigger the action: See Add and Edit a Firewall Rule to see the list of available IP protocols that can be displayed here.

Once a rule is applied, the firewall monitors all traffic relating to the application and takes the specified action if the conditions are met. Users should also see the section 'Global Rules' to understand the interaction between 'Application Rules' and 'Global Rules'.

\* If you chose to add a descriptive name when creating the rule then this name is displayed here rather than it's full parameters. See the next section, 'Add and Edit a Firewall Rule', for more details.

\*\* If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)

### Add and Edit a Firewall Rule

The firewall rule interface is used to configure the actions and conditions of an individual rules. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading 'Understanding Firewall Rules', 'Overview of Rules and Policies' and 'Create and Modify Firewall Rulesets'.

- Click 'Add' in the 'Application Rule' interface to create a new rule
- Double click on an existing rule or select a rule and click 'Edit' to edit an existing rule

сомодо	Firewall Rule	?	×
Action:	Allow	Log as firewall event if this rule is fired	ł
Protocol:	TCP or UDP <		
Direction:	In or Out		
Description			
SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT DESTINATION PORT	
Exclude (i.e. N	OT the choice below)		
Ту	pe: Any Address	•	
		OK CAN	CEL

#### **General Settings**

• Action: Specify how firewall should handle the connection request when the conditions of the rule are met. Options available are 'Allow' (*Default*), 'Block' or 'Ask'.

COMODO Creating Trust Online\*

сомодо	Firewall	Rule			?	×
Action:	Allow		•	Log as firewall event if this rule is fire	ed	
	Allow					
Protocolo	Block	•	-			
	Ask	3				

Protocol: Specify which protocol the data packet should be using. Options available are 'TCP', 'UDP', 'TCP or UDP' (*Default*), 'ICMP' or 'IP'.

Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- Direction: Define whether the rule should intercept inbound or outbound traffic. Options available are 'In', 'Out' or 'In/Out' (*Default*).
- Log as a firewall event if this rule is fired: Creates an entry in the firewall event log viewer whenever this rule is triggered. (i.e. when ALL conditions have been met) (*Default = Disabled*).
- **Description**: Enter a friendly name for the rule. For example, 'Allow Outgoing HTTP requests'. The friendly name is shown in the **Application Rules interface**.

#### Protocol

### i. TCP', 'UPD' or 'TCP or UDP'

If you select 'TCP', 'UPD' or 'TCP or UDP' as the protocol, then you also have to set the source and destinations:

SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT	DESTINATION	PORT
Exclude (i.e. NOT	the choice below)			
Type	Any Address Host Name IPv4 Address Range IPv4 Single Address IPv4 Subnet Mask IPv6 Address Range	•		
	IPv6 Single Address IPv6 Subnet Mask MAC Address Network Zone		ок	CANCEL

### Source Address and Destination Address:

- Any Defaults to an IP range of 0.0.0.0- 255.255.255 to allow connection from all IP addresses.
- Host Name Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field

### COMODO

### Comodo Client Security - User Guide

- IPv4 Address Range Choose all IP addresses covered by a range for example a range in your private network.
  - Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.
- IPv4 Single Address Choose a single IPv4 address
  - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
- IPv4 Subnet mask Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and Mask of the network.
- IPv6 Address Range Choose all IPv6 addresses covered by a range for example a segment in your private network
  - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
- Single IPv6 Address Choose an IPv6 address
  - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- IPv6 Subnet Mask Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and 'Mask' of the network in the respective fields
  - MAC Address Choose a single source/destination by specifying its physical address
  - Enter the physical address in the 'MAC Address' text box.
- **Network Zone** Choose an entire network. This menu defaults to Local Area Network. But you can also define your own zone by first creating a 'Network Zone' through the 'Network Zones' area.
  - Exclude (i.e. NOT the choice below) Applies the action to all items except the one you specify. For example, you create a block rule, specify an IP address, then select 'Exclude'. The rule will block traffic for every address except the one you specified.

Source Port and Destination Port:

SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT	DESTINATION POR	r
Exclude (i.e. NC	T the choice below)			
Тур	e: Any A Port Range A Set of Ports A Single Port Any			
			ок	CANCEL

- Any Apply the rule to any port number set by default, 0- 65535.
- A Single Port Specify a one port number

COMODO Creating Trust Online\*

- Enter the single port number in the 'Port' drop-down combo-box .
- A Port Range Specify a set of ports covered by a range.
  - Enter the first port number and last port number in the respective fields
- A Set of Ports Choose a predefined Port Set. If you wish to create a custom port set then please see the section 'Port Sets'.

#### ii. ICMP

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

#### ICMP Details

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

Source' and 'Destination' addresses - Enter the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.

SOURCE ADDRESS	DESTINATION ADDRESS	DETAILS	
Type:	ICMPv4		
Message:	Any		
wessage.	Custom	1	
	Any		
	ICMP Echo Request		
	ICMP Echo Reply		
	ICMP Net Unreachable		
	ICMP Host Unreachable		
	ICMP Protocol Unreachable		
	ICMP Port Unreachable	ок	CANCEL
	ICMP Time Exceeded	OK	CANCEL
	ICMP Source Quench		
	ICMP Fragmentation Needed	1	

- **Type** Choose the ICMP version.
- **Message** Specify the type of the ICMP Message.

When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

iii. IP

When you select IP as the protocol in **General Settings**, you are shown a list of IP message type in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are

COMODO Creating Trust Online\*

configured identically to the explanation above. You cannot see the source and destination port tabs.

Description A	ют месеза 10 200ранск	Züne		
SOURCE ADDRESS	DESTINATION ADDRESS	IP DETAILS		
Exclude (i.e. NOT	the choice below)			
Type:	Network Zone	•		
	Any Address			
Zone	Host Name			
	IPv4 Address Range			
	IPv4 Single Address			
	IPv4 Subnet Mask			
	IPv6 Address Range			
	IPv6 Single Address			
	IPv6 Subnet Mask			
	MAC Address			CANCEL
	Network Zone		OK	CANCEL

#### IP Details

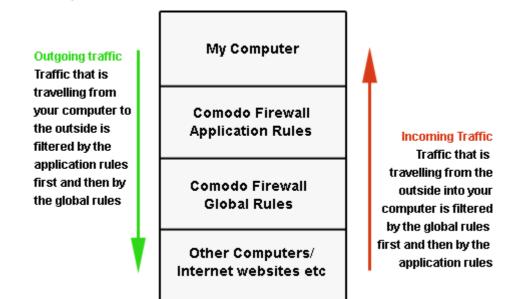
Select the types of IP protocol that you wish to be intercepted by the rule, from the ones that are listed.

Description			
SOURCE ADDRESS	DESTINATION ADDRESS	IP DETAILS	
IP Protocol	: Any Custom Any TCP UDP ICMPv4 IGMP Raw IP		
	GGP GRE	OK CANCEL	
	RSVP ICMPv6		

• Click 'OK' to save the firewall rule.

6.3.3. Global Rules

- Click 'Settings' > 'Firewall' > 'Global Rules'
- 'Global Rules' apply to all traffic in and out of your computer. This makes them different to application rules, which apply to the traffic of a specific application.
- Comodo firewall analyzes every packet of data in and out of your PC using combination of application rules and global rules.
  - Outgoing connection attempts Application rules are consulted first and the global rules second.
  - Incoming connection attempts Global rules are consulted first and the application rules second.



- So outgoing traffic has to pass the application rule first then any global rules before it is allowed out. Similarly, incoming traffic has to pass the global rules first then the application rules.
- Global rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

### Manage Global Rules

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Global Rules'

COMODO Creating Trust Online

COMODO Creating Trust Online\*

<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	ced Settings ? - C X								
Firewall Settings Application Rules Global Rules	+ Add	Edit	X Remove	t Move Up	<b>↓</b> Move Down				Q
Rulesets Network Zones Portsets HIPS Containment File Rating		Allow All Inco Allow IP Out Allow ICMPv Allow ICMPv	oming Request From MAC An 4 In From MAC 4 In From MAC	ts If The Send y To MAC Any C Any To MAC C Any To MAC	et Is In [Work # er Is In [Work # y Where Protoc Any Where IC Any Where IC	t] col Is Anj MP Mes: MP Mes:	sage Is Fl		
					ок			ANCEL	

### **General Navigation:**

The controls above the table let you create and manage global rules:

ļ	Global Rules										
1	The following global rules are active on this computer:										
<	+ Ado	ł	Edit	<b>X</b> Remove	🕇 Move Up	<b>↓</b> Move Down					
	Rules										
	Allow All Outgoing Requests If The Target Is In [Work #2]										
		Allow All Incoming Requests If The Sender Is In [Work #2]									

- Add Create a new global rule. See 'Add and Edit a Firewall Rule' in the previous section 'Application Rules' for guidance on creating a new rule.
- Edit Modify an existing global rule. See 'Add and Edit a Firewall Rule' in the previous section 'Application Rules' for guidance on editing a new rule.
- Remove Deletes the selected rule.
- **Purge** Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged',

COMODO Creating Trust Online\*

#### from the list.

- Move Up and Move Down Rules at the top of the list have a higher priority. In the event of a
  conflict in settings for a piece of traffic, CCS will apply the setting in the rule nearer the top of the
  list. The 'Move Up' and 'Move Down' buttons let you change the priority of a rule.
- The configuration of global rules is identical to that of application rules. See **Application Rules** for an introduction to the rule setting interface.
- See **Understand Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See Add and Edit a Firewall Rule for an explanation of individual rule configuration.

### 6.3.4. Firewall Rule Sets

- Click 'Settings' > 'Firewall' > 'Rulesets'
- A firewall ruleset is a collection of one or more firewall rules which can be deployed to applications on your computer.
- CCS ships with six predefined rulesets that provide a very high level of protection. You can also create your own, custom rulesets.

This section contains advice on the following:

- Predefined Rulesets
- Custom Rulesets
- Create a new ruleset

#### Open the 'Rulesets' panel

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Rulesets'

Creating Trust Online\*

COMODO Advance	d Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Rulesets The following rulesets are defined on this computer:				
Firewall Settings Application Rules	<b>+ .∕ X</b> Add Edit Remove				
Global Rules	Ruleset Name				Q
Rulesets	Web Browser				
Network Zones	Email Client				
Portsets	Ftp Client				
✓ HIPS	Allowed Application				
✓ Containment	Blocked Application				
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Outgoing Only				
	ок		c	ANCEL	

- The interface shows all existing rulesets. These may be Comodo predefined rules, or custom rulesets.
- Use the search feature to look for a specific ruleset

#### **Predefined Rulesets**

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring separate rules, this practice would prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Chrome'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can modify pre-defined policies to suit their environment and requirements. For example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of its rules.

CCS ships with six predefined firewall rulesets for different categories of applications:

- Web Browser
- Email Client
- FTP Client
- Allowed Application
- Blocked Application
- Outgoing Only

These rulesets can be edited for adding new rules or re-configuring the existing rules. For more details, see Add and Edit Firewall Rules in 'Application Rules'.

#### **Custom Rulesets**

COMODO Creating Trust Online

You can create new rulesets with custom network access control rules as per your requirements. These can then be applied to specific applications when **creating an application rule**.

#### **The Firewall Alert**

You can apply a firewall ruleset to an application at a firewall alert. Both predefined and custom rulesets are made available. An example alert is shown below:

сом	ODO Firewall	?
	MyRoamer.exe is trying to connect to the interr	et 🕟
MB	Application:         MyRoamer.exe           Remote:         10.108.56.1 - UDP           Port:         5351	
	Treat as Lets you choose a ruleset to apply	$\bigcirc$
0	FTP Client	^
0	Allowed Application	
0	Blocked Application	
0	Outgoing Only	
0	Grazing Applications	~
Remem	ber my answer <u>Sh</u>	ow Activities

• See **answering firewall alerts** if you want more help with alerts.

#### Add a new ruleset

Click the 'Add' button at the top of the list of rulesets in the 'Rulesets' panel

COMODO Creating Trust Online\*

COMODO Firewa	ll Ruleset	?	σ×
Name: Custom ruleset fo	Copy from 🔻		
Add     Edit       Rules	Ruleset Another Application	Web Browser Email Client Ftp Client Allowed Application Blocked Application Octoing Only	Q
		ок	CANCEL

- Enter a name for this new ruleset. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for.
- Next you should add and configure the individual rules for this ruleset. You can choose to use an
  existing ruleset as a starting point and add/edit rules as required. See 'Add and Edit a Firewall Rule'
  for more advice on this.

Once created, this ruleset can be quickly called when **creating or modifying a firewall ruleset** for an application:

Use Ruleset: Web Browser           Use a Custom Ruleset       Copy from           Image: Copy from Ima	Use a Custom Ruleset	ame: C:\	Program File	es (x86)\Drivin	ngSpeed2\Dr	ivingSpeed.exe	Browse 🔻	
Ruleset     Web Browser       Add     Edit     Remove       Rules     Move Up     Move Down         Rules     Q         Web Browser         Email Client         Howe Down         Rules           Rules	+     *     *     Image: Constraint of the second	Use Rule	eset:				Web Browser 🔻	
Image: Construction of the co	Image: Construction of the product	Use a Cu	istom Rulese	et			Copy from 🔻	
Add     Edit     Remove     Move Up     Move Down       Rules     Q     Ftp Client	Add     Edit     Remove     Move Up     Move Down       Rules     Q     Ftp Client     Allowed Application       Blocked Application     Outgoing Only							Web Browser
Rules     Allowed Application       Blocked Application	Rules Q Allowed Application Blocked Application Outgoing Only	+		×		.↓	Another Application	Email Client
Rules Q Blocked Application	Rules Q Blocked Application Outgoing Only	Add	Edit	Remove	Move Up	Move Down		Ftp Client
Blocked Application	Blocked Application Outgoing Only							Allowed Application
Outroing Only		_	es				Q	Blocked Application
		Rul						

#### View or edit an existing predefined Ruleset

• Double click on the ruleset Name in the list

Or

- Select the ruleset name then click the 'Edit' button
- Details of the process from this point on can be found here.

COMODO Creating Trust Online\*

### 6.3.5. Network Zones

- Click 'Settings' > 'Firewall' > 'Network Zones'
- A 'Network Zone' can consist of an individual machine (like a home computer connected to the internet), or a network of thousands of machines. Access to any network zone can be easily granted or denied in the network zones panel.
- The 'Network Zones' panel lets you configure:
  - Automatic detection of networks to which your computer can connect
  - Alerts for network connections
  - Trusted network zones which you want to allow
  - Untrusted network zones which you want to block

#### Open the 'Network Zones' panel

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'

COMODO Advance	d Settings ? — $\Box$ X
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>Firewall Settings</li> <li>Application Rules</li> <li>Global Rules</li> <li>Rulesets</li> </ul>	<ul> <li>Network Zones</li> <li>Enable automatic detection of private networks</li> <li>Do not show popup alerts and treat location as Work *</li> <li>The following network zones are defined on this computer:</li> <li>NETWORK ZONES</li> </ul>
Network Zones         Portsets         HIPS         Containment         File Rating         Advanced Protection	Add Edit Remove     Zone Name Q     Image: Dopback Zone     Image: Dopback #1
	OK CANCEL

- Enable automatic detection of private networks The firewall monitors attempted connections to any
  new wired or wireless network (*Default = Enabled*). Deselect this option if you are an experienced user and
  wish to manually set-up your own trusted networks (this can be done in 'Network Zones' and through the
  'Stealth Ports Wizard').
- **Do not show popup alerts and treat location as** CCS can show an alert when your computer attempts to connect to a new network.

COMODO Creating Trust Online\*

- **Disabled** The alert is shown. Select the appropriate network type for your connection. CCS will optimize the firewall for security and usability based on your choice. (*Default*)
- **Enabled** The alert is not shown. You now need to pick a default network type from 'Home', 'Work', or 'Public'. CCS will automatically apply your choice of network type to all new connections.

сом	ODO Network Detected	?
(lit.	Join a New Network Wired:	
Please se	elect your location:	
Î	I am at Home Choose if you are at home and have just connected your computer to a local network	
値	I am at Work Choose if you are at work place and have just connected your computer to a local network	
	I am at a Public Place Choose this option if you are at public place such as a coffee shop, hotel or school, etc.	
Do not	t detect new networks again	

 Select 'Do not detect new networks again' If you are an experienced user that wishes to manually set-up their own trusted networks. This can be done in 'Network Zones' and through the 'Stealth Ports Wizard'.

The panel has two tabs:

•

- Network Zones Define network zones with specific access rights. Application access privileges are specified in the Application Rule interface. See 'Create or Modify Firewall Rules' for more details.
- Blocked Zones Define networks that are not trusted. CCS will deny all connections to blocked zones.

#### 6.3.5.1. Network Zones

- Click 'Settings' > 'Firewall' > 'Network Zones' > 'Network Zones'
- A 'Network Zone' can consist of an individual machine (like a home computer connected to the internet) or a network of thousands of machines. You can grant or deny access to a network zone as required.

#### Background Note:

- A computer network is a connection between computers through a cabled or wireless connection.
- A network allows users to share information and resources with other computers/users on the network.
- There are some networks which you trust and want to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.

COMODO Creating Trust Online\*

• The network zones panel lets you configure trusted and untrusted networks.

#### Add and manage network zones

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab

COMODO Advance	ed Settings ? - C X
<ul><li>General Settings</li><li>Antivirus</li></ul>	Retwork Zones
— Firewall	☑ Enable automatic detection of private networks
Firewall Settings	Do not show popup alerts and treat location as Work *
Application Rules	The following network zones are defined on this computer:
Global Rules	NETWORK ZONES BLOCKED ZONES
Rulesets	
Network Zones	+ 🧟 🗱 Add Edit Remove
Portsets	Zone Name Q
✓ HIPS	🔲 🗈 🗄 Loopback Zone
✓ Containment	□
✓ File Rating	
<ul> <li>Advanced Protection</li> </ul>	
	OK CANCEL

The network zones tab shows zones that have already been added to CCS. You can add new zones and manage existing zones.

Note 1: Adding a zone to this area does not, by itself, define any permissions or access rights to the zone. This area lets you define the zones so you can assign such permissions in other areas of the firewall.

**Note 2**: A network zone can be designated as 'Trusted' and allowed access from the 'Manage Network Connections' interface. An example would be your home computer or network.

Note 3: A network zone can be designated as 'Blocked' and denied access by using the 'Blocked Zones' interface.

**Note 4**: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** assigned to a zone will inspect all traffic to/from a zone.

**Note 5**: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) once you connect to them. This can be disabled by deselecting the option 'Enable automatic detection of private networks' in the

COMODO Creating Trust Online\*

#### Firewall Settings panel.

You can use search for a specific zone by clicking the search icon and entering the name of the zone in part or full.

#### Defining a new Network Zone

To add a new network zone:

- Step 1 Define a name for the zone.
- Step 2 Select the addresses to be included in the zone.

#### Step 1 - Define a name for the zone

- Click 'Settings' on CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
- Click the 'Add' button at the top of the list and choose 'New Network Zone' from the options.

NETWORK ZO	DNES BLC	OCKED ZONES				
+ Add	ي Edit	<b>X</b> Remove				
	work Zone					Q
New Add	dress U Loopback .	Zone				
сом	000	Network Zone		?	×	
Zone Nar	ne					
My Home	e					
🔲 Public	Network					
			ОК	CANCEL		

- Choose a name that accurately describes the network zone you are creating.
- Select 'Public Network' if you are defining a network zone for a network in a public place. For example, when you are connecting to a Wi-Fi network at an airport, restaurant etc. The firewall will optimize the connection accordingly.
- Click 'OK' to confirm your zone name.

This adds your new zone to the 'Network Zones' list.

#### Step 2 - Select the addresses to be included in this zone

- Select the network zone name then click the 'Add' button at the top
- Choose 'New Address' from the options

COMODO Creating Trust Online\*

Alternatively, right click on the network zone and choose 'Add' > 'New Address' from the context sensitive menu

The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below (*Default* = *Any Address*).

The 'Exclude' check box will become active if you select anything other than 'Any Address'

The	e following netv	work zones are defined on this computer:	
N	ETWORK ZONES	BLOCKED ZONES	
	+ Add Ed	dit Remove	
	New Network Z		0
	] 🗈 🖽 Worl	rk/#2	
( ⊵	2 ) My Hon	me	
	сомо	Address ? ×	
	Exclude	e (i.e. NOT the choice below)	
	Туре:	Any Address 🔹	
		OK CANCEL	

#### Address Types:

.

- Any Defaults to an IP range of 0.0.0.0- 255.255.255 to block connection from all IP addresses.
- Host Name Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field
- IPv4 Address Range Choose all IP addresses covered by a range for example a range in your private network.
  - Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.
- IPv4 Single Address Choose a single IPv4 address

COMODO

### Comodo Client Security - User Guide

- Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
- IPv4 Subnet mask Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and Mask of the network.
- IPv6 Address Range Choose all IPv6 addresses covered by a range for example a segment in your private network
  - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
- Single IPv6 Address Choose an IPv6 address
  - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- IPv6 Subnet Mask Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and 'Mask' of the network in the respective fields
- MAC Address Choose a single source/destination by specifying its physical address
  - Enter the physical address in the 'MAC Address' text box.
- Exclude (i.e. NOT the choice below) The opposite of what you specify is applicable.
- Click 'OK' to confirm your choice.
- Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

• Quickly called as 'Zone' when creating or modifying a firewall ruleset

COMODO Creating Trust Online\*

сомодо	Firewall Rule ?	×
Action:	Allow   Log as firewall event if this rule is fired	
Protocol:	TCP or UDP 🔻	
Direction:	In or Out	
Description		
SOURCE ADDRESS	DESTINATION ADDRESS SOURCE PORT DESTINATION PORT	
Тур		
Zo	ne Loopback Zone Loopback Zone Work #1 Work #2 Work #3 Work #4 Talkatives Computers Work #5 OK CANC	EL

• Quickly called and designated as a blocked zone from the 'Blocked Zones' interface

#### Edit the name of an existing Network Zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
- Select the zone from the list (e.g., My Home) and click the 'Edit' button from the top or double click on the network zone name.

Creating Trust Online\*

COMODO Network Zone		? ×
Zone Name My Home Public Network		
	ОК	CANCEL

• Change the name of the zone and click 'OK'.

#### To add more addresses to an existing Network Zone

- Select the network name, click the 'Add' > 'New Address' from the top.
- Add new address from the 'Address' interface.

#### To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click 'Edit' at the top
- Edit the address from the 'Address' interface.

#### To remove an existing address in a zone

- Click the '+' button beside the network zone name to expand the addresses
- Select the address and click 'Remove' from the top

#### 6.3.5.2. Blocked Zones

- Click 'Settings' > 'Firewall' > 'Network Zones' > 'Blocked Zones'
- A computer network lets you share information and resources with other users and computers.
- There are some networks which you trust and want to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.
- The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not trust.

Note: We advise new or inexperienced users to first read 'Network Zones', 'Stealth Ports Wizard' and 'Application Rules' before blocking zones in this interface.

#### Add and manage blocked zones

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab:

COMODO Creating Trust Online\*

COMODO Advanced	Settings ? - □ ×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Network Zones
— Firewall	✓ Enable automatic detection of private networks
Firewall Settings	Do not show popup alerts and treat location as Work *
Application Rules	The following network zones are defined on this computer:
Global Rules	NETWORK ZONES BLOCKED ZONES
Rulesets	
Network Zones	+ 🧟 🗱 Add Edit Remove
Portsets	Zone Name Q
✓ HIPS	
<ul> <li>Containment</li> </ul>	
✓ File Rating	
✓ Advanced Protection	
	OK CANCEL

The 'Blocked Network Zones' tab allows you to:

- Deny access to an existing network zone
- Deny access to a network by manually defining a new blocked zone

Note 1: You must create a zone before you can block it. There are two ways to do this;

- 1. Using 'Network Zones' to name and specify the network you want to block.
- 2. Directly from this interface using 'New blocked address...'

**Note 2**: You cannot reconfigure *existing* zones from this interface (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

You can search for specific blocked zone by clicking the magnifying glass icon and entering the name of the zone in part or full.

#### Deny access to an existing network zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- · Click 'Add' button at the top and choose 'Network Zones' from the options
- Select the particular zone you wish to block.

COMODO Creating Trust Online\*

NETWORK ZO	DNES BLOCI	KED ZONES	
+ Add	<b>e</b> Edit	<b>X</b> Remove	
	Zones cked Address Cottee Cup T	Loopback Zone Work #1 Work #2 Work #3 Coffee Cup Network Hotel Stale Food Work #6	
		Home #1	

The selected zone will appear in the 'Blocked Zones' interface.

+ Add	ے۔ Edit	<b>X</b> Remove		
Zoi	ne Name			
	🗄 Coffee Ci	up Network	Name of the	
	🗏 Hotel Sta	le Food 🦊	Blocked Network Zone	
	— IP 10.10	.111.111	IP address(es) that are associated with	
	_ IP 10.10	222.222	the Blocked Zone. You can modify these settings under the 'Network Zones' tab	

COMODO Creating Trust Online\*

- Click 'OK' to confirm your choice.
- All traffic to and from devices in this zone is now blocked.

#### Deny access to a network by manually defining a new blocked zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- Click the 'Add' button and choose 'New Blocked Address':

	BLOCKED ZONES	
	💒 🗰 Edit Remove	
4		
Network Zone		
New Blocked	Address Tree cup Network	
] 🗈 🖽 Но	tel Stale Food	
	<u></u>	
	Λ.	
	N	
сомо	Address	? ×
сомо	Address	? ×
	Address e (i.e. NOT the choice below)	? ×
Exclude	e (i.e. NOT the choice below)	? ×
	e (i.e. NOT the choice below)	? ×
Exclude	e (i.e. NOT the choice below)	? ×
Exclude	e (i.e. NOT the choice below)           Any Address <ul> <li>Any Address</li> <li>Host Name</li> </ul>	? ×
Exclude	e (i.e. NOT the choice below)          Any Address         Any Address         Host Name         IPv4 Address Range	? ×
Exclude	e (i.e. NOT the choice below)           Any Address <ul> <li>Any Address</li> <li>Host Name</li> </ul>	? ×
Exclude	e (i.e. NOT the choice below)          Any Address         Any Address         Host Name         IPv4 Address Range         IPv4 Single Address         IPv4 Subnet Mask	
Exclude	e (i.e. NOT the choice below)          Any Address <ul> <li>Any Address</li> <li>Any Address</li> <li>Host Name</li> <li>IPv4 Address Range</li> <li>IPv4 Single ddress</li> </ul>	? × CANCEL

Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

#### Address Types:

- Any Defaults to an IP range of 0.0.0.0- 255.255.255 to block connection from all IP addresses.
- Host Name Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field
- IPv4 Address Range Choose all IP addresses covered by a range for example a range in your

private network.

- Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.
- IPv4 Single Address Choose a single IPv4 address
  - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
- IPv4 Subnet mask Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and Mask of the network.
- IPv6 Address Range Choose all IPv6 addresses covered by a range for example a segment in your private network
  - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
- Single IPv6 Address Choose an IPv6 address
  - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- IPv6 Subnet Mask Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and 'Mask' of the network in the respective fields
- MAC Address Choose a single source/destination by specifying its physical address
  - Enter the physical address in the 'MAC Address' text box.
- Exclude (i.e. NOT the choice below) The opposite of what you specify is applicable.
- Select the address to be blocked and click 'OK'

The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

 Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

### 6.3.6. Port Sets

- Click 'Settings' > 'Firewall' > 'Portsets'
- Port sets are predefined groups of one or more ports. These sets can be named as the target of Application Rules and Global Rules. For example, you might want to block all inbound traffic to certain set of ports.
- The port sets panel lets you add, view and manage port sets

#### Open the Portsets panel

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

COMODO Creating Trust Online\*

COMODO Advanced Settings ? - C ×			
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Portsets The following portsets are defined on this computer:		
Firewall Settings Application Rules	+ 💉 🗱 Add Edit Remove		
Global Rules	Portset		Q
Rulesets	E HTTP Ports		
Network Zones	E POP3/SMTP Ports		
Portsets	🗌 🗄 Privileged Ports		
✓ HIPS			
✓ Containment			
✓ File Rating			
✓ Advanced Protection			
	ок		CANCEL

- The interface lists all existing port sets. Click the + button to view all ports in a set.
- CCS ships with three default portsets:
  - HTTP Ports: 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.
  - **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
  - Privileged Ports: 0-1023. Privileged ports are so called because it is usually desirable to prevent
    users from running services on these ports. Network admins usually reserve or prohibit the use of
    these ports. This set can be deployed if you wish to create a rule that allows or blocks access to the
    privileged port range.

#### Define a new port set

After defining a new port set, you can apply it to applications through the **Application Rule** interface. See 'Creating or **Modifying Firewall Rules**' for more details.

#### Add a new portset

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Portsets'
- Click the 'Add' button at the top.

COMODO Creating Trust Online\*

COMODO Add Portset						×
Name: Spec	ial Ports					]
+ Add	Edit	<b>X</b> Remove				
Por	ts					Q
			OK		CANCEL	//

- Create a name for the port set
- Click 'Add' to specify ports and port ranges for the set:

COMODO Add Portset	?		×
Name: Special Ports			
+ & * Add Edit Remove			
Ports			Q
COMODO Port	?	×	
Exclude (i.e. NOT the choice below)			
⊖ Any			
● A Single Port 0			
O A Port Range 0 ÷ - 0 ÷			
ОК	CANCEL		

COMODO Creating Trust Online\*

- Specify the ports to be included in the new portset:
  - Any to choose all ports
  - A single port Specify the port number
  - A port range Enter the start and end port numbers in the respective combo boxes.
  - Exclude (i.e. NOT the choice below): Means all ports will be included in the portset except the ones you specify here
- · Click 'OK' in the 'Port' dialog then click 'OK' in the 'Add Portset' interface

You can now select 'A Set of Ports', then choose this rule-set, when **creating or modifying a Firewall Ruleset** 

	rewall Rule ?	×
Action: Al	llow <ul> <li>Log as firewall event if this rule is fired</li> </ul>	
Protocol: TC	CP or UDP 🔻	
Direction: In	n or Out	
Description		
SOURCE ADDRESS	DESTINATION ADDRESS SOURCE PORT DESTINATION PORT	
Exclude (i.e. NOT	the choice below)	
Туре:	A Set of Ports	
Ports:	HTTP Ports	
	HTTP Ports	
	POP3/SMTP Ports	
( C	Privileged Ports Special Ports	
	Special Ports	
1		
	OK CANCE	-

#### Edit an existing port set

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Portsets'
- Select the port set from the list
- Click the 'Edit' button
- The editing procedure is similar to adding the portset explained above.

COMODO Creating Trust Online\*

### 6.4. HIPS Configuration

- Click 'Settings' > 'HIPS'
- The host intrusion protection system (HIPS) constantly monitors system activity and stops processes from modifying important files and interfaces.
- Comodo Client Security ships with a default HIPS ruleset that works 'out of the box' providing extremely high levels of protection.
  - For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs.
- Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

#### **Configure HIPS settings**

- Click 'Settings' on the CCS home screen
- · Click 'HIPS' on the left:

COMODO Advanced	Settings ? - $\Box$ ×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	HIPS Settings
<ul><li>✓ Firewall</li><li>→ HIPS</li></ul>	Safe Mode  Monitoring Settings
HIPS Settings HIPS Rules Rulesets Protected Objects HIPS Groups Containment File Rating Advanced Protection	This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.
	OK CANCEL

- HIPS Settings General settings that govern the overall behavior of the HIPS component.
- HIPS Rules These rules determine what actions an application is allowed to perform, and what level of
  protection it enjoys from other processes.
- Rulesets View predefined rulesets and create new rulesets that can be applied to your applications in your system.
- · Protected Objects Define objects to be protected by HIPS such as specific folders, system critical

COMODO Creating Trust Online\*

registry keys and so on.

 HIPS Groups - View and edit predefined 'Registry Groups' and 'COM Groups', create new groups so as to add them to Protected Objects.

#### Note for beginners:

- This section often refers to 'executables' (or 'executable files'). An executable is a file that can instruct your computer to perform a task or function.
- Every program, application and device you run on your computer requires an executable file of some kind to start it.
- The most recognizable type of executable file is the '.exe' file. For example, 'winword.exe' is the name of the executable that instructs your computer to start and run Microsoft Word. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.
- Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can
  instruct your computer to delete valuable data, steal your identity, corrupt system files, hand control of your
  PC to a hacker and more. You may also have heard these referred to as Trojans, scripts and worms.

### 6.4.1. HIPS Settings

- Click 'Settings' > 'HIPS' > 'HIPS Settings'
- HIPS settings let you enable/disable HIPS, set HIPS security level, and configure the general behavior of the HIPS module.

#### Open the 'HIPS Settings' panel

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'HIPS Settings'

COMODO Creating Trust Online\*

COMODO Advanced	Settings ? - □ ×
<ul><li>General Settings</li><li>Antivirus</li></ul>	HIPS Settings
✓ Firewall	Enable HIPS
- HIPS	Safe Mode  Monitoring Settings
HIPS Settings	This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.
HIPS Rules Rulesets Protected Objects HIPS Groups Containment File Rating Advanced Protection	<ul> <li>Do not show popup alerts Allow Requests </li> <li>Set popup alerts to verbose mode</li> <li>Create rules for safe applications</li> <li>Set new on-screen alert timeout to 60 secs</li> <li>Advanced</li> <li>Enable adaptive mode under low system resources</li> <li>Block all unknown requests when the application is not running</li> </ul>
	OK CANCEL

• Enable HIPS - Activate or deactivate the HIPS protection. (Default=Disabled)

If enabled, you can configure the HIPS security level and monitoring settings:

#### **Configure HIPS Security Level**

• Choose the security level from the drop-down under the 'Enable HIPS' check-box:

Enable HIPS	
Safe Mode 🔻 Monit	oring Settings
Paranoid Mode	Host Intrusion Protection
Safe Mod្រា	tivities to protect the
Training Mode	

The choices available are:

Paranoid Mode: This is the highest security level setting and means that HIPS monitors and controls all
executable files apart from those that you have deemed safe. Comodo Client Security does not attempt to
learn the behavior of any applications - even those applications on the Comodo safe list and only uses your
configuration settings to filter critical system activity. Similarly, CCS does not automatically create 'Allow'
rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS
alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced
users that require complete awareness of activity on their system.

COMODO Creating Trust Online\*

- Safe Mode: While monitoring critical system activity, HIPS automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules for these activities, if the checkbox 'Create rules for safe applications' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the HIPS rules list by choosing 'Treat as' and selecting 'Allowed Application' at the alert with 'Remember my answer' checked. This instructs the HIPS not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats then 'Safe Mode' is recommended setting for most users combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Training Mode**: HIPS monitors and learns the activity of any and all executables and creates automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

#### **Configure Monitoring Settings**

Click the Monitoring Settings link to select the activities and objects that should be monitored by HIPS

**Note**: The settings you choose here are universally applied. If you disable monitoring of an activity or object here, it completely switches off monitoring of that activity on a *global* basis - effectively creating a universal '*Allow*' rule for the activity. This 'Allow' setting *over-rules* any specific 'Block' or 'Ask' setting for the activity that you may have created in the 'Access Rights' and 'Protection Settings' interfaces.

Creating Trust Online\*

ced Settings	?	-		>
HIPS Settings				
☑ Enable HIPS				
Safe Mode Monitoring	ttings			
-	trusion Protection System, the compores to protect the computer against ma			S
COMODO Monitoring Settings			?	×
Activities to Monitor				
✓ Interprocess Memory Accesses	Process Execution			
☑ Windows/WinEvent Hooks	Window Messages			
Device Driver Installations	DNS/RPC Client Service			
Processes' Terminations				
Objects to Monitor Against Mod	ifications			
Protected COM Interfaces	Protected Registry Keys			
Protected Files/Folders				
Objects to Monitor Against Direc	t Access			
	_			
Physical Memory	Disks			

#### **Activities To Monitor:**

- Interprocess Memory Access Malware programs use memory space modification to inject malicious code for numerous types of attacks. These include recording your keyboard strokes; modifying the behavior of applications and stealing data by sending confidential information from one process to another. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of a compromised process to 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application (Default = Enabled).
- Windows/WinEvent Hooks In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events *before* they reach an application. Example intercepted events include messages, mouse actions and keystrokes. Hooks can react to these events and, in some cases, modify or

COMODO Creating Trust Online

discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer and take remote control of your computer. Leaving this box checked means that you are warned every time a hook is executed by an untrusted application (*Default = Enabled*).

- Device Driver Installations Device drivers are small programs that allow applications and/or operating systems to interact with hardware devices on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application (*Default* = *Enabled*).
- Processes' Terminations A process is a running instance of a program. (for example, the Open VPN GUI process is called 'openvpn.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, HIPS monitors and alerts you to all attempts by an untrusted application to close down another application (*Default = Enabled*).
- Process Execution Malware such as rootkits and key-loggers often execute as background processes. With this setting enabled, HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. (Default = Enabled).
- Windows Messages This setting means Comodo Client Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM\_PASTE command) (*Default = Enabled*).
- DNS/RPC Client Service This setting alerts you if an application attempts to access the 'Windows DNS service' possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service (DDoS) attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed so that they appear to come from the target or 'victim' server but in fact come from different sources often a network of 'zombie' PCs which are sending out these requests without their owners' knowledge. The DNS servers are tricked into sending all their replies to the victim server overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack (*Default = Enabled*).

**Background Note**: DNS stands for Domain Name System. It is the part of the internet infrastructure that matches a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the internet routes messages to their destinations using these IP addresses, not the domain name you type into your browser. Whenever you enter a domain name, your internet browser contacts a DNS server and makes a 'DNS Query'. In simple terms, this query is 'What is the IP address of example.com?'. The DNS server replies to your browser, telling it to connect to the IP in question.

#### **Objects To Monitor Against Modifications:**

- Protected COM Interfaces HIPS monitors the COM interfaces you specified from the COM Protection pane. (Default = Enabled)
- Protected Registry Keys HIPS monitors the Registry keys you specified from the Registry Protection pane. (Default = Enabled).
- Protected Files/Folders HIPS monitors the files and folders you specified from the File Protection pane. (Default = Enabled).

#### **Objects To Monitor Against Direct Access:**

 Whether or not Comodo Client Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these

COMODO

settings enabled:

- Physical Memory: Monitors your computer's memory for direct access by applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code (Default = Enabled).
- Computer Monitor: Comodo Client Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, spyware can also use such access to take screen shots of your current desktop, record your browsing activities and more. (Default = Enabled).
- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data (*Default = Enabled*).
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Client Security alerts you every time an application attempts to establish direct access to your keyboard (*Default = Enabled*).

#### **Checkbox Options**

 Do not show popup alerts - Whether or not you want to be notified when the HIPS encounters malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness (Default = Disabled).

If you choose not to show alerts then you have a choice of default responses that CCS should automatically take - either 'Block Requests' or 'Allow Requests'.

o not show popup alerts	Allow Requests 🔻	
Set popup alerts to verbose n	Allow Requests Block Requests	
Create rules for safe applications		
Set new on-screen alert timeout to 120 secs		

- Set popup alerts to verbose mode HIPS alerts provide more information and options for the user to allow or block the requests (Default = Disabled).
- Create rules for safe applications HIPS trusts applications if:
  - The application is on the Comodo safe list, a global white-list of trusted software.
  - The application has a 'Trusted' rating in the local file list. See File List if you need more details.
  - The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file. See **Vendor List** if you need more details.

By default, CCS does not automatically create 'allow' rules for safe applications. This helps to reduce resource usage, to simplify the rules interface by reducing the number of 'Allow' rules, and can reduce the number of pop-up alerts. Enabling this option instructs CCS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **HIPS Rules** interface. Advanced users can edit / modify the rules as they wish.

• Set new on-screen alert time out to: How long a HIPS alert remains on-screen if it is not answered. The default timeout is 120 seconds. You may adjust this setting to your own preference.

#### **Advanced HIPS Settings**

COMODO Creating Trust Online\*

Note: These settings are recommended for advanced users only.

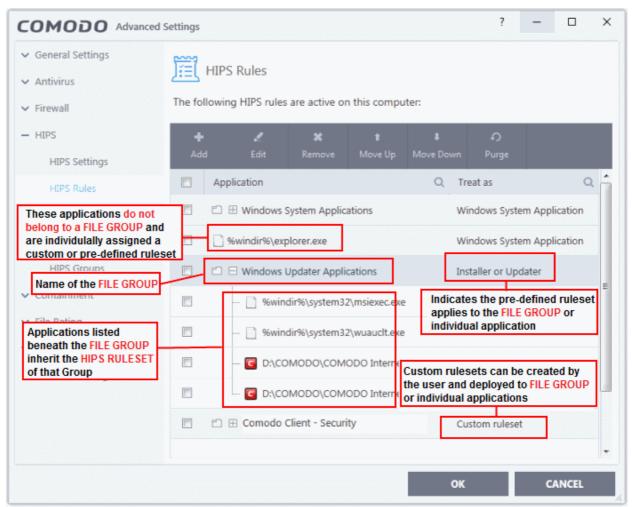
- Enable adaptive mode under low system resources Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems (*Default = Disabled*).
- 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 CCS
  security settings then it is OK to leave this box unchecked. (Default = Disabled)

### 6.4.2. Active HIPS Rules

- Click 'Settings' > 'HIPS' > 'HIPS Rules'
- The rules screen shows your installed applications classified into file groups, and the HIPS ruleset that applies to them.
- You can change the ruleset of a specific application or file group, and create your own custom rulesets.

#### Open the 'HIPS Rules' panel

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'HIPS Rules'



COMODO Creating Trust Online\*

The first column, **Application**, displays a list of the applications on your system for which a HIPS ruleset has been defined. If the application belongs to a file group, then all member applications assume the ruleset of the group. The second column, **Treat As**, displays the name of the HIPS ruleset assigned to the application or group of applications.

You can use the search option to find a specific file in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

#### **General Navigation:**

The control buttons at the top of the list enable you to create and manage application rule sets.

ed Settings					?	—		×
Fill HIP	S Rules							
The followin	ng HIPS rules	are active o	n this compu	iter:				
+ Add	<b>.</b> Edit	🗱 Remove	t Move Up	<b>↓</b> Move Down	Ю Purge		>	
Ap	plication			Q Trea	t As		c	2 ^
	%windir%\ex	olorer eve		Wind	lows Sys	tem Ap	plication	

- Add Allows the user to add a new application to the list and then create its ruleset. See the section 'Creating or Modifying a HIPS Ruleset'.
- Edit Allows the user to modify the HIPS rule of the selected application. See the section 'Creating or Modifying a HIPS Ruleset'.
- **Remove** Deletes the selected ruleset.

Note: You cannot add or remove individual applications from a file group using this interface - you must use the 'File Groups' interface to do this.

- Purge Runs a system check to verify that all the applications for which rulesets are listed are actually
  installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- Move UP/Move Down Users can re-order the priority of rules by simply selecting an application name or file group and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the 'File Groups' interface.

#### **Creating or Modifying a HIPS Ruleset**

•

Defining a HIPS Ruleset for an application or File group involves two steps:

- 1. Select the application or file group that you wish the ruleset to apply to.
- 2. Configure the ruleset for this application.

#### Step 1 - Select the application or file group that you wish the ruleset to apply to

To define a rule for a new application (i.e. one that is not already listed), click the 'Add' button at the top of the **HIPS Rules pane**.

This brings up the 'HIPS Rule' interface as shown below.

COMODO Creating Trust Online\*

COMODO HIPS Rule		? [	- ×
Name:		[	Browse 🖲
Use Ruleset:	Allowed Appl	lication <b>•</b>	
⊖ Use a Custom Ruleset		Сор	y from 🖲
ACCESS RIGHTS PROTECTION SETTIN	GS		
Access Name	Action	Exclusions	
Access Name	Action Ask	Exclusions Modify (0\0)	
Run an executable	Ask	Modify (0\0)	
<ul> <li>Run an executable</li> <li>Interprocess Memory Accesses</li> </ul>	Ask	Modify (0\0) Modify (0\0)	

The 'Name' box is blank because you are defining a HIPS rule settings for a new application. If you were editing an existing rule, this field would show the application name and its installation path, or the application group name.

• Click 'Browse' to begin.

You now have 3 methods available to choose the application for which you wish to create a Ruleset - File Groups; Applications and Running Processes.

 File Groups - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl \*\cmd.exe, \*.bat, \*.cmd. Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

COMODO Creating Trust Online

		? 🗆	ı x	
Name:		B	rowse 🔻	
Our Search State Stat		Allowed Ap	File Groups	Executables All Applications Important Files/Folders
O Use a Custom Ruleset		Copy	from ¥	Windows Updater Applications
ACCESS RIGHTS PROTECTION SETTIN				Windows System Applications Temporary Files COMODO Client Files/Folders
Access Name	Action	Exclusions	^	Comodo Client - Security
		11. // mm		COMODO Applications
Run an executable	<u>Ask</u>	Modify (0\0)		Startup Folders Windows Management
Interprocess memory accesses	Ask	Modify (0\0)		3rd Party Protocol Drivers
		1		Metro Apps
Windows/WinEvent hooks	<u>Ask</u>	Modify (0\0)		Management and Productivity Applications
Processes' termination	Ask	Modify (0\0)		Web Browsers
				Email Clients
Device drivers' installation	<u>Ask</u>	Modify (0\0)	<b>.</b>	Suspicious Locations
				Shared Spaces
		OK CAN	CEL	File Downloaders Pseudo File Downloaders
			A	Pseudo File Downloaders File Archivers
				Containment Folders
				Browser Plugins
				Media Players

To view the file types and folders that are affected by choosing one of these options, you need to visit the **'File Groups'** interface.

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.

COMODO Creating Trust Online\*

- → × ↑ 📙 « I	Progra > DrivingSpeed2 > V	ල් Search DrivingSpeed2	Q
Organize 👻 New fo	der		
🖈 Quick access	Name	Date modified	Туре
	🔄 data	11/9/2016 4:05 PM	VI File fold
aneDrive 🍊 🗥	🛷 DrivingSpeed	1/6/2012 3:58 PM	Applicat
💻 This PC	📄 eula	9/9/2009 9:02 PM	Text Doo
	e helpfaq	3/20/2010 12:34 P	M HTML F
💣 Network	readme	10/11/2011 10:35	Text Do
🔩 Homegroup	📄 unins000.dat	11/9/2016 4:06 PM	M DAT File
	🔂 unins000	11/9/2016 4:04 PM	M Applicat
	📄 website	8/26/2007 4:13 PM	M Internet
	<		
File	name: DrivingSpeed	<ul> <li>All Files (*.*)</li> </ul>	~

3. **Running Processes** - as the name suggests, this option allows you choose any process that is currently running on your PC in order to create and deploy a ruleset for its parent application.

COMODO Creating Trust Online\*

	815	
Application	PID 2624	2000
▼ III unit_manager.exe		^
▲ III unit.exe	4264	
conhost.exe	4464	
🕫 🙀 explorer.exe	2440	
🔺 磕 OneDrive.exe	3236	
<ul> <li>DrivingSpeed.exe</li> </ul>	4152	
RuntimeBroker.exe	3168	
🛚 🚨 SearchIndexer.exe	3304	
🖉 🔄 System	4	
smss.exe	284	
svchost.exe	8	
🛚 🌕 GeekBuddyRSP.exe	1600	
SearchUl.exe	3808	
cavwp.exe	2324	
csrss.exe	428	
🖷 🔀 vkise.exe	4040	
svchost.exe	1824	
	coo	Y
	OK CANCEL	

Having selected the individual application, running process or file group, the next stage is to configure the rules for this ruleset.

#### Step 2 - Configure the HIPS Ruleset for this application

There are two broad options available for selecting a ruleset that applies to an application - Use Ruleset or Use a Custom Ruleset.

1. Use Ruleset - Selecting this option allows you to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the HIPS Rules interface (*Default = Enabled*).

COMODO HIPS Rule		?		×	
Name: C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe			Brow	se 🔻	
Use Ruleset:	Allo		Applicatio		
Use a Custom Ruleset			lows Syst ained Ap		
			ted Applie ller or Up		

COMODO Creating Trust Online\*

**Note on 'Installer or Updater' Rule**: Applying this rule to an application defines it as a trusted installer. All files created by this application will also be trusted. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this 'Predefined Ruleset' - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.

**General Note**: Predefined Rulesets cannot be modified directly from this interface - they can only be modified and defined using the '**Rulesets**' interface. If you require the ability to add or modify settings for a specific application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use a Custom Ruleset** option instead.

2. **Use a Custom Ruleset** - Designed for more experienced users, the 'Custom Ruleset' option grants full control over the configuration of each rule within that ruleset.

The custom ruleset has two main configuration areas - Access Rights and Protection Settings.

In simplistic terms 'Access Rights' determine what the application *can do to other processes* and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

	ule	?		
lame: C:\Program Files	(x86)\DrivingSpeed2\DrivingS	peed.exe	Browse 🔻	
Use Ruleset:		Allowed Ap	oplication •	
Use a Custom Ruleset		C	opy from 🔻	
ACCESS REGISTS PROPER	778096 98777894G5		Ruleset Another Applic	Allowed Application Windows System Applicat Contained Application
Access Name	Action	Exclusions		Limited Application

i. Access Rights - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset. These activities are called 'Access Names'.

COMODO Creating Trust Online\*

		? 🗆	×
Name: C:\Program Files (x86)\Drivin	gSpeed2\DrivingS	peed.exe Bro	owse 🔻
○ Use Ruleset:		Allowed Applica	ation 🔻
Output Use a Custom Ruleset		Copy f	rom 🔻
ACCESS RIGHTS PROTECTION SETTING	GS		
Access Name	Action	Exclusions	^
37 Run an executable	Ask	Modify (0\0)	
Interprocess Memory Accesses	Ask	<u>Modify (0\0)</u>	
Windows/WinEvent Hooks	Ask	Modify (0\0)	
Processes' Termination	Ask	<u>Modify (0\0)</u>	
Device Drivers' Installation	Ask	Modify (0\0)	
		OK CANC	EL

See HIPS Settings > Activities to Monitor to see definitions of the 'Action Names' listed above, and the implications of choosing 'Ask', 'Allow' or 'Block':

Interprocess Memory Accesses	Ask	<u>Modify (0\0)</u>	
Windows/WinEvent Hooks	Ask	Modify (0\0)	

- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.

Creating Trust Online\*

Run an executable Ask	Modify (0\0)
Interprocess Memory Accesses Block	
Windows/WinEvent Hooks Ask	Modify (0\0)
COMODO Interprocess Memory Accesses	? 🗆 X
ALLOWED FILES/FOLDERS BLOCKED FILES/FOLDERS	
+ X X Add Edit Remove	
Path	Q
🔲 🖆 🗄 File Downloaders	
	OK CANCEL

Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

In **the example above**, the default action for 'Interprocess Memory Access' is 'Block'. This means HIPS will block the action if 'DrivingSpeed.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'File Downloaders' File Group to the 'Allowed Files\Folders' area creates an exception to this rule. 'DrivingSpeed.exe' can now modify the memory space of files belonging to the 'File Downloaders' File Group.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.

COMODO Creating Trust Online\*

COMODO HIPS Rule ? D X						
Name: C:\Program Files (x86)\DrivingSp	eed2\DrivingSpeed.exe	Browse 🔻				
O Use Ruleset:	Allowed Application <b>•</b>					
Output State St		Copy from 🔻				
ACCESS RIGHTS PROTECTION SETTINGS	_					
Protection	State	Exclusions				
Interprocess Memory Accesses	Inactive	Modify (0)				
Windows/WinEvent Hooks	Inactive	Modify (0)				
Processes' Termination	Inactive	Modify (0)				
Window Messages	Inactive	Modify (0)				
	OF	CANCEL				

• Set the 'State' as 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

### 6.4.3. HIPS Rule Sets

- Click 'Settings' > 'HIPS' > 'Rulesets'
- A ruleset is a collection of access rights and protection settings that can be applied to applications on your computer.
- Each ruleset consists of a number of rules, and each of these rules is defined by a set of conditions and parameters. Rulesets govern an application's rights to access memory, other programs, the registry etc.
- CCS ships with six predefined rulesets that provide a very high level of protection. You can also create your own.

Note: This section is for advanced users. If you are new CCS user, we advise you first read the Active HIPS Rules

COMODO Creating Trust Online\*

### section in this help guide.

Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo provide a set of pre-defined rulesets which optimize security on a range of application types.

- You can modify these predefined rulesets to suit your requirements.
- You can also create new custom rule sets with your own constituent rules
- You can also apply a HIPS ruleset to an application at a HIPS alert. Both predefined and custom rulesets are made available. An example alert is shown below:

сом	ODO HIPS	?
	SunGazer.exe is trying to modify a protected registry key	$\odot$
SunG	Sazer.exe Modify	ey
	Treat as Lets you choose a ruleset to apply	$\sim$
0	Allowed Application	^
0	Windows System Application	
0	Contained Application	
0	Limited Application	
0	My Fav Games	~
Remem	iber my answer Show	Activities

See **answering HIPS alerts** if you want more help with alerts.

### View the list of HIPS Rulesets

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Rulesets'

COMODO Creating Trust Online\*

COMODO Advanced	Settings	?	_		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Rulesets The following rulesets are defined on this computer:				
— HIPS HIPS Settings	+     ✓       Add     Edit				
HIPS Rules	Ruleset Name				Q
Rulesets	Allowed Application				
Protected Objects	Windows System Application				
HIPS Groups	Contained Application				
✓ Containment	Limited Application				
✓ File Rating					
✓ Advanced Protection					
Website Filtering					
	ок		C	ANCEL	

• Click the search icon and enter the name of a ruleset name in full or part to search for a specific ruleset.

#### View or edit a ruleset

• Double click on the 'Ruleset' in the list

or

• Select the 'Ruleset' and click the 'Edit' button at the top of the interface

From here, you can make changes to its 'Access Rights' and 'Protection Settings'. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset.

#### Create a new ruleset

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Rulesets'
- · Click the 'Add' button at the top of the interface

COMODO Creating Trust Online\*

General Settings   Antivirus   Firewall   HIPS   HIPS Settings   HIPS Rules   Ruleset Name   Rulesets	MODO Advanced Settings			?
Firewall The following rulesets are defined on this computer:   HIPS Add   Edit Remove   Add Edit   Ruleset Remove     Rulesets Allowed Application     COMODO HIPS Ruleset ? ×     Name: Copy from •     Access RiGHTS PROTECTION SETTINGS     Access Name Action   Exclusions *   Access Name Action   Edit *   Access Name Action   Edit *   Modify (0\0)   Interprocess Memory Accesses Ask   Modify (0\0)   Processes' Termination Ask   Modify (0\0)   Window Messages Ask   Modify (0\0)	i Rule	esets		
HIPS Settings HIPS Settings HIPS Rules Rulesets Rulesets Rulesets Ruleset Ru			d an this annual an	
Add       Edit       Remove         HIPS Rules       Ruleset Name         Rulesets       Allowed Application         COMODO       HIPS Ruleset       ? ×         Name:       Copy from •         Access Rights       PROTECTION SETTINGS         Access Name       Action       Exclusions         ### Run an executable       Ask       Modify (0\0)         Interprocess Memory Accesses       Ask       Modify (0\0)         Windows/WinEvent Hooks       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Device Drivers' Installation       Ask       Modify (0\0)         Window Messages       Ask       Modify (0\0)	irewall	ig rulesets are define	d on this computer:	
HIPS Rules   Rulesets     Allowed Application     COMODO HIPS Ruleset   ?     X     Name:     Copy from •     ACCESS RIGHTS   PROTECTION SETTINGS     Access Name   Access Name   Access Name   Access Name   Access Name   Access Name   Action   Exclusions     ***   Run an executable   Ask   Modify (0\0)   Interprocess Memory Accesses   Ask   Modify (0\0)   Processes' Termination   Ask   Modify (0\0)   ***   Device Drivers' Installation   Ask   Modify (0\0)   ***   Modify (0\0)	Add		ve	
COMODO HIPS Ruleset       ? ×         Name:       Copy from •         ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action         Exclusions       *         Sar Run an executable       Ask         Modify (0\0)         Interprocess Memory Accesses       Ask         Modify (0\0)         Windows/WinEvent Hooks       Ask         Modify (0\0)         Processes' Termination       Ask         Modify (0\0)         Device Drivers' Installation       Ask         Modify (0\0)         Window Messages       Ask		eset Name		
COMODO HIPS Ruleset       ? ×         Name:       Copy from •         ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action         Exclusions       ^         S27 Run an executable       Ask         Modify (0\0)         Interprocess Memory Accesses       Ask         Modify (0\0)         Windows/WinEvent Hooks       Ask         Modify (0\0)         Processes' Termination       Ask         Modify (0\0)         Device Drivers' Installation       Ask         Modify (0\0)         Window Messages       Ask	Rulesets Allo	wed Application		
Name:       Copy from •         ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action       Exclusions         Access Name       Action       Exclusions         Image:       Access Name       Action       Exclusions         Access Name       Action       Exclusions       Access Name         Image:       Access Name       Action       Exclusions         Image:       Ask       Modify (0\0)       Image:       Image:         Image:       Ask       Modify (0\0)       Image:       Image				
Name:       Copy from •         ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action       Exclusions         Access Name       Action       Exclusions         Image:       Access Name       Action       Exclusions         Access Name       Action       Exclusions       Access Name         Image:       Access Name       Action       Exclusions         Image:       Ask       Modify (0\0)       Image:       Image:         Image:       Ask       Modify (0\0)       Image:       Image				2 4
ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action       Exclusions         Access Name       Ask       Modify (0\0)         Interprocess Memory Accesses       Ask       Modify (0\0)         Interprocess Memory Accesses       Ask       Modify (0\0)         Windows/WinEvent Hooks       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Device Drivers' Installation       Ask       Modify (0\0)         Window Messages       Ask       Modify (0\0)	COMODO HIPS Ruleset			r x
ACCESS RIGHTS       PROTECTION SETTINGS         Access Name       Action       Exclusions         Access Name       Ask       Modify (0\0)         Interprocess Memory Accesses       Ask       Modify (0\0)         Interprocess Memory Accesses       Ask       Modify (0\0)         Windows/WinEvent Hooks       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Device Drivers' Installation       Ask       Modify (0\0)         Window Messages       Ask       Modify (0\0)	Name:		C	opy from 🔻
Access Name       Action       Exclusions         Image: Run an executable       Ask       Modify (0\0)         Image: Interprocess Memory Accesses       Ask       Modify (0\0)         Image: Nindows/WinEvent Hooks       Ask       Modify (0\0)         Image: Processes' Termination       Ask       Modify (0\0)         Image: Device Drivers' Installation       Ask       Modify (0\0)         Image: Window Messages       Ask       Modify (0\0)				
Access Name       Action       Exclusions         Image: Stress Name       Ask       Modify (0\0)         Image: Interprocess Memory Accesses       Ask       Modify (0\0)         Image: Interprocess Memory Accesses       Ask       Modify (0\0)         Image: Windows/WinEvent Hooks       Ask       Modify (0\0)         Image: Processes' Termination       Ask       Modify (0\0)         Image: Processes' Termination       Ask       Modify (0\0)         Image: Device Drivers' Installation       Ask       Modify (0\0)         Image: Window Messages       Ask       Modify (0\0)	ACCESS RIGHTS PROTECTION SETTIN	IGS		
Interprocess Memory Accesses       Ask       Modify (0\0)         Windows/WinEvent Hooks       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Device Drivers' Installation       Ask       Modify (0\0)         Window Messages       Ask       Modify (0\0)	Access Name	Action	Exclusions	^
Windows/WinEvent Hooks       Ask       Modify (0\0)         Processes' Termination       Ask       Modify (0\0)         Device Drivers' Installation       Ask       Modify (0\0)         Window Messages       Ask       Modify (0\0)	🖅 Run an executable	Ask	Modify (0\0)	
Image: Processes' Termination       Ask       Modify (0\0)         Image: Device Drivers' Installation       Ask       Modify (0\0)         Image: Window Messages       Ask       Modify (0\0)	Interprocess Memory Accesses	Ask	<u>Modify (0\0)</u>	
Image: Construction     Ask     Modify (0\0)       Image: Construction     Ask     Modify (0\0)       Image: Construction     Ask     Modify (0\0)	Windows/WinEvent Hooks	Ask	<u>Modify (0\0)</u>	
Window Messages     Ask     Modify (0\0)	Processes' Termination	Ask	Modify (0\0)	
	Device Drivers' Installation	Ask	Modify (0\0)	
	Window Messages	Ask	Modify (0\0)	

- Enter a name for the new ruleset.
- To copy the Access Rights and Protection Settings from an existing ruleset, click 'Copy From' and choose the ruleset from the drop-down.

COMODO Creating Trust Online\*

сом					?	×	
Name:	Rules for	Games			Copy fro	m 🔻	
ACCES	5 406405	PROTECTION SETTINGS			Rule	eset	Allowed Application Windows System Application
Access	: Name		Action	Enhniovs		h.	Contained Application Limited Application

- To customize the Access Rights and Protection Settings of this new rule set, follow the procedure explained under Use a Custom Ruleset in the section Active HIPS Rules.
- ? × COMODO Advanced Settings General Settings Rulesets šΞ Antivirus The following rulesets are defined on this computer: Firewall - HIPS **HIPS Settings** Q Ruleset Name **HIPS Rules** All Allowed Apps Rulesets Protected Objects Ruleset for Windows System Apps **HIPS Groups** Rules for Limited Applications Containment ✓ File Rating Advanced Protection CANCEL ОК
- Click 'OK' to save the new ruleset.

Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.

COMODO Creating Trust Online\*

соморо	COMODO HIPS Rule				×	
Name: C:\Progra	am Files (x86)\DrivignSpeed2\DrivingSpeed.exe			Bro	wse 🔻	
Ose Ruleset:			Allowe	d Applica	tion 🔻	
Use a Custom F	Ruleset			llowed App /indows Sy		ication
ACCESS ORDERS			Li	ontained A imited App uleset for 0	lication	
Access Name	Action	indusi	In	istaller or U	<del>pdater</del>	

### 6.4.4. HIPS Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups'
- HIPS groups are collections of one or more COM interfaces or registry keys.
- After defining a HIPS group, it will be available for selection and protection in the Registry Keys and COM Interfaces.
- CCS ships with predefined 'Registry' and 'COM' groups, and allows you to add new groups.
- You can view manage all groups in the 'HIPS Groups' interface.

### Open the 'HIPS Groups' interface

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left:

COMODO Creating Trust Online\*

COMODO Advance	ed Settings	?	-		×
COMODO Advance Seneral Settings Antivirus HIPS HIPS Settings HIPS Rules Rulesets Protected Objects HIPS Groups Seneral Settings Containment File Rating Advanced Protection	Add Edit   Registry Groups   Add   Edit   Registry Groups   Add   Edit   Registry Groups   Image:	?	-		Q
	□       □       Important Keys         □       □       Temporary Keys         □       □       Accounts Software		c	ANCEL	

• Please note, this area is just where you can view and define the groups. You need to select the group in the **Protected Objects** interface to actually apply the protections.

The panel has two sections:

- **Registry Groups** View, edit and create groups of registry keys which you want to protect from changes.
- COM Groups View, edit and create groups of COM interfaces which you want to protect from changes.

### 6.4.4.1. Registry Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups' > 'Registry Groups'
- Registry groups are predefined batches of one or more registry keys.
- Comodo Client Security ships with a set of important registry groups: 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.
- Creating a registry group allows you to quickly add it to the list of protected keys. See 'Protected Registry Keys' for help with this.

### To open the 'Registry Groups' section

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.
- Click the 'Registry Groups' tab:

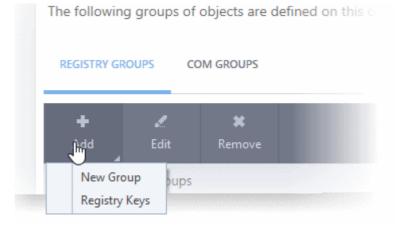
COMODO Creating Trust Online\*

COMODO Advance	ed Settings ? — $\Box$ ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>HIPS Settings</li> <li>HIPS Rules</li> </ul>	HIPS Groups The following groups of objects are defined on this computer: REGISTRY GROUPS COM GROUPS
Rulesets Protected Objects HIPS Groups Containment File Rating Advanced Protection	Add Edit Remove     Registry Groups       Automatic Startup     Automatic Startup     COMODO Keys     Comodo Keys     Important Explorer Keys     Important Keys     Important Keys     Accounts Software
	OK CANCEL

• Click the search icon on the right to find a specific item. You can enter a full or partial name.

This interface allows you to:

- Create a new Registry Group
- Add Registry key(s) to an existing group
- Edit the names of an Existing Registry Group
- Remove existing group(s) or individual key(s) from existing group
- To add a new group or add key(s) to an existing group, click the 'Add' button



Creating Trust Online\*

Add a new group - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.

COMODO Edit property		?	×
Choose Registry Group Name MediaGet			]
	ОК	CANCEL	

The group will be added to the list.

•

Add keys to a group - Select the group from the list, click 'the Add' button and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.

dd new item:	
<ul> <li>BCD00000000</li> <li>DRIVERS</li> <li>HARDWARE</li> <li>SAM         <ul> <li>SECURITY</li> <li>SOFTWARE</li> <li>COMODO</li> <li>Classes</li> <li>Clients</li> <li>ComodoGroup</li> <li>Dell</li> <li>Intel</li> <li>Macromedia</li> <li>FlashPlayer</li> <li>FlashPlayerActiveX</li> <li>Microsoft</li> <li>Mozilla</li> <li>OPDEC</li> </ul> </li> </ul>	HKLM\SOFTWARE\Macromedia\FlashPlaye.

- Select a key on the left then click the right arrow to add a new key to the group. You can add a key manually by typing its name in the 'Add new item' field then clicking the '+' button.
- To edit an existing group, select the group from the list and click the 'Edit' button.

Creating Trust Online\*

COMODO Edit property		?	×
Edit Registry Key MediaGet			
	ок	CANCEL	

- Modify the name of the group as required and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.

ed Settings	?	-	×
HIPS Groups			
The following groups of objects are defined on this con	nputer:		
REGISTRY GROUPS COM GROUPS			
+ X Add Edit Remove			
Registry Groups			Q
🔲 🗈 🖽 Automatic Startup			
🔲 🖆 🗄 Internet Explorer Keys			
🔲 🖆 🗄 Important Keys			
🗆 🗈 🗄 Temporary Keys			
🖂 🗈 🗄 MediaGet			

• To remove a key from a group, first expand the group by clicking its '+' symbol, select the key to be removed and click the 'Remove' button.

### 6.4.4.2. COM Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups' > 'COM Groups'
- COM groups are predefined collections of COM interfaces. COM interfaces are used by Windows to define

COMODO Creating Trust Online\*

how objects interact within a single application or between applications.

- COM is used as the basis for Active X and OLE two favorite targets of hackers and malicious programs to launch attacks. It is therefore essential that COM interfaces are protected.
- Comodo Client Security ships with the following, important COM groups: 'Internet Explorer/Windows Shell', 'Windows Management', 'Miscellaneous Classes', 'Pseudo COM Interfaces - Privileges' and 'Pseudo COM Interfaces - Important Ports'.
- Creating a COM group allows you to quickly add it to the 'COM' protection list. See 'Protected COM Interfaces' for more details.

#### To open the 'COM Groups' section

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.
- Click the 'COM Groups' tab:

COMODO Advance	ed Settings ? — 🗆 🗙
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>HIPS Settings</li> <li>HIPS Rules</li> </ul>	HIPS Groups         The following groups of objects are defined on this computer:         REGISTRY GROUPS         COM GROUPS
Rulesets Protected Objects	+ X X Add Edit Remove
HIPS Groups	COM Groups Q C Internet Explorer/Windows Shell
✓ File Rating	□
<ul> <li>Advanced Protection</li> </ul>	□       ⊡       ⊞ Miscellaneous Classes         □       ⊡       ⊞ Pseudo COM Interfaces - Privileges
	B Pseudo COM Interfaces - Important Ports      B Special COM Classes
	OK CANCEL

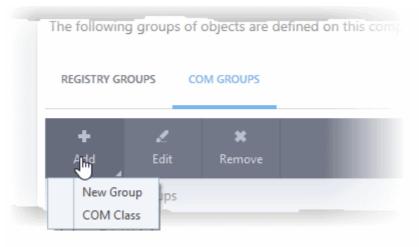
• Click the search icon on the right to find a specific item. You can enter full or partial names.

This interface allows you to:

- Create a new COM Group
- Add COM Component(s) to an existing group
- Edit the names of an Existing COM Group
- Remove existing group(s) or individual COM Component(s) from existing group

COMODO Creating Trust Online\*

• To add a new group or add new COM Component(s) to an existing group, click the 'Add' button



Add a new group - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.

COMODO Edit property		? ×
Add new COM Group Special COM Ports		
	ОК	CANCEL

The group will be added to the list.

 Add COM Components to a group - Select the group, click the 'Add' button and choose 'COM Class'. The 'Select COM Interface' dialog will be opened.

COMODO Creating Trust Online\*

d new item:		
AccClientDocMgr.AccClientDoc AccClientDocMgr.AccClientDoc AccDictionary.AccDictionary AccDictionary.AccDictionary.1 AccessControlEntry AccessControlList AccServerDocMgr.AccServerDoc AccServerDocMgr.AccServerDoc ADODB.Command ADODB.Connection ADODB.Connection ADODB.Connection ADODB.Error ADODB.Error ADODB.Error ADODB.ErrorLookup ADODB.ErrorLookup ADODB.Parameter ADODB.Parameter ADODB.Parameter.6.0	AccessControlList	

You can add new items by selecting them on the left and clicking the right arrow button. To add items manually, type their name in the 'Add new item' field and press the '+' button.

To edit an existing group, select the group from the list and click the 'Edit' button.

сомодо	Edit property		? ×	
Edit COM Group Special COM Ports				
		ок	CANCEL	
		ОК	CANCEL	

- Edit the name of the group in the 'Edit Property' dialog and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.

COMODO Creating Trust Online\*

Advanced S	ettings ? — 🗆 🗙
	HIPS Groups
	The following groups of objects are defined on this computer:
	REGISTRY GROUPS
	+ Add Edit Remove
je <b>cts</b>	
	Internet/Explorer/Windows Shell
	🔲 🗈 🗄 Windows Management
	E      Hiscellaneous Classes
	Pseudo COM Interfaces - Privileges
	Pseudo COM Interfaces - Important Ports
	🗆 🗈 🗄 Game Ports
1	🗹 🗈 🗄 Special COM Ports
	×
	OK CANCEL

• To remove an individual COM component from a group, click + at the left of the group to expand the group, select the item to be removed and click the 'Remove' button.

COMODO Creating Trust Online\*

### 6.5. Protected Objects

• The protected objects area lets you protect files, folders, registry keys and COM interfaces against access or modification by unauthorized processes.

There are two basic options you can choose:

•

- Read access only Processes can access but not modify the protected item
  - Click 'Advanced Settings' > 'HIPS' > 'Protected Objects'.
  - See 'Protected Objects HIPS' for more help
- Deny all Applications in the container cannot read or modify the protected item
  - Click 'Advanced Settings' > 'Containment' > 'Protected Objects'
  - · See 'Protected Objects Containment' for more help

### 6.5.1. Protected Objects - HIPS

- This area lets you protect specific files, folders, registry keys and COM interfaces against modification by unauthorized processes.
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'Protected Objects' on the left:

COMODO Advanced	Settings ? - D	×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Protected Objects The following groups of objects are defined on this computer: PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM INTERFACES	
HIPS Settings HIPS Rules	+ .≪ ¥ ↔ Add Edit Remove Purge	
Rulesets Protected Objects HIPS Groups	Path  Startup Folders  Important Files/Folders	2 ^
<ul> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Executables      Windows Management	
Auvanced Protection	B B 3rd Party Protocol Drivers      B Metro Apps	
	COMODO Client Files/Folders  Communication Client	
	OK CANCEL	• •

COMODO Creating Trust Online\*

The interface has the following sub-sections:

- Protected Files Applications and files which are protected from modification by other processes
- · Blocked Files Applications and files that are prevented from running
- Registry Keys Registry keys that are protected from modification by other processes
- COM Interfaces COM interfaces that are protected from modification

### 6.5.1.1. Protected Files

- The protected files screen shows file groups that are protected from access by other programs.
- Files in this area are 'read only'. They can be accessed and read by other programs, but not modified.
- This prevents malicious programs from hijacking important files. It is also useful for safeguarding valuable files (spreadsheets, databases, documents) against accidental or deliberate sabotage.
- A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Adding your host file to this area will allow web browsers to use the file as normal, but will block any attempt to modify it.
- You can create exceptions if you want to allow a trusted application to access a protected file. See
   Exceptions for more details about how to allow access to files placed in 'Protected Files'.

### Open the 'Protected Files' area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Protected Files' tab:

COMUDU

The follo	Protected Objects owing groups of objects are defined on this computer:
+ Add	Edit Remove Purge
	Path Q
	🗈 🗉 Startup Folders
	🗇 🗄 Important Files/Folders
	🖆 🗄 COMODO Client Files/Folders
	🗈 🗄 Executables
	🗈 🗄 Windows Management
	🗈 🗄 3rd Party Protocol Drivers
	OK CANCEL

The buttons at the top provide the following options:

- Add Select files/folders that you want to protect
- Edit Modify the path of the file or group
- **Remove** Delete the currently highlighted item
- **Purge** Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

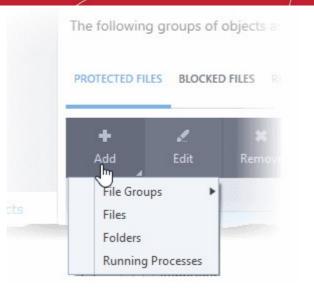
Click the search icon on the right to find a specific item. You can enter full or partial names.

#### Manually add protected items

You can protect individual files, folders, file groups or processes:

• Click the 'Add' button above the list:

COMODO Creating Trust Online\*



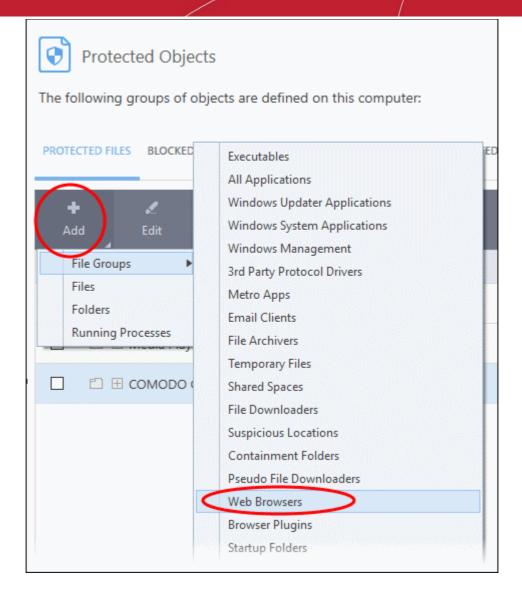
You can add items using any of the following methods:

- Select from File Groups
- Browse to a File
- Browse to a Folder
- Select from currently running processes

### Add a File Group

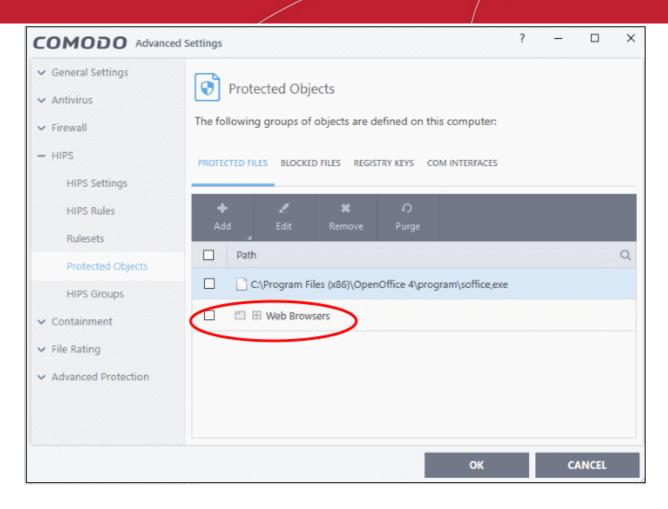
- Choosing 'File Groups' allows you to protect a category of pre-set files or folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, \*\cmd.exe, \*.bat, \*.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.
  - Background CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > 'File Groups'. You can also add your own file groups if required.
- · Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:

COMODO Creating Trust Online\*



The selected group will be added to the 'Protected Files' list:

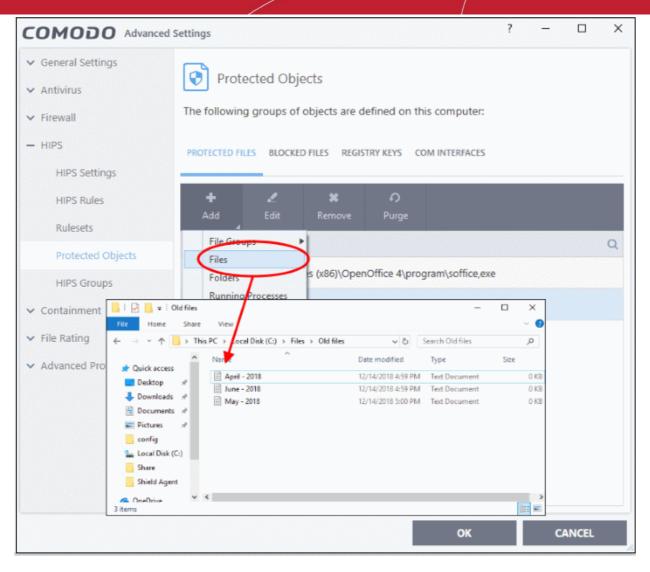
COMODO Creating Trust Online\*



### Add an individual file

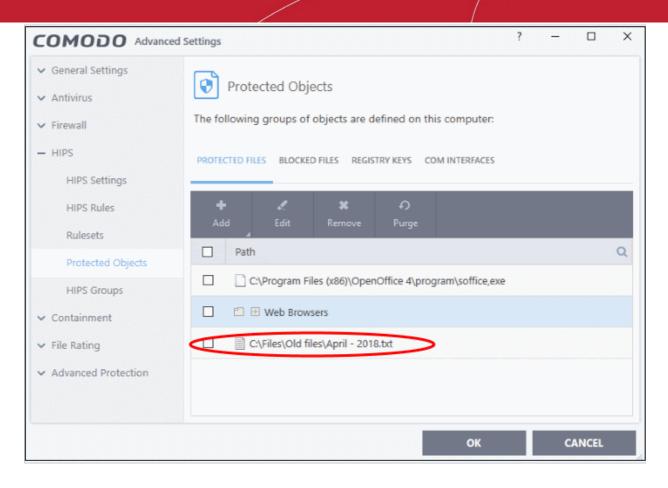
• Click 'Add' and choose 'Files' from the options:

COMODO Creating Trust Online\*



• Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open' The file will be added to 'Protected Files'.

COMODO Creating Trust Online\*



### Add a Drive Partition/Folder

• Click 'Folders' from the 'Add' drop-down.

COMODO Creating Trust Online

PROTECTED FILES BLOCKED FILES	REGISTRY KEY
🕂 🦨 🛃	🗙 🥻 move Pu
File Groups	
	olders
Runn Processee	
browse For Folder	×
Browse For Folder	>
browse For Folder	>
	> 
🗸 🏪 Local Disk (C:)	>
✓ 🏪 Local Disk (C:) → 📴 24x7	^
✓ 🏪 Local Disk (C:) > 24x7 CIS Setup	^
✓ 🏪 Local Disk (C:) > 24x7 CIS Setup ✓ did man files	^
✓ <sup>*</sup> Local Disk (C:) > 24x7 CIS Setup ✓ old man files ■ Bank States	^
<ul> <li>Local Disk (C:)</li> <li>24x7</li> <li>CIS Setup</li> <li>old man files</li> <li>Bank Stater</li> <li>PerfLogs</li> </ul>	^
<ul> <li>Local Disk (C:)</li> <li>24x7</li> <li>CIS Setup</li> <li>old man files</li> <li>Bank Stater</li> <li>PerfLogs</li> <li>Program Files</li> </ul>	ments
<ul> <li>Local Disk (C:)</li> <li>24x7</li> <li>CIS Setup</li> <li>old man files</li> <li>Bank Stater</li> <li>PerfLogs</li> <li>Program Files</li> <li>Program Files</li> </ul>	ments (x86)
<ul> <li>Local Disk (C:)</li> <li>24x7</li> <li>CIS Setup</li> <li>old man files</li> <li>Bank Stater</li> <li>PerfLogs</li> <li>Program Files</li> </ul>	ments (x86)
<ul> <li>Local Disk (C:)</li> <li>24x7</li> <li>CIS Setup</li> <li>old man files</li> <li>Bank Stater</li> <li>PerfLogs</li> <li>Program Files</li> <li>Program Files</li> </ul>	ments (x86)

The 'Browse for Folder' dialog will appear.

• Select the folder/drive and click 'OK'. Repeat the process to add more items.

### Add an application from a running process

- Choose 'Running Processes' from the 'Add' drop-down
- This will open a list of processes that are currently running on your computer:

COMODO Creating Trust Online

PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM INT		
+ 🖍 🗱 ᡝ Add Edit Remove Purge		
Files Folders		
Running Profinesses	?	>
Application	PID	
4 🚳 mspaint.exe	7572	^
🖌 🖶 MSASCuiL.exe	1404	
schedhlp.exe	6364	
🖌 🝊 OneDrive.exe	6224	
	8304	
🖌 🕥 openvpn-gui.exe		
<ul> <li>Periode Antiparties</li> <li>Periode Antiparties&lt;</li></ul>	7532	
	7532 8220	
4 🔮 firefox.exe		
<ul> <li>▲ ● firefox.exe</li> <li>▲ ● DAP.exe</li> </ul>	8220	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> </ul>	8220 560	
<ul> <li>▲ ● firefox.exe</li> <li>▲ ● DAP.exe</li> <li>▲ ■ csrss.exe</li> <li>▼ ■ winlogon.exe</li> </ul>	8220 560 624	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> <li>winlogon.exe</li> <li>fontdrvhost.exe</li> <li>fontdrvhost.exe</li> <li>dwm.exe</li> <li>Maxthon.exe</li> </ul>	8220 560 624 760	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> <li>winlogon.exe</li> <li>fontdrvhost.exe</li> <li>dwm.exe</li> </ul>	8220 560 624 760 968	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> <li>i csrss.exe</li> <li>i ontdrvhost.exe</li> <li>i fontdrvhost.exe</li> <li>i dwm.exe</li> <li>Maxthon.exe</li> </ul>	8220 560 624 760 968 2896	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> <li>csrss.exe</li> <li>fontdrvhost.exe</li> <li>fontdrvhost.exe</li> <li>dwm.exe</li> <li>dwm.exe</li> <li>Maxthon.exe</li> <li>erl.exe</li> </ul>	8220 560 624 760 968 2896 4132	
<ul> <li>firefox.exe</li> <li>DAP.exe</li> <li>csrss.exe</li> <li>winlogon.exe</li> <li>fontdrvhost.exe</li> <li>fontdrvhost.exe</li> <li>dwm.exe</li> <li>dwm.exe</li> <li>m Maxthon.exe</li> <li>erl.exe</li> <li>inet_gethost.exe</li> </ul>	8220 560 624 760 968 2896 4132 4260	

- Select the process you want to protect
- Click 'OK'

The parent application will be added to the 'Protected Files' list:

COMODO Creating Trust Online\*

COMODO Advanced	Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Protected Objects The following groups of objects are defined on this computer:				
- HIPS HIPS Settings HIPS Rules	PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM INTERFACES	PROTEC	CTED DAT		
Rulesets Protected Objects HIPS Groups	Path C\Program Files (x86)\OpenOffice 4\program\soffice,ex	e			Q
<ul> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	<ul> <li>Web Browsers</li> <li>C:\Files\Old files\April - 2018.txt</li> <li>C:\Program Files (x86)\Mozilla Firefox\firefox.exe</li> </ul>		>		
	ок		C/	NCEL	

 Repeat the process to add more files. The items added to the 'Protected Files' will be protected from access by other programs.

### To edit an item in the Protected Files list

• Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit property	?	×
Edit File Path C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe		
ОК	CANCEL	

• Edit the file path, if you have relocated the file and click 'OK'

#### To delete an item from Protected Files list

• Select the item from the list and click the 'Remove' button

The selected item will be deleted from the protected files list. CCS will not generate alerts, if the file or program is subjected to unauthorized access.

COMODO Creating Trust Online\*

### **Exceptions**

Users can selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in 'Active HIPS Rules' interface.

A simple example would be the imaginary file 'April - 2018.odt'. You would want the 'Open Office Writer' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potentially malicious program. You would first **add** the document to the 'Protected Files' area. Once added to 'Protected Files', you would go into 'Active HIPS Rules' and create an exception for 'swriter.exe' so that it alone could modify 'June - 2016.odt'.

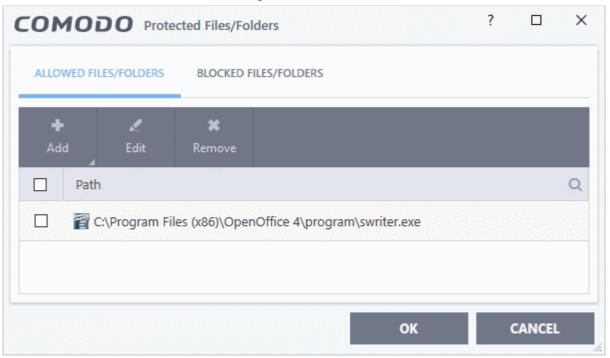
- First add 'April 2017.odt' to 'Protected Files'
- Then go to the 'HIPS Rules' interface and add it to the list of applications.
- Click the 'Edit' button after selecting it.
- In the 'HIPS Rule' interface, select 'Use a Custom Ruleset'.

COMODO Advanced	Settings				?	-		×
General Settings     Antivirus	HIPS Rule	s						
✓ Firewall	The following HIPS	rules are active on	this computer:					
— HIPS HIPS Settings	+ Add Ed		t Move Up Mo	I we Down	ව Purge			
HIPS Rules	Applicatio	1		Q Tre	at as			Q
Rulesets	C:\old	nane files\Fedaral Ba	nk Statements\Ap	oril Allo	wed Appl	lication		
Protected Objects	📄 🕘 C:\Pro	ram Files\Mozilla Fire	efox\firefox.exe	Cus	tom rules	et		
сомодо на	PS Rule			?		×		
Name: C:\old mane f	iles\Fedaral Bank S	Statements\April-	2017.odt		Brow	se 🔻		
O Use Ruleset:				Allowed A	pplicatio	on 🔻		
Ose a Custom Rules	set			(	Copy fro	m 🔻		
ACCESS RIGHTS PR	OTECTION SETTINGS							
Access Name		Action	Exclusio	ons		*		
Window messages	;	Ask	Modify	(0\0)				
Protected COM int	terfaces	Ask	Modify	(0\0)				
• Protected registry	keys	Ask	<u>Modify</u>	(0\0)				
Protected files/fold	ders	Ask	Modify	(0\0)				
DNS client service		Ask				-		
			ОК					
							8	

 Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'. The 'Protected Files/Folders' interface will appear.

Creating Trust Online\*

Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add swriter.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32\\* to the 'Protected Files area (\* = all files in this directory). Next go to 'HIPS Rules', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

### 6.5.1.2. Blocked Files

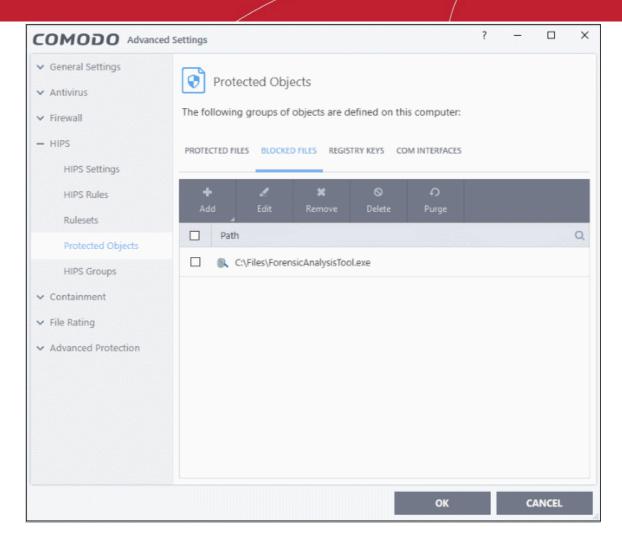
•

- CCS allows you to lock-down files and folders by denying all access rights to them from other processes or users effectively cutting them off from the rest of your system.
- If the file you block is an executable, then neither you nor anything else is able to run that program.
- Unlike files in 'Protected Files', users cannot selectively allow access to a blocked file.

#### Open the blocked files section

- Click 'Settings' on the CCS home screen.
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Blocked Files' tab:

COMODO Creating Trust Online\*



The buttons at the top provide the following options:

- Add Select files/folders that you want to block
- Edit Modify the path of the file or group
- Remove Releases the currently highlighted file from the blocked files list.
- Delete Deletes the highlighted file from your computer
- **Purge** Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

### Manually add an item to the block list

• Click the 'Add' button:

PROTECTED FI	LES BLOCKE	D FILES REGI	STRY KEYS CO	MINT
+ Add	🗶 Edit	🗱 Remove	<b>O</b> Delete	P
	g Processes		te\CPILSuite.ex	

COMODO Creating Trust Online\*

You can add the files by following methods:

- Select a file
- Select a currently running process

### Add a File

- Choose 'Applications' from the 'Add' drop-down.
- Navigate to the file you want to add and click 'Open'.

Open × Look in: ∎ regtest ✓ ⓒ ♪ ▷ Ⅲ ✓ Name ^ Date modified Type ■ regsrvgs 11/10/2016 11:00 Applicati ↓ regtest 11/10/2016 11:00 Applicati	Add Edit Remove Delete Purge	Add Edit Remove Delete Purge     Applications   Bunnink-Processor   C:\Suspicious Files\cpil_suite\CPILSuite.exe     Copen     Look in:   regtest   Quick access   Determodified   Type   Interpretein   Pesktop     Image: State of the state
Applications Runnin-Proces Open C(SUSPICIOUS Files\cpi]_suite\CPILSuite.exe Open Look in: Reget Runnin-Proces Runn	Applications Running Processor CC\Suspicious Files\cpil_suite\CPILSuite.exe CC\Suspicious Files\cpil_suite\CPILSuite.exe Copen Look in: regrest Name Date modified Type Regress Cuick access Determodified Type Regress Pregrest Pregre	Applications Runnin-Process CC\Suspicious Files\cpil_suite\CPILSuite.exe Copen Look in: regtest Quick access Destrop Destrop Runnin-Process Runnin-Pr
Running Process       Files\cpil_suite\CPILSuite.exe         Open       ×         Look in:       regtest       ✓       Image: Second	Bunning Processor         C:\Suspicious Files\cpil_suite\CPILSuite.exe         Copen         Look in:       regtest         Name       Date modified       Type         Quick access       Intropy of the second se	Bunning Processor         C:\Suspicious Files\cpil_suite\CPILSuite.exe         Copen         Look in:       regtest         Name       Date modified       Type         Quick access       Intropy regtest       11/10/2016 11:00       Applicat         Desktop       regtest       11/10/2016 11:00       Text Doc
Open       ×         Look in:       Image to the second sec	C:\Suspicious Files\cpil_suite\CPILSuite.exe Copen   Look in:  regtest  Rame  Dete modified  Type  regsrvgs  11/10/2016 11:00  Applicati regtest  11/10/2016 11:00  Applicati regtest  11/10/2016 11:00  Text Doc	C:\Suspicious Files\cpil_suite\CPILSuite.exe C:\Suspicious Files\cpil_suite\CPILSuite.exe Cook in:
Open × Look in: ☐ regtest ✓ ⓒ ♪ ▷ □ ✓ Name	☑ Open       >         Look in:       Imagest       >         ☑ nogtest       >       Imagest       >         ☑ nogtest       >       Imagest       >         ☑ nogtest       >       Imagest       Imagest       >         ☑ nogtest       Imagest       Imagest       Imagest       >         ☑ nogtest       Imagest       Imagest       Imagest       Application         Imagest       Imagest       Imagest       Imagest       Imagest       Application         Imagest	Copen >> Look in: regtest → Control of the second
✓ Open       ×         Look in:       regtest       ✓       ③       ●       □         ✓       ●       ●       ●       ●       ●       ●         ✓       ●	Image: Copen       >         Look in:       Image: regtest       >         Quick access       Name       ^       Date modified       Type         Quick access       11/10/2016 11:00       Applicati         Image: Personal control of the second contrelevee contro	Copen Look in: regtest Quick access Desktop Copen Name Date modified Type Type 11/10/2016 11:00 Applicat 11/10/2016 11:00 Applicat 11/10/2016 11:00 Text Door Text Door Tex
✓ Open       ×         Look in:       regtest       ✓       ③       ●       □         ✓       ● </td <td>Image: Copen       &gt;         Look in:       Image: regtest       &gt;         Quick access       Name       ^       Date modified       Type         Quick access       11/10/2016 11:00       Applicati         Image: Personal control of the second contrelevee contro</td> <td>Copen Look in: regtest Quick access Desktop Copen Name Date modified Type Type 11/10/2016 11:00 Applicat 11/10/2016 11:00 Applicat 11/10/2016 11:00 Text Door Text Door Tex</td>	Image: Copen       >         Look in:       Image: regtest       >         Quick access       Name       ^       Date modified       Type         Quick access       11/10/2016 11:00       Applicati         Image: Personal control of the second contrelevee contro	Copen Look in: regtest Quick access Desktop Copen Name Date modified Type Type 11/10/2016 11:00 Applicat 11/10/2016 11:00 Applicat 11/10/2016 11:00 Text Door Text Door Tex
Look in: regtest Name Name Date modified Type Type 11/10/2016 11:00 Applicati regtest 11/10/2016 11:00 Applicati Type 11/10/2016 11:00 Applicati Type 11/10/2016 11:00 Text Doct	Look in: regtest Quick access Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtest Name Desktop Cook in: regtest Desktop Cook in: regtest Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtestest Cook in: regtestestestestestestestestestes	Look in: regtest Quick access Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtest Name Date modified Date modified Type
Look in: regtest Name Name Date modified Type Type 11/10/2016 11:00 Applicati regtest 11/10/2016 11:00 Applicati Type 11/10/2016 11:00 Applicati Type 11/10/2016 11:00 Text Doct	Look in: regtest Quick access Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtest Name Desktop Cook in: regtest Desktop Cook in: regtest Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtestest Cook in: regtestestestestestestestestestes	Look in: regtest Quick access Desktop Cook in: regtest Desktop Cook in: regtest Cook in: regtest Name Date modified Date modified Type
Name     Date modified     Type       Image: state	Name     Date modified     Type       Quick access     II/10/2016 11:00     Applicati       Image: Desktop     II/10/2016 11:00     Text Doc	Name     Date modified     Type       Quick access     III/10/2016 11:00     Applicat       Image: Desktop     III/10/2016 11:00     Text Doc
Image: spin regsrvgs         11/10/2016 11:00         Applicati           uick access         Image: spin regsrvgs         11/10/2016 11:00         Applicati           Image: spin regsrvgs         Image: spin regsrvgs         11/10/2016 11:00         Applicati           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs	Quick access Quick access Quick access Desktop	Quick access Quick access Quick access Desktop
Image: spin regsrvgs         11/10/2016 11:00         Applicati           uick access         Image: spin regsrvgs         11/10/2016 11:00         Applicati           Image: spin regsrvgs         Image: spin regsrvgs         11/10/2016 11:00         Applicati           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs         Image: spin regsrvgs           Image: spin regsrvgs	Quick access Quick access Desktop	Quick access Quick access Quick access Desktop
uick access Pregtest 11/10/2016 11:00 Applicati	Quick access Tregtest 11/10/2016 11:00 Applicati	Quick access Pregtest 11/10/2016 11:00 Applicat
regtest 11/10/2016 11:00 Text Doct	Pregtest 11/10/2016 11:00 Application	Desktop
in regress in the book in the book	Desktop	Desktop
Desktop		
e estade ( )		
	Libraries	Libraries
	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·		
libraries	승규는 것은 것은 것이 같아요. 이 것은 것은 것이 같아요. 이 것이 ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?	
Libraries		
Libraries	철 위독 학생님께서 이번 것이 있는 것이 같이 있는 것이 없다.	
		This PC
Libraries Dis PC	This PC	This PC
	This PC	This PC
	Charles Contract Contra	L'ANDRES .
	Libraries	Libraries
·	Libraries	Libraries
Libraries		
Libraries		
Libraries	2011년 1월 1991년 1월 19	
Libraries		North State
Libraries		
Libraries		(2) - 20 · 20 · 20 · 20 · 20 · 20 · 20 · 20
Libraries	방향은 것 같은 것	
Constant Sector		and the second
Libraries		
Libraties		
Libraries		Status 💼 status
Libraries		
	Contraction of the second se	standica
	Contraction of the second se	standics
	Libraries	Lioraries
	Libraries	Libraries
	Libraries	Libraries
	Libraries	Libraries
1 📻 실황 · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· 그 사용. · · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· 그 사용. · · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
· - 신송	Libraries	Libraries
1 📻 실황	Libraries	Libraries
1 📻 실황 · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
1 📻 실황 · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
1 📻 실황 · · · · · · · · · · · · · · · · · ·	Libraries	Libraries
	Libraries	Libraries
	Libraries	Libraries
	Libraries	Libraries

The file will be added to 'Blocked Files' list.

COMODO Creating Trust Online\*

COMODO Advanced	Settings					?	-		×
✓ General Settings									
✓ Antivirus	Protec	cted Obje	ects						
✓ Firewall	The following	groups of	objects are d	lefined on th	is computer:				
- HIPS	PROTECTED FILE	S BLOCKE	D FILES REGIS	STRY KEYS CO	M INTERFACES				
HIPS Settings									_
HIPS Rules	+	2	×	0	ę				
Rulesets	Add	Edit	Remove	Delete	Purge				
Protected Objects	Path								Q
HIPS Groups	🔲 🦉 D:	Suspicious	files\Master_	Of_The_Voice	CRACKED-ARG	GENTINA	-CRACK	1.exe	
✓ Containment	💿 🚺 ୯	\Suspiciou	is Files\regte	est\regtest.e	xe				
✓ File Rating									
✓ Advanced Protection									

• Repeat the process to add more files.

### Add a running process

· Choose 'Running Processes' from the 'Add' drop-down

This will open a list of processes that are currently running on your computer:

- Select the process you want to protect
- Click 'OK'

COMODO Creating Trust Online

PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM INT	ERFACES	
	<b>O</b> urge	
Applications Running Processes		0
COMODO Browse for Processes		? X
Application	PID	
▲ 📧 svchost.exe	4504	^
▼ 📊 explorer.exe	2528	
🔻 🥮 firefox.exe	3124	
Image: plugin-container.exe	3680	
A S DrivingSpeed.exe	2540	
▲ 🗯 jumper.exe	2176	
4 🚳 vkise.exe	1108	
💌 🛄 System	4	
A 💽 smss.exe	288	
4 💽 csrss.exe	448	
👻 🖭 winlogon.exe	484	
4 💽 fontdrvhost.exe	4492	
4 📧 dwm.exe	732	
4 💽 csrss.exe	380	
4 📧 sychost.exe	964	
🔺 🕘 notepad.exe	1440	
4 🦀 OneDrive.exe	4744	~

The parent application will be added to the 'Protected Files' list:

COMODO

COMODO Advanced	Settings					?	-		×
✓ General Settings									
✓ Antivirus	Pro Pro	tected Obje	ects						
✓ Firewall	The followi	ng groups of	objects are d	efined on this	s computer:				
- HIPS	PROTECTED	FILES BLOCKED	FILES REGIS	TRY KEYS CO	M INTERFACES				
HIPS Settings									_
HIPS Rules	+		×	0	Ð				
Rulesets	Add	Edit 4	Remove	Delete	Purge				
Protected Objects	Pa	th							Q
HIPS Groups	E 🦉	D:\Suspicious	files\Master_0	Of_The_Voice-	CRACKED-ARG	ENTINA	-CRACK	1.exe	
✓ Containment		D:\Suspicious	files\ProAgen	t.exe					
✓ File Rating	*	C:\Suspiciou	s Files\Jump	er\Jumper\ji	umper.exe		>		
✓ Advanced Protection									
Website Filtering	1								

• Repeat the process to add more files.

To edit an item in the Blocked Files list

• Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit property		?	×
Edit File Path C:\Suspicious Files\Jumper\Jumper\jump	er.exe		
	ОК	CANCEL	

• Edit the file path, if you have relocated the file and click 'OK'

#### To release an item from Blocked Files list

Select the item from the list and click the 'Remove' button

The selected item will be removed from the 'Blocked Files' list. CCS will not block the application or file from execution or opening then onwards.

### To permanently delete a blocked file from your system

• Select the item from the list and click the 'Delete' button

The selected item will be deleted from your computer immediately.

**Warning**: Deleting a file from from the 'Blocked Files' interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

### 6.5.1.3. Protected Registry Keys

The 'Registry Keys' area lets you define system critical registry keys which should protected against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified.

### Open the 'Registry Keys' section

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Registry Keys' tab:

COMODO Advanced	Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Protected Objects The following groups of objects are defined on this computer:				
<ul> <li>HIPS</li> <li>HIPS Settings</li> <li>HIPS Rules</li> </ul>	PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM INTERFACES				
Rulesets Protected Objects HIPS Groups Containment File Rating Advanced Protection	Keys    COMODO Keys    HKCR\*   Automatic Startup				Q
	ОК		C/	NCEL	

The buttons at the top provide the following options:

- · Add Select registry groups or individual keys that you want to protect
- Edit Modify the path of the key or key group
- Remove Delete the currently highlighted item
- Click the magnifying glass on the right to search for a specific item.

#### Manually add individual keys or registry groups

Click the 'Add' button

You can add keys individually or by registry group:

 Add Registry Groups - Adding a registry group allows you to batch select and import groups of important registry keys. Comodo Client Security provides the following, pre-defined groups - 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

You can also create custom registry groups containing keys you wish to protect.

 To add a new group, click the 'Add' button > 'Registry Groups' and select the predefined group from the list and click 'OK'

COMODO Creating Trust Online\*

Prote	ected Obje	ects				
The followin	g groups of	objects are de	fined on	this comput	er:	
PROTECTED FI	LES BLOCKEI	D FILES REGIST	RY KEYS	COM INTERFAC	CES	
+ Add	🖌 Edit	XX Remove				
Registry	Groups 🕨	Automatic	artup			Q
Registry	Entries	COMODO Internet Explo Important Ke Temporary K	orer Keys ys			

See Registry Groups in the HIPS Groups section if you want to read more on this interface.

- Add individual Registry Keys -
  - Click the 'Add' button and then select 'Registry Entries'
  - · Choose a key on the left then click the right arrow to add it to the protected list:

dd new item:	
<ul> <li>HKEY_CLASSES_ROOT</li> <li>HKEY_CURRENT_USER</li> <li>HKEY_LOCAL_MACHINE</li> <li>BCD0000000</li> <li>HARDWARE</li> <li>SAM SECURITY</li> <li>SOFTWARE</li> <li>COMODO</li> <li>CA</li> <li>CIS Cam Data</li> <li>DbgTrace</li> <li>Installer</li> <li>Options VolatileData</li> <li>Classes</li> </ul>	HKLM\SOFTWARE\COMODO\CIS\*

COMODO Creating Trust Online\*

• Alternatively, you can type the key name in the field at the top then click '+'.

### Edit an item in the Registry Protection list

• Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit property		? ×
Edit File Path HKLM\SOFTWARE\COMODO\CIS\*		
	ок	CANCEL

· Edit the key path, if you have relocated the key and click 'OK'.

**Note**: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

### To delete an item from Registry Protection list

• Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the 'Registry Keys' protection list. CCS will not generate alerts, if the key or the group is modified by other programs.

### 6.5.1.4. Protected COM interfaces

- The Component Object Model (COM) is Microsoft's object-oriented programming model. It defines how
  objects interact within a single application, or between applications.
- COM is used as the basis for Active X and OLE two favorite targets of hackers and malware for launching attacks on your computer.
- Comodo Client Security automatically protects COM interfaces against modification and manipulation by malicious processes.
- 'Protected Objects' > 'COM Interfaces' lets you view, add and edit these protected interfaces.
  - Background CCS ships with a set of COM groups category based collections of COM interface components.
  - Click 'Settings' > 'HIPS Groups' > 'COM Groups' if you want to view these groups. You can create
    custom groups if required. See COM Groups for the help page on this area.

#### Open the protected COM interfaces area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'COM Interfaces' tab:

COMODO

COMODO Advance	d Settings	?	_		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Protected Objects The following groups of objects are defined on this computer PROTECTED FILES BLOCKED FILES REGISTRY KEYS COM	INTERFACES			
HIPS Settings HIPS Rules Rulesets	+ 2 X Add Edit Remove				Q
Protected Objects HIPS Groups Containment File Rating Advanced Protection	<ul> <li>Internet Explorer/Windows Shell</li> <li>Windows Management</li> <li>Besudo COM Interfaces - Privileges</li> <li>Besudo COM Interfaces - Important Ports</li> </ul>				
Advanced Protection	E E Miscellaneous Classes				
	ОК		c	ANCEL	

The buttons at the top provide the following options:

- Add Select COM groups or individual components that you want to protect
- Edit Edit the COM Class.
- Remove Deletes the currently highlighted COM group or COM component.

You can search for a specific interface by clicking the magnifying glass icon at the far right of the column header.

### Manually add a COM group or individual component

Click the 'Add' button

You can add items as follows:

•

- Add COM Groups Batch select and import predefined groups of important COM components.
  - Click 'Add' > 'COM Groups'
  - Select the group you want to add
  - Click 'OK'

COMODO Creating Trust Online\*

ed Settings				?	-	×
Prot	ected Obje	ects				
The followir	ng groups of o	objects are d	lefined on this computer:			
PROTECTED F	ILES BLOCKED	FILES REGIS	STRY KEYS COM INTERFACES			
		~				
	• Edit	Remove				
Add						
Add COM G	roups 🕨	Internet	Explorer/Windows Shell			Q
COM G	omponents		Explorer/Windows Shell s Management			Q
COM G		Windows				Q
COM G	omponents	Window: Miscellar	Management			Q
COM G	omponents	Windows Miscellar Pseudo C	Management neous Classes			Q

For explanations on editing existing 'COM Groups' and creating new groups, see COM Groups.

- Add individual components
  - Click the 'Add' button then 'COM Components'.
  - Select a component on the left
  - Click the right arrow to add it to the protected list:

Creating Trust Online\*

dd new item:			 
AccClientDocMgr.AccClientDoc AccClientDocMgr.AccClientDoc AccDictionary.AccDictionary AccDictionary.AccDictionary.1 AccessControlEntry AccessControlList AccServerDocMgr.AccServerDoc AccServerDocMgr.AccServerDoc ADODB.Command ADODB.Command ADODB.Connection ADODB.Connection ADODB.Connection.6.0 ADODB.Error ADODB.Error ADODB.ErrorLookup ADODB.ErrorLookup ADODB.Parameter ADODB.Parameter.6.0		AccessControlList	

Click 'OK' to add the items to the list

Edit an item in the COM Interfaces protection list

• Select the COM component from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit pro	perty		?	×
Edit File Path AccessControlList				
		ОК	CANCEL	

• Edit the COM Class file path and click 'OK'

**Note**: The COM Groups cannot be edited from this interface. You can edit only from **COM Groups** in **HIPS Groups** section.

#### To delete an item from COM Interfaces protection list

• Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the 'COM Interfaces' protection list. CCS will not generate alerts, if the COM component or the group is modified by other programs or processes.

COMODO Creating Trust Online\*

### 6.5.2. Protected Objects - Containment

- Click 'Settings' > 'Containment' > 'Protected Objects'
- Items that you add to this area cannot be read or modified by applications running in the container.
- Examples items you can add are files, folders and registry keys.
- This prevents unknown/untrusted applications from causing damage to, or stealing data from, important items

settings		?	-	٥	×
The followi	wing objects are protected from applications running in the container:				
РПОТЕСТЕС	TED DATA PROTECTED KEYS				
+ Add	e at Edit Remove				
Par	Path			٩	^
	— 11/1/1/2017/AppDetat_coahPackagen/Microsoft/Microsoft/Lidge_Iweekyb3dibblever/AC/Microsoft/Lidge_"\Defaulty"				
	- 📄 ?h(Users),"\AppData\Roaming\Opera\Opera\"				
	- 📄 Müsero, "AppDate/Ibarring/Opera Software/Opera Stable				
	- 🗋 %Users/;"AppDats/Local/Apple Computer/"				
	- 📄 Müsers("AppData)toamingApple Computer(Safari);"				
	- 🔝 1\(Users"\AppDats\Roaming\(Maxthon3"				
	- 📄 ?\(Usero\"\AppData).Locah/Comodo).Dragon\"				1
	- 📄 1\Users\"\AppDatn\.oca\/Comodo\iceDragon\"				
	- 🗋 ?klusers("UppData)Roaming(Comodol)"				1
	- 🗋 TAUsers\"AppData(Local)Chromium\"				
	- 📄 ?:\Users\"\AppData\Local\Comodo\Chromodo\"				1
	TAUsens\"/AppData/Roaming\Thunderbird\Profiles\"				
					¥
	ox		CA	NCEL	
		Protected Objects         The following objects are protected from applications running in the container:         PROTECTED DATA         MOTECTED DATA         PROT         Cold         Renova         Path         -	Protected Objects   The following objects are protected from applications running in the container:  PROTECTED DATA    PROTECTED DATA     Protected Objects   Protected DATA     Protected DATA      Protected DATA    Protected DATA     Protected DATA    Protected DATA       Protected DATA     Protected DATA      Protected DATA         Protected DATA     Protected DATA         Protected DATA        Protected DATA        Protected DATA             Protected DATA            Protected DATA   Protected DATA                      Protected DATA          Protected DATA        Protected DATA        Protected DATA <td>Protected Objects         The following objects are protected from applications running in the container:         Protected OM       MOTECTED KKS         Image: Control of the container:         Image: Control of the container:</td> <td>Protected Objects         The following objects are protected from applications running in the container:         MOTECTED DATA       MOTECTED Strp         Add       Edd         Reth       C         Cdd       Renove         Path       C         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.Microsoft.Microsoft.dige. Basekyb3dtbbese/AC/Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backings/Opera State/*         -       -         -       TAUSers/"VepEData/Backings/Comodo/Chrosoft         -       -         -       TAUSers/"VepEData/Backings/Comodo/Chrosoft         -       -         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSe</td>	Protected Objects         The following objects are protected from applications running in the container:         Protected OM       MOTECTED KKS         Image: Control of the container:         Image: Control of the container:	Protected Objects         The following objects are protected from applications running in the container:         MOTECTED DATA       MOTECTED Strp         Add       Edd         Reth       C         Cdd       Renove         Path       C         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.Microsoft.Microsoft.dige. Basekyb3dtbbese/AC/Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backages/Microsoft.dige."/Default,"         -       -         -       TAUSers/"VepEData/Data/Backings/Opera State/*         -       -         -       TAUSers/"VepEData/Backings/Comodo/Chrosoft         -       -         -       TAUSers/"VepEData/Backings/Comodo/Chrosoft         -       -         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSers/"VepEData/Backing/Comodo/         -       TAUSe

Click the following links for more details:

- Protected Files and Folders
- Protected Keys

### 6.5.2.1. Protected Files and Folders

- Click 'Settings' > 'Containment' > 'Protected Objects' > 'Protected Data'
- Items in 'Protected Data' cannot be seen, accessed or modified by applications running in the container.
- This fortifies files containing sensitive data from unrecognized and potentially malicious programs.

### Protected Files versus Protected Data

- Items in 'Protected Files' ('Settings' > 'HIPS' > 'Protected Objects' > 'Protected Files') can be read by any
  program, but not modified by them. This contrasts to items in 'Protected Data', which are totally hidden to
  contained programs.
  - If you want a file/folder to be read by other programs, but protected from modification, then add it to 'Protected Files' list.
  - If you want to totally conceal an item from contained programs, but allow read/write access to trusted programs, then add it to 'Protected Data'.
  - You can add the same item to both areas. This means trusted programs have read-only access to the file, and contained programs have no access rights.

COMODO Creating Trust Online\*

### Add and manage protected data

- Click 'Settings' on the CCS home screen.
- Click 'Containment' > 'Protected Objects'
- Select the 'Protected Data' tab

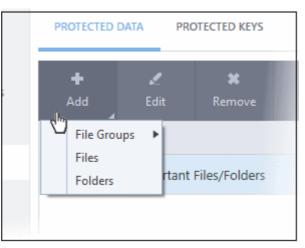
COMODO Advanced	Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Protected Objects The following objects are protected from applications run PROTECTED DATA PROTECTED KEYS	ning ir	n the co	ntainer:	
<ul> <li>Containment</li> <li>Containment Settings</li> <li>Auto-Containment</li> </ul>	+     *       Add     Edit       Remove				Q
Protected Objects	🗌 🗈 🗄 Open Office				
Virtual Desktop <ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Important Files/Folders				
	ОК		C/	ANCEL	

The buttons at the top provide the following options:

- Add Select files/folders that you want to protect
- Edit Modify the path of the file or group.
- Remove Delete the currently highlighted item
- · Click the search icon at the far right to search for a specific item

#### Manually add a file, folder or file group

• Click the 'Add' button



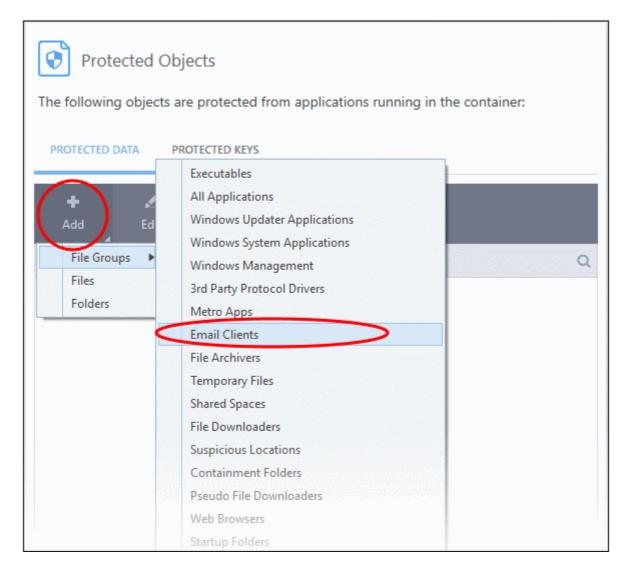
You can add items using any of the following methods:

COMODO Creating Trust Online\*

- Select from File Groups
- Browse to a File
- Browse to a Folder

#### Add a File Group

- · Choose 'File Groups' from the 'Add' drop-down and select a file group
- CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > 'File Groups'. You can also add your own file groups if required.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, \*\cmd.exe, \*.bat, \*.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.



The selected group will be added to the 'Protected Files' list:

#### Add an Individual File

Click 'Add' and choose 'Files' from the options:

COMODO Creating Trust Online\*

GOMO	Advanced Se	ttings			? – 🗆
<ul> <li>General Settin</li> <li>Antivirus</li> </ul>	ıgs	Protected Object	S		
<ul> <li>Firewall</li> </ul>		The following objects are p	rotected from applicat	tions running i	in the container:
HIPS		PROTECTED DATA PROTEC	CTED KEYS		
- Containment					
Containme	nt Settings	🕇 🏒 Add Edit	<b>X</b> Remove		
Auto-Conta	ainment	File Groups			
Protected (	Objects	Files Folders Clients			
Virtual Des	-			×	
	-	~	G 🦻 📂 ⊞マ Date modified		
📴 Open	11-10-18 Name E brutus.exe i iamangel.eo	^	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM	Type Applicatic Applicatic	
Copen Look in	1: 11-10-18 Name i brutus.exe i iamangel.eo j jupiter.exe	^	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM 10/11/2018 3:35 PM	Type Applicatic Applicatic Applicatic	
Copen Look in Quick access Desktop	11-10-18 Name E brutus.exe i iamangel.eo	ie.	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM	Type Applicatic Applicatic	
Copen Look in Quick access	1: 11-10-18 Name Drutus.exe Diamangel.ex Dijupiter.exe moon.exe	ie.	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM 10/11/2018 3:35 PM 10/11/2018 3:35 PM	Type Applicatic Applicatic Applicatic Applicatic	
Copen Look in Quick access Desktop	1: 11-10-18 Name Drutus.exe Diamangel.ex Dijupiter.exe moon.exe	ie.	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM 10/11/2018 3:35 PM 10/11/2018 3:35 PM	Type Applicatic Applicatic Applicatic Applicatic	CANCEL
Copen Look in Quick access Desktop Libraries	1: 11-10-18 Name Drutus.exe Diamangel.ex Dijupiter.exe moon.exe	ie.	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM 10/11/2018 3:35 PM 10/11/2018 3:35 PM	Type Applicatic Applicatic Applicatic Applicatic	CANCEL
Copen Look in Quick access Desktop Libraries	t: 11-10-18 Name Drutus.exe Diamangel.ex Diamangel.exe Diama	ie.	Date modified 10/11/2018 3:32 PM 10/11/2018 3:30 PM 10/11/2018 3:35 PM 10/11/2018 3:35 PM	Type Applicatic Applicatic Applicatic Applicatic	CANCEL

• Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open' The file will be added to 'Protected Files'.

### Add a Drive Partition / Folder

• Click 'Folders' from the 'Add' drop-down.

COMODO Creating Trust Online

+ Add		🗶 🗱 Edit Remove	
File File Fold		Clients	
Br	owse For	Folder	×

The 'Browse for Folder' dialog will appear.

• Select the folder/drive and click 'OK'. Repeat the process to add more items. The items added to the 'Protected Files' will be protected from programs that are contained.

### Edit an item in the Protected Files list

• Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit property		? ×	
Edit File Path E:\CCAV\11-10-18\jupiter.exe			
	ок	CANCEL	

• Update as required and click 'OK'

### **Delete an item from Protected Files list**

- Select the item from the list and click the 'Remove' button
- The selected item will be deleted from the protected files list.

COMODO

### 6.5.2.2. Protected Keys

- Click 'Settings' > 'Containment' > 'Protected Objects' > 'Protected Keys'
- Registry items in 'Protected Keys' cannot be seen, accessed or modified by applications running in the container.
- Adding important registry keys to this area will protect them from unknown and potentially malicious programs.

### Open the 'Protected Keys' section

- Click 'Settings' on the CCS home screen.
- Click 'Containment' > 'Protected Objects'
- Select the 'Protected Keys' tab

COMODO Advanc	ed Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>Settings</li> </ul>	Protected Objects The following objects are protected from applications run PROTECTED DATA PROTECTED KEYS  Add Edit Remove	nning i	in the co	ontainer	
Auto-Containment Protected Objects Virtual Desktop Virtual Desktop Virtual Advanced Protection	□       Keys         □       Image: Application Keys         □       Image: Application Keys         □       Image: Application Keys				۹
	ок		C	ANCEL	

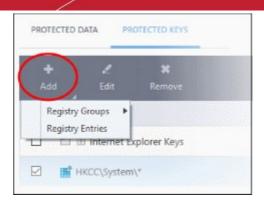
The buttons at the top provide the following options:

- · Add Select registry groups or individual keys that you want to protect
- Edit Modify the path of a key or key group
- **Remove** Delete the currently highlighted item
- · Click the search icon at the far-right to search for a specific item

Manually add individual keys or registry groups

Click the 'Add' button

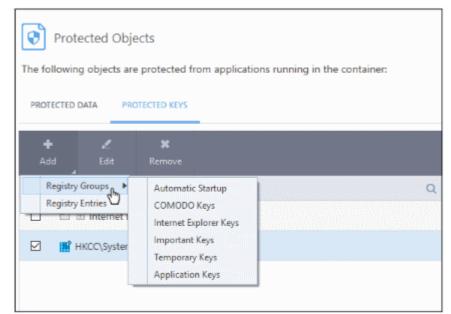
COMODO Creating Trust Online\*



- Registry Groups Select a pre-defined group of important registry keys. CCS ships with the following, predefined groups:
  - Automatic Startup keys
  - Comodo Keys
  - Internet Explorer Keys
  - Important Keys
  - Temporary Keys

You can also create custom groups of the keys you want to protect. See **Registry Groups** in **HIPS Groups** if you want help on this.

Click the 'Add' button > 'Registry Groups' > Select a key group from the list > Click 'OK'



- Registry Entries Add individual keys to the protected list
  - Click 'Add' > 'Registry Entries'
  - Select the keys you want to protect in the left-pane
  - Click the right-arrow to move them to the protected list:

COMODO

COMODO Select Registry Keys	
dd new item:	+
<ul> <li>S-1-5-21-57727447-3575129862- A</li> <li>AppEvents</li> <li>Console</li> <li>Control Panel</li> <li>EUDC</li> <li>Environment</li> <li>Keyboard Layout</li> <li>Preload</li> <li>Substitutes</li> <li>Toggle</li> <li>Network</li> <li>Printers</li> <li>Software</li> <li>System</li> <li>CurrentControlSet</li> <li>GameConfigStore</li> <li>Volatile Environment</li> </ul>	HKUS\S-1-5-21-57727447-3575129862-3883

- Alternatively, you can type the key name in the field at the top then click the '+' button
- Click OK. All items in the right pane will be added to the protected keys list

#### Edit an item in the list

• Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.

COMODO Edit property		? ×
Edit File Path HKCC\System\*		
	ОК	CANCEL

Update as required and click 'OK'

**Note**: Click 'Settings' > 'HIPS' > 'HIPS groups' > 'Registry Groups' to edit registry groups. See **Registry Groups** if you need more help.

### **Delete an item from Registry Protection list**

• Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the protected register list.

COMODO Creating Trust Online\*

### 6.6. Containment Settings

- Click 'Settings' > 'Containment' to open this interface.
- If CCS encounters a file that has a trust status of 'Unknown' then you have the option to automatically run that file in the container.
- The container is a secure, virtual environment where unknown files can run, but cannot affect the rest of your computer.
  - Files in the container are isolated from other processes, write to a virtual file system and registry, and cannot access your user data.
- Shared Space Because applications in the container cannot save files to your local file system, CCS creates a special folder at 'C:\ProgramData\Shared Space' for you to save files from the container. You can access files in this folder from your local desktop.
- If required, you can also allow contained applications save files to external storage devices. For example, to USB sticks and external storage drives.
- The containment settings area lets you configure all aspects of the container:

COMODO Advanced	Settings ? - □ ×
<ul><li>General Settings</li><li>Antivirus</li></ul>	Containment Settings
<ul><li>Firewall</li><li>HIPS</li></ul>	<ul> <li>Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.</li> <li>Do not virtualize access to <u>the specified files/folders</u></li> </ul>
- Containment Containment Settings	<ul> <li>Do not virtualize access to <u>the specified registry keys/values</u></li> <li>Do not virtualize access to the removable media</li> </ul>
Auto-Containment Protected Objects Virtual Desktop	Advanced ✓ Enable automatic startup for services installed in the container ✓ Show highlight frame for contained applications
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	<ul> <li>Detect programs which require elevated privileges e.g. installers or updaters</li> <li>Do not show privilege elevation alerts</li> <li>Run inside the Container •</li> </ul>
	OK CANCEL

See the following sections for more help:

- Containment Settings Configure exceptions to virtualization and other general settings
- Auto-Containment Rules Create and manage rules which tell CCS how to handle unknown files.
- **Protected Objects Containment** Define files, folders and registry keys which cannot be accessed by applications running in the container.
- Virtual Desktop Settings Configure options related to the Virtual Desktop application.
- Containment An Overview Background information about the containment process
- Unknown Files: The Scanning Processes Background information on how CCS determines the reputation of a file.

Note: The containment feature is not supported on the following platforms:

COMODO Creating Trust Online\*

- Windows XP 64 bit
- Windows Server 2003 64 bit

### 6.6.1. Containment Settings

• Click 'Settings' > 'Containment' > 'Containment Settings'.

The settings area lets you configure how proactive the auto-containment feature should be, and which types of files it should check.

#### **Configure containment settings**

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Containment Settings'

COMODO Advanced	Settings ? - $\Box$ X
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Containment Settings
✓ Firewall	Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.
- Containment	<ul> <li>Do not virtualize access to <u>the specified files/folders</u></li> <li>Do not virtualize access to <u>the specified registry keys/values</u></li> </ul>
Containment Settings	Do not virtualize access to the removable media
Auto-Containment	Advanced
Protected Objects	☑ Enable automatic startup for services installed in the container
Virtual Desktop	Show highlight frame for contained applications
✓ File Rating	☑ Detect programs which require elevated privileges e.g. installers or updaters
✓ Advanced Protection	☑ Do not show privilege elevation alerts Run inside the Container ▼
	OK CANCEL

Click the following links to find out more about each section:

- Shared Space Settings Shared space is a special folder which lets you swap files between the virtual environment and your real computer. You can also choose folders and registry keys that contained applications are allowed to access on your local system.
- Advanced Settings Configure containment alerts, enable automatic startup for programs installed in the container, and more.

### Shared Space Settings:

- 'Shared Space' is a dedicated area on your local drive that contained applications are allowed to write to.
- You should place files and folders in shared space if you want to access them from your real system.
- Shared space is located at 'C:\ProgramData\Shared Space'. The Virtual Desktop also uses shared space.
- Click 'Containment Tasks' > 'Open Shared Space' to get started:

COMODO Creating Trust Online\*

COMODO Client - Security 11	- ×
K HOME (j) SETTINGS	
Secure All systems are active and running	
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASKS	DVANCED TASKS
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Open Shared Space Open the storage space shared between virtual and real applications.
Reset the Container Clean container data by erasing all its content.	Watch Activity Open COMODO KillSwitch to monitor advanced process and system activity.
Run Virtual Desktop Create a secure virtual desktop and start using it.	<ul> <li>Containment Statistics Analyzer</li> <li>View analysis of Containment events and protection statistics of the component.</li> </ul>
	?

#### Exclusions

- By default, contained applications can access folders, files and registry keys on your local system, but cannot make changes to them.
- The 'Do not virtualize...' links let you create exceptions to this policy, so contained applications can make changes to certain files/folders.
- You can also enable contained applications to access removable storage devices like USB sticks and external hard disk drives.

#### Define exclusions for files and folders

- Do not virtualize access to the specified files/folders Specify files/folders on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual file system, and cannot access files/folders on the host system.
  - Select the option then click 'the specified files/folders' link.
  - The 'Manage Exclusions' dialog shows files and folders that can be modified by contained applications. By default, 'Shared Space' is the only folder they can write to:

COMODO Creating Trust Online\*

сомо	?		×							
+ Add	Edit	X Remove	ච Purge							
Path	Path Q									
	🗄 Shared Spa	aces								
			_							
			•	ок	C	ANCEL				

#### Add a file/folder exception

• Click the 'Add' button in the 'Manage Exclusions' dialog.

COMODO Creating Trust Online\*

COMODO Manage Exclusions ?								
+ Add Edit	× の Remove Purge							
File Groups Files Folders Running Processes	<ul> <li>Executables</li> <li>All Applications</li> <li>Windows Updater Applications</li> <li>Windows Management</li> <li>3rd Party Protocol Drivers</li> <li>Metro Apps</li> <li>Email Clients</li> <li>File Archivers</li> <li>Temporary Files</li> <li>Suspicious Locations</li> <li>Shared Spaces</li> <li>File Downloaders</li> <li>Web Browsers</li> <li>Browser Plugins</li> <li>Startup Folders</li> <li>Open Office</li> <li>Management and Productivity Applications</li> <li>COMODO Client - Security Manager</li> <li>COMODO Client Files/Folders</li> <li>Important Files/Folders</li> <li>Communication Client</li> <li>Windows System Applications</li> </ul>	ations						

- File Groups Choose a category of files or folders to which access should be granted. For example, select 'Executables' to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, \*\cmd.exe \*.bat, \*.cmd. See 'File Groups', for more details on file groups.
- · Files Pick specific files or applications that contained applications can access
- **Folders** Specify folders that can be accessed by contained applications. Access is granted to all files in the folder.
- **Running Processes** Choose a process currently running on your computer. The parent application of the process is added to the exclusions.
- Edit Select an item and click 'Edit' to change the target file or folder
- Remove Select an item and click 'Remove' to delete an exception
- **Purge** Checks that all files and folders covered in exceptions are still present on your computer. Purge automatically removes any items it can no longer locate.

• Click 'OK' to implement your settings

#### Define exclusions for specific Registry keys and values

- Do not virtualize access to the specified registry keys/values Specify registry keys on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual registry, and cannot access the real registry on the host system.
  - Select the option then click 'the specified registry keys/values' link.
  - The 'Manage Exclusions' dialog shows keys which you have allowed contained applications to access:

сомор	O Advance	d Settings					? —		
✓ General Setti	ings	~U~							
✓ Antivirus		•	Containment Settin	gs					
✓ Firewall			Shared Space(s) are the locations that contained applications and other applications and other applications are not virtualized.						
✓ HIPS		🗹 Do n	Do not virtualize access to the specified files/folders						
- Containment	t		ot virtualize access to				alues		
Containm	ent Settings	Advan		J.		-			
Auto-Cop		DO Mar	nage Exclusions		?		×		
	Exc	clusions					Q		
				ок	(	ANCEL			

### Add a Registry key exclusion

• Click the 'Add' button in the 'Manage Exclusions' dialog.

СС	)MOi	?	×				
(	+ Add	ي Edit	XX Remove				
	Registry Groups 🕨		Automatic	Startup	1		Q
	Registry E	Entries	COMODO Keys				
			Internet Exp	lorer Keys			
			Important K	(eys			
			Temporary	Keys			
			Application	к			

 Registry Groups - Batch select a predefined group of important registry keys as exclusions. See 'Registry Groups' for an explanation of registry groups defined in CCS.

dd new item:		
HKEY_CLASSES_ROOT	^	
HKEY_CURRENT_USER		
HKEY_LOCAL_MACHINE		
BCD0000000		
HARDWARE		
► SAM		
SECURITY		
<ul> <li>SOFTWARE</li> </ul>		
7-Zip	-	
AVAST Software		
COMODO		
Classes		
Clients		
ComodoGroup		
Google		
Intel		
Macromedia		
Microsoft	*	

• Registry Entries - Browse to individual Windows registry keys and add them as exclusions:

- Edit Select an item and click 'Edit' to change the target path
- Remove Select a key or group and click 'Remove' to delete the exception
- Click 'OK' to implement your settings

#### Enable access to removable storage devices

• Do not virtualize access to the removable storage media - Allow contained applications and virtual desktop applications to write to external storage devices. Example devices include USB sticks and external hard

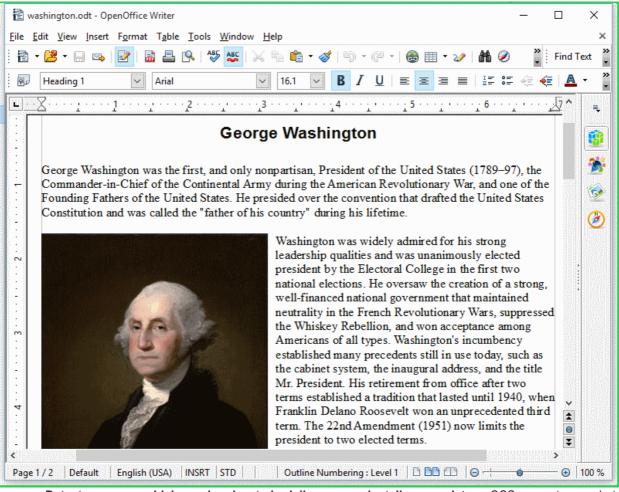
COMODO Creating Trust Online\*

drives. (Default = Disabled)

### **Advanced Settings:**

- Enable automatic startup for services installed in the container CCS launches contained services at Windows startup if this option is enabled. (*Default = Enabled*)
- Show highlight frame for contained applications CCS displays a green border around the windows of programs that are running in the container. (*Default = Enabled*)

The following screenshot shows an Open Office document running in the container:



- Detect programs which require elevated privileges, e.g., installer or updaters: CCS generates an alert when it detects an installer/updater that requires admin/elevated privileges to run. An installer that is allowed to run with elevated privileges can make changes to important areas of your computer such as the registry. (Default = Enabled)
- Example alert:

COMODO Creating Trust Online\*

сом	ODO Containment ?
	TrojanSimulator.exe could not be recognized and requests unlimited access to your computer
<b>M</b>	<u>TrojanSimulator.exe</u> Unidentified Publisher
(!)	Run Isolated (Default) Runs the application with limited access rights
$\bigcirc$	Run Unlimited Grants unlimited access to the application above
$\bigcirc$	Block Stops execution of the application above
Trust th	is application

- Run Isolated Runs the installer/updater in the container
- Run Unlimited Runs the installer/updater on your local computer, outside the container.
- Block Terminates the installer/updater.
- See 'Understand Security Alerts' for more details.
- Disable this option if you want CCS not to monitor applications that request elevated privileges on your computer
- **Do not show privilege elevation alerts**: CCS will not show alerts (as shown above) when a new or unrecognized application requires admin or elevated privileges to run.
  - If you disable alerts, you need to choose a default action that CCS should implement when it detects such an application:

COMODO Creating Trust Online\*

### Advanced

Enable automatic startup for services installed in the container

Show highlight frame for contained applications

Detect programs which require elevated privileges e.g. installers or updaters

Run inside the Container

Run Unlimited

Block

Run i de the Container

Run Unlimited and Trust

Do not show privilege elevation alerts

### 6.6.2. Auto-Containment Rules

- Click 'Settings' > 'Containment' > 'Auto-Containment'
- Auto-containment rules determine whether a program is allowed to run as normal, run with restrictions, or run in the virtual environment.
- A contained application has much less opportunity to damage your computer because it is isolated from your operating system, important system files and personal data.
- CCS consults these rules whenever you open an application. Rules at the top of the list have a higher priority. You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons.
- Programs running in the container have a green border around them.
- CCS ships with a set of pre-configured rules which provide maximum protection against unknown, potentially malicious applications. You can also create your own custom rules.

#### Manage Auto-Containment rules

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Auto-Containment'

COMODO Creating Trust Online\*

<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Enable /	o-Containm Auto-Containn tion enables au defined below.	nent	ontainment of e	executable	files and script	s according to th
<ul> <li>Containment</li> <li>Containment Settings</li> </ul>	+ Add	K. Edit	X Remove	∎ Move Up	↓ Move Do	C wn Reset to Default	
Auto-Containment		tion	Q	larget	Q Rat	ing Q	Enable Rule
Protected Objects		Block	ĺ	All Applicati	ons Mal	icious	
Virtual Desktop		Block		Cuspicious L	.oc Any		
<ul> <li>File Rating</li> </ul>	□ ⊘	Block	Í	Containmen	t F Any	•	
<ul> <li>Advanced Protection</li> </ul>		Ignore	É	Metro Apps	Any		
		Run Virtually	Í	All Applicati	ons Unr	ecognized	
		Run Virtually	Ē	All Applicati	ons Unr	ecognized	
		Run Virtually	Ē	All Applicati	ons Unr	ecognized	
		Run Virtually		Shared Space	es Unr	ecognized	

- The higher a rule is in the list, the higher priority it has. Use the move up/down buttons to change a rule's priority. In the event of a conflict in settings, CCS will obey the rule that is higher in the list.
- You can also add new rules and manage existing rules from this panel.

### **General Settings**

• Enable Auto-Containment - Enable or disable the containment system. If enabled, applications are run in the container as per the rules in this interface. (*Default = Enabled*)

#### **Containment Rules**

A rule performs a specific action on targets which have a certain reputation.

Containment Rules - Column Descriptions						
Column Header	Description					
Action	The operation that the containment system should perform on the target if the rule is triggered.					
Target	The file, file group, or location on which the rule should run.					
Rating	The trust status of the target item - 'Malware', 'Trusted', 'Unrecognized' or 'Any'.					
	The rule will apply to target items which have the reputation you choose here.					

COMODO Creating Trust Online\*

Enable Rule	Activate / deactivate	the rule
	Activate / deactivate	uic iuc.

- CCS ships with a set of pre-defined auto-containment rules which provide maximum protection for your system.
- There are five 'Block' rules, seven 'Run Virtually' rules, and one 'Ignore' rule.
- The rule numbers indicate their default priority in CCS. If there is a conflict, CCS implements the rule with the highest priority. You can, of course, rearrange priorities as required.
- The following tables show the settings of the pre-defined rules.

#### 'Block' Rules

- 1 Block and quarantine any malicious application
- 2 Block any file in the 'Suspicious locations' file group (i.e. anything in CCS quarantine and recycle bin)
- 3 Block any file in the folders Comodo uses for the container (i.e. anything in the \vtroot\ folder)

9 - Block pseudo file downloaders which are downloaded by browsers. Example downloaders are wscript.exe, powershell.exe, perl.exe etc.

13 - Block any file in the 'File Transfer Protocols' file group (i.e. any file in a URL starting with 'http:// or https://. This blocks installation of MSI packages via URL in a command line)

	R	ule Number	1	2	3	9	13
		Action	Block	Block	Block	Block	Block
		Target	File Group - All Applications	File Group - Suspicious Locations	File Group - Containme nt Folders	File Group - Pseudo File Downloader s	File Group - File Transfer Protocols
	Fil	e Reputation	Malicious	Any	Any	Any	Any
File	Source of file	Application	Any	Any	Any	Any	Any
origi n	creatio n	tio Process(es)	Any	Any	Any	Web Browsers Rating = Any	Any
		user(s)	Any	Any	Any	Any	Any
	Downloaded from		Any	Any	Any	Any	Any
		Vendor	Any	Any	Any	Any	Any
		Age of file	Any	Any	Any	Any	Any
	l	og Action	On	On	On	On	On
	Res	triction Level	N/A	N/A	N/A	N/A	N/A
	Limit M	aximum Memory	N/A	N/A	N/A	N/A	N/A
L	imit Prog	ram Execution Time	N/A	N/A	N/A	N/A	N/A
	(	Quarantine	On	Off	Off	Off	On
Ex	clude chi	ld processes from the	N/A	N/A	N/A	N/A	N/A

COMODO Creating Trust Online\*

#### action

#### 'Run Virtually' Rules

- 5 Virtualize unrecognized files which are less than three days old
- 6 Virtualize unrecognized files downloaded from the intranet, internet or removable storage devices.
- 7 Virtualize unrecognized files created by applications that belong to any of these file groups:
  - Web Browsers
  - Email Clients
  - File Downloaders
  - Pseudo File Downloaders
  - File Archivers
  - Management and Productivity Applications
  - Browser Plug-ins
  - Media Players
- 8 Virtualize any unrecognized file in the 'Shared Spaces' file group

10 - Virtualize 'msiexec.exe' if it was started by any process in the 'Management and Productivity Applications' group. The rule will search back ten parent levels of the process tree. 'msiexec.exe' is the MSI installer application.

- 11 Virtualize 'cmd.exe' if it was started by 'eqnedt32.exe'
- 12 Virtualize 'powershell.exe' if it was started by 'eqnedt32.exe'

'cmd.exe' is the name of the command shell executable, and 'powershell.exe' runs the task automation framework in Windows. 'eqnedt32.exe' is Microsoft's Equation Editor program. Rules 11 and 12 block malware which is impersonating or using the editor to launch attacks.

#### COMODO Creating Trust Online\*

	Rule Number		5	6	7	8	10	11	12
	Action		Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually
	Target		File Group - All Applications	File Group - All Applications	File Group - All Applications	File Group - Shared Spaces	File Location - *.msiexec.exe	File Location - *\cmd.exe	File Location - *\powershell.exe
F	ile Reputation		Unrecognized	Unrecognized	Unrecognized	Unrecognized	Any	Any	Any
File origin	File origin       Source of file creation       Applo         File origin       Source of file creation       o		Any	Any	Web Browsers Email Clients File Downloaders Pseudo File Downloaders File Archivers Management and Productivity Applications Browser Plug-ins Media Players	Any	Any	*\EQNEDT32.EX E	*\EQNEDT32.EX E
		Process( es)	Any	Any	Any	Any	File Group - Management and Productivity Applications	Any	Any



					Number of parent process levels to be analyzed = 10		
user(s)	Any	Any	Any	Any	Any	Any	Any
Downloaded from	Any	Intranet Removable media Internet	Any	Any	Any	Any	Any
Vendor	Any	Any	Any	Any	Any	Any	Any
Age of file	Less than 3 days	Any	Any	Any	Any	Any	Any
Log Action	On	On	On	On	On	On	On
Restriction Level	Off	Off	Off	Off	Off	Off	Off
Limit Maximum Memory	Off	Off	Off	Off	Off	Off	Off
Limit Program Execution Time	Off	Off	Off	Off	Off	Off	Off
Quarantine	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Exclude child processes from the action	N/A	N/A	N/A	N/A	N/A	N/A	N/A

COMODO Creating Trust Online\*

### Ignore Rule

4 - Do not auto-contain metro apps

	F	Rule Number	4			
	Action		Ignore			
	Target		File Group - Metro Apps			
	Fil	le Reputation	Any			
File	Source of file	Application	Any			
origi n	creation	Process(es)	Any			
	user(s)		Any			
		Downloaded from	Any			
		Vendor	Any			
		Age of file	Any			
		Log Action	On			
	Re	striction Level	N/A			
	Limit N	Aaximum Memory	N/A			
	Limit Prog	gram Execution Time	N/A			
		Quarantine	N/A			
Ex	clude child p	processes from the action	Off			

### Add an Auto-Containment Rule

- Auto-containment rules can be created for a single application, for all applications in a folder/file group, for running processes, or for a file/process hash value.
- You can create precision rules by specifying 'file creation source', 'file rating of the source', 'file origin', 'file rating' or 'file age'.
- You can also create simple rules to run an application in the container just by specifying the action and the target application.
- Click the 'Add' button at the top of the list in the Auto-Containment panel:

COMODO Creating Trust Online\*

Settings	?	-		×	
Auto-Containment					
Enable Auto-Containment					
This option enables automatic containment of executable files and policy defined below.	d script	s accor	ding to	the	
+     *     +     +       Add     Edit     Remove     Move Up     Move Down	C Reset to Default				
Action Q Target Q Reputation	Q	Enab	le Rule		
🔲 🥥 Block 📄 D:\Suspicious f Any			2		
COMODO Manage Contained Program			?		×
Action Run Virtually					•
The selected containment action will be applied if file properties	match	the fol	lowing	criteria	:
CRITERIA OPTIONS					
			E	dit	
No criteria selected					
	ОК		С	ANCEL	

The 'Manage Contained Program' dialog will appear. The 'Manage Contained Program' displays the action at the top and contains two tabs:

- Criteria Allows you to define conditions upon which the rule should be applied.
- Options Allows you to configure additional actions like logging, setting memory usage and execution time restrictions.

Creating a new containment rule involves the following steps:

- Step 1 Choose the action
- Step 2 Select the target file/group and set the filter criteria for the target files
- Step 3 Select the options

#### Step 1 - Choose the action

The settings in the 'Action' drop-down combined with the restriction level in the 'Options' tab determine the privileges of an auto-contained application. This determines what right it has to access other processes and hardware resources on your computer.

COMODO Creating Trust Online\*

сомо	DDO Manage Contained Program	?		×
Action	Run Virtually Run Restricted		(	
CRITERIA	Run Virtually Block Ignore			

The options available under the 'Action' drop-down are:

- **Run Virtually** The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- Run Restricted The application is allowed to access very few operating system resources. The
  application is not allowed to execute more than 10 processes at a time and is run with very limited
  access rights. Some applications, like computer games, may not work properly under this setting.
- Block The application is not allowed to run at all.
- **Ignore** The application will not be contained and allowed to run with all privileges.
- Choose the action from the options.

### Step 2 - Select the target file/group and set the filter criteria

- The next step is to select the target files and configure filters.
- You can filter a rule so it applies to specific types of file.
  - For example, you can specify 'All executables' as the target, then add a filter so it only affects executables from the internet.
  - Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target, then add 'Files created by a specific user' as the filter.

#### Select the target and set the filters

• Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

• To add new target and filter criteria, click the 'Edit' button at the far right

COMODO Creating Trust Online\*

COMODO Manage Contained Program	? 🗆	×
Action Run Virtually		•
The selected containment action will be applied if file properties match	the following criteria:	
CRITERIA OPTIONS		
	Edit	D
No criteria selected		
COMODO File Criteria	? 🗆 🗙	
Please select the criteria to be applied.		
File location:		
	Browse 🔻	
File created by applications: Any	Add 🔻 🔨	
File started by processes: Any	Add 🔻 🗸	
File created by users: Any	Add 🗸	
File origin: Any	Add 🔻 🗸	
File rating: Any	Select 🔻 🗸	
File signed by vendors: Any	Add 🔻 🗸	
File age: Any	Select 🗸	
	CANCEL	
ОК	CANCEL	

The 'File Criteria' dialog will open. The file criteria dialog allows you:

- Select the target
- Configure the filter criteria
- Select the target

Creating Trust Online

File Criteria	? ×	
Please select the criteria to be applied.		
File location:	Browse 🚽	
File created by applications:	Any Files Runting Proce	esses
	File Groups Folder File Hash Process Hash	

There are six types of target you can add:

.

- Files Apply the rule to specific files.
- **Running Processes** Apply the rule to a process that is currently running on your computer.
- File Groups Apply the rule to predefined file groups. See File Groups for help to add or modify a file group.
- Folder Apply the rule to a folder or drive.
- File Hash Create a hash value from a file and use it as the rule target. A hash value is a large number which is generated by passing the file through a hashing algorithm. The number uniquely identifies and represents the file, and it is extremely unlikely that two files will ever generate the same hash value. The benefit of using a file hash is that the rule will still work even if the file name changes.
- Process Hash Create a hash value of a process and use it as the rule target. Please see description
  above if required.

#### Add an individual File

• Choose 'Files' from the 'Browse' drop-down.

COMODO Creating Trust Online\*

	e Criteria	? 🗆 ×
Please select the criter	ia to be applied.	
File location:		
File created by applicat	tions:	Any Files File Groups
		Folder File Hash Process Hash
☑ Open ← → · ↑ □ « Pr Organize • New fold	rog → MB Free Astrolog ~ ひ	Search MB Free Astrology Birt 🔎
<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Documents</li> <li>Pictures</li> <li>Music</li> <li>old man files</li> <li>Suspicious</li> <li>Videos</li> <li>OneDrive</li> </ul>	Name          Image: Second system         Image: Second system	Date modified     Type       16-07-2000 16:20     Application       17-03-2010 16:12     Application       17-03-2010 15:23     Application
This PC 🗸	<	>
File r	name:	Executable Files (*.exe, *.dll, *.or ∨ Open ▼ Cancel

• Navigate to the file you want to add as target in the 'Open' dialog and click 'Open' The file will be added as target and will be run as per the action chosen in **Step 1**.

COMODO Creating Trust Online\*

OMODO File Criteria		?		×
Please select the criteria to be applied.				
File location:				
File location.				_
C:\Program Files (x86)\MB Free Astrology Birth Chart\M	IBFreeAstro	Br	owse	•

 Click 'OK', if you want to just add an application for a particular action as selected in Step 1 without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

• If required you can **configure filter criteria** and file rating and **options** for the rule.

Add a currently running application by choosing its process

• Choose 'Running Processes' from the 'Browse' drop-down.

COMODO Creating Trust Online\*

OMODO File Criteria		
Please select the criteria to be applied.		
File location:		
	Bro	wse 🔻
ette annatural la complicación de		Files
File created by applications:		Running Processes
		file Groups
		Folder
		File Hash
		Process Hash
		? ×
		ND
Application		PID
chrome.exe		4212 ^
chrome.exe		3840
chrome.exe		5928
chrome.exe		2452
chrome.exe		4332
chrome.exe		908
chrome.exe		3940
chrome.exe		2384
chrome.exe		4220
explorer.exe		3732
▼ <b>⊆</b> cis.exe		6120
✓ 🧧 cis.exe		6348
▼ C cis.exe		5916
<ul> <li>Cis.exe</li> <li>MSASCuiL.exe</li> </ul>		4428
<ul> <li>MSASCuil.exe</li> </ul>		6128
		4896
🖌 🝊 OneDrive.exe		24.00
		3168 🗸

A list of currently running processes in your computer will be displayed.

• Select the process, whose target application is to be added to target and click 'OK' from the 'Browse for Process' dialog.

The parent application of the process is added as the target and run as per the action in Step 1.

COMODO Creating Trust Online\*

File Criteria		?		×
Please select the criteria to be applied.				
File location:		P	rowse	
C:\Program Files (x86)\MB Free Astrology Birt	n Chart\IVIDFreeAstr	D	rowse	
File created by applications:	Any	Ad	d 🔻	^

 Click 'OK', if you want to just add the application for a particular action as selected in Step 1 without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

• If required you can **configure filter criteria** and file rating and **options** for the rule.

#### Add a File Group

• Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of files or folders configured as a 'File Group'. See **File Groups**, for more details on viewing and managing pre-defined and user-defined file groups.

COMODO Creating Trust Online\*

<b>OMODO</b> File Criteria	?		
Please select the criteria to be applied.			
File location:			
		Browse 🔻	
File created by applications:	Any	Files Running Processes	
		File Groups Folder File Hash Process Hash	Executables         All Applications         Important Files/Folders         Windows Updater Applications         Windows System Applications         Temporary Files         COMODO Client Files/Folders         COMODO Internet Security         COMODO Applications         Startup Folders         Windows Management         3rd Party Protocol Drivers         Metro Apps         Management and Productivity Applications         Web Browsers         Email Clients         Suspicious Locations         Shared Spaces         File Downloaders
			Pseudo File Downloaders File Archivers Containment Folders
			Browser Plugins
			Media Players

• Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in Step 1.

• Click 'OK', if you want to just add the file group for a particular action as selected in Step 1 without specifying any filters or options.

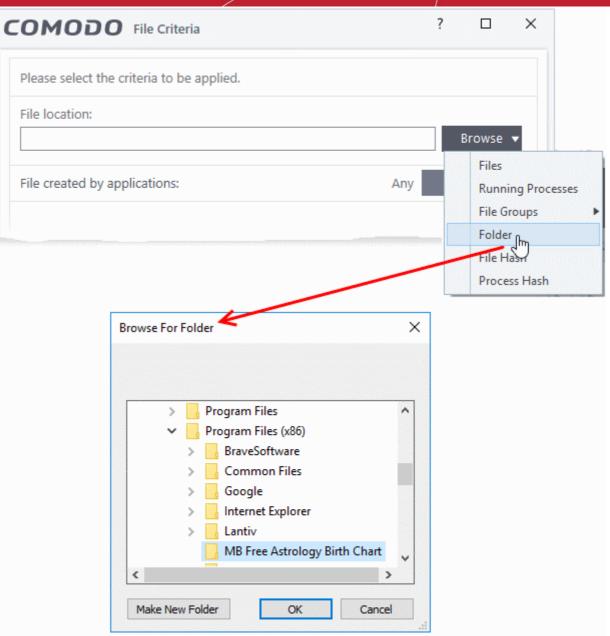
The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

• If required you can configure filter criteria and file rating and options for the rule.

#### Add a folder/drive partition

• Choose 'Folder' from the 'Browse' drop-down.

Creating Trust Online\*



The 'Browse for Folder' dialog will appear.

• Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as the target. All executable files in the folder will be run as per the action chosen in **step 1**.

• Click 'OK', if you want to just add the applications for a particular action as selected in **step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

• If required you can **configure filter criteria** and file rating and **options** for the rule.

#### Add a file based on its hash value

Choose 'File Hash' from the 'Browse' drop-down

Creating Trust Online\*

соморс	File Criteria	?		<
Please select the	criteria to be applied.			
File location:				
			Browse 🔻	
File created by a	oplications:	Any	Files Running Proce File Groups Folder File Hash Process Jash	esses
Copen $\leftarrow$ $\rightarrow$ $\sim$ $\uparrow$ $\square$ Organize $\checkmark$ Ne	« Prog » MB Free Astrolog ~ ひ	Search M	IB Free Astrolog	× / Birt , P
<ul> <li>Documents</li> <li>Pictures</li> <li>Music</li> <li>old man files</li> <li>Suspicious</li> <li>Videos</li> <li>OneDrive</li> </ul>	*	16 17	te modified -07-2000 16:20 -03-2010 16:12 -03-2010 15:23	Type Applicatio Applicatio
This PC	File name:	Executal Oper	ole Files (*.exe, * n <b> ▼</b> (	> dll, *.or ~ Cancel

- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'
- Click 'OK', if you want to just add the file for a particular action as selected in **step 1** without specifying any filters or options.
- If required you can **configure filter criteria** and file rating and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

COMODO Creating Trust Online\*

#### Add an application from a running process based on its hash value

• Choose 'Process Hash' from the 'Browse' drop-down.

File Criteria ? $\Box$ ×	
iteria to be applied.	
Browse	
lications: Any Files File Groups Folder File Hash	cesse
Process Has	հ լի
Browse for Processes ?	;
PID	
xe 4212	
xe 3840	
xe 5928	
xe 2452	
xe 4332	
xe 908	
xe 3940	
xe 2384	
xe 2384 xe 4220	
xe 2384 xe 4220 3732	
xe 2384 xe 4220 3732 6120	
xe 2384 xe 4220 3732 6120 6348	
xe 2384 xe 220 3732 6120 6348 5916	
xe 2384 xe 4220 3732 6120 6348 5916 exe 4428	
xe 2384 xe 4220 3732 6120 6348 5916 exe 4428 Lexe 6128	
xe 2384 xe 4220 3732 6120 6348 5916 exe 5916 4428 Lexe 6128	
xe 2384 xe 4220 3732 6120 6348 5916 exe 4428 Lexe 6128	

A list of currently running processes in your computer is shown.

- Select the process, to add the hash value of its parent application as the target and click 'OK'
- Click 'OK', if you want to just add the application for a particular action as selected in step 1 without

COMODO Creating Trust Online\*

specifying any filters or options.

- If required you can **configure filter criteria** and file rating and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the process name changes.

#### **Configure the Filter Criteria and File Rating**

You can apply an action to a file if the file meets certain criteria.

The available criteria are:

- By application that created the file
- By process that created the file
- By user that created the file
- By file origin
- By file rating
- By vendor who signed the file
- By file age

#### Auto-contain a file if it was created by a specific application

- You can create a filter to apply an action to a file based on its source application.
- You can also specify the file rating of the source application. The rule will then only contain a file if its parent app has a certain trust rating.

Specify source application(s):

Click the 'Add' button in the 'File Created by applications' stripe.

COMODO File Criteria	?		×
Please select the criteria to be applied.			
File Belongs to (File Group):			
Temporary Files		Browse	•
File created by applications:	Arv /	Add 🔻	
		Files	
		Run Ög F	
		File Group	15
		Folder	
		File Hash	
		Process H	ash

The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.

The selected source application, file group or the folder will be added.

• Click the 'Any' link beside 'File Rating' and select the file rating of the source

Creating Trust Online\*

сомо	e Belongs to (File Group): emporary Files le created by applications: 1 process(es Executables File Rating: Any Any	?		×	
Please sele	ect the criteria to be applied	l.			
File Belong	js to (File Group):				
Temporar	Please select the criteria to be applied. File Belongs to (File Group): Temporary Files File created by applications: 1 process(es) Add Executables File Ration: Any	•			
File created	d by applications:	1 process(es)	A	dd 🔻	^
	$\sim$			;	×
	Any				
	Trusted				
	Unrecognized				
	Malicious 🖑				

• Repeat the process to add more applications or groups/folders.

#### Auto-contain a file if it was created by a specific process

- You can create a filter to apply an action to a file based on its parent process.
- Optionally, you can also specify:
  - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
  - The number of levels in the process chain that should be inspected.

To specify source process(es)

• Click the 'Add' button in the 'File Created by Process(es)' stripe.

OMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files			Browse	•
File created by applications:	Any	ļ	Add 🔻	$\sim$
File started by processes:	Any	ļ	Add 🔻	^
			Files	
			Running	Processe
			File Gr	ps
			Folder	
			File Hash	
			Process H	Hash

COMODO Creating Trust Online\*

- The options available are same as those available under the 'Browse' button beside 'Target', as explained above.
- The selected source application, file group or the folder will be added. The file created / invoked by the process, started by the selected source will be added as the target for the rule.
- ? × COMODO File Criteria Please select the criteria to be applied. File Belongs to (File Group): Browse **Temporary Files** Add File created by applications: Any Add File started by processes: 1 process(es) All Applications × File Rating: Any Any \* Number vels to be analyzed: Trusted Unrecognized Malicious
- Click the 'Any' link beside 'File Rating' and select the file rating of the source

'Number of parent process levels to be analyzed' - Specify how far up the process tree CCS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.

	File started by processes:	1 process(es)	Add 🖣	^
<	All Applications File Rating: <u>Malicious</u>	zed:	1	×
	File created by users:	Any	Add	~

• Repeat the process to add more process(es)

#### Auto-contain a file created by specific user(s)

• Click the 'Add' button in the 'File Created by User(s)' stripe.

COMODO Creating Trust Online\*

Please select the criteria to be applied.	
File Belongs to (File Group):	
Temporary Files	Bi
File created by applications:	Any Ado
File started by processes:	Any Ado
File created by users:	Any Add
Select User or Group	
Select User or Group Select this object type: User, Group, or Built-in security principal	Object Types
Select this object type:	
Select this object type: User, Group, or Built-in security principal	
Select this object type: User, Group, or Built-in security principal From this location:	Object Types
Select this object type: User, Group, or Built-in security principal From this location: DESKTOP-FKQF9QT	Object Types
Select this object type: User, Group, or Built-in security principal From this location: DESKTOP-FKQF9QT	Object Types
Select this object type: User, Group, or Built-in security principal From this location: DESKTOP-FKQF9QT	Object Types

- The 'Select User or Group' dialog will appear.
  - Type the names of the users to be added to the rule. Use the format <domain name>\<user/group name> or <user/group name>@<domain name>.
  - Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.

COMODO Creating Trust Online\*

Select this object t		1	
User, Group, or B	uilt-in security principal		Object Types
From this location:			
DESKTOP-1N2U	S38		Locations
Enter the object na	ame to select ( <u>examples</u> ):		
******			Check Names
	×		
Advanced		ОК	Cancel
1			
Select User or Gro			
elect user of on	ир 		
Select this object t	ype:		
User, Group, or B	uilt-in security principal		Object Types
From this location:			
DESKTOP-1N2U	S38		Locations
Common Queries			
Sommon Spence			
Name:	Starts with $\sim$		Colu
Description:	Starts with 🖂		Find
Disabled ac			St
Non expiring			
	, password		
Days since last	logon: 🗸 🗸		/ *
		/	
Search results:			OK Car
Vame	In Folder	1	
	DESKTOP-1N2		
	DESKTOP-IN2		
Everyone	K		
<mark>o</mark> Guest	DESKTOP-1N2		
Guests	DESKTOP-1N2		
Hyper-V Admi	DESKTOP-1N2 DESKTOP-1N2		
linfra	DESKTOP-1N2		
	DESKTOP-1N2		

The user will be added to the list.

COMODO Creating Trust Online\*

(	<b>COMODO</b> File Criteria		?		×
	Please select the criteria to be applied.				
	File Belongs to (File Group):				
	Temporary Files			Browse	•
	File created by applications:	Any	A	\dd ▼	$\mathbf{v}$
	File started by processes:	Any	A	∖dd ▼	$\mathbf{v}$
	File created by users:	1 user(s)	A	١dd	^
	Guests				×

- Repeat the process to add more users.
- To remove the user added by mistake or no longer needed in the list, click the 'X' icon at the right end of the user name.

#### Auto-contain a file downloaded/copied from a specific source

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:

OMODO File Criteria		?		×	
Please select the criteria to be applied.					
File Belongs to (File Group):					
Temporary Files			Browse	•	
File created by applications:	Any	A	dd 🔻	~	
File started by processes:	Any	A	dd 🔻	$\sim$	
File created by users:	1 user(s)	A	dd	$\sim$	
File origin:	Any	A	dd 🔻	^	
			Internet		
			Rec Va Intranet	ble Meo	dia

- **Internet** The rule will only apply to files that were downloaded from the internet.
- **Removable Media** The rule will only apply to items copied to the computer from removable devices like a USB drive, CD/DVD or external storage.

COMODO Creating Trust Online\*

- Intranet The rule will only apply to files that were downloaded from the local intranet.
- Repeat the process to add more sources

#### Select the file rating as filter criteria

•

• Click the 'Select' button in the 'File Rating' stripe:

<b>COMODO</b> File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files		В	rowse	•
File created by applications:	Any	Ad	d 🔻	$\sim$
File started by processes:	Any	Ad	d 🔻	$\checkmark$
File created by users:	1 user(s)	Ad	d	$\checkmark$
File origin:	2 origin(s)	Ad	d 🔻	$\mathbf{\vee}$
File rating:	Any	Sele	ect 🔻	^
		Ti	rusted	
		U	nrecogi	nized
	Annual Conditional and Grannel at 116 address damages (2015)	N	laliciou	s 🖑

- This will apply the rule to files which match the trust rating you set. You can choose from the following trust ratings:
  - **Trusted** Applications are categorized as 'Trusted' if:
    - · The file is on the global whitelist of safe files
    - The file is signed by a trusted company in the Vendor List
    - · The file was installed by a trusted installer
    - The file was given a trusted rating in the File List by a user
    - See File Rating Settings for more information.
  - Unrecognized Files that do not have a current trust rating. The file is on neither the blacklist nor the safelist, so is given an 'unknown' trust rating. See File List for more information.
  - Malware Malicious files those that are on the blacklist of known harmful files...

#### Auto-contain a file based on the software vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.
- You can also specify the file rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

Specify vendors

- Click the 'Add' button in the 'File signed by vendors' stripe.
- There are three ways you can add a vendor:
  - 1. Directly select a vendor

COMODO Creating Trust Online\*

OMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files		В	rowse	•
File created by applications:	Any	Ad	d 🔻	$\mathbf{v}$
File started by processes:	Any	Ad	d 🔻	$\sim$
File created by users:	1 user(s)	Ad	d	$\sim$
File origin:	2 origin(s)	Ad	d 🔻	$\sim$
File rating:	Unrecognized	Sele	ct 🔻	$\sim$
File signed by vendors:	Any	Ad	d 🔻	^
		V Ve Fi	le Sign	rom Vend er Process S

- Choose 'Vendor from a Vendor List' from the drop-down
- The 'Add Vendor' dialog opens with a list of vendors in the Vendor List

Creating Trust Online\*

Vendor	Q	Rated By	Y	Rating	Y	1
Itannex B.V.		Comodo		✓ Trusted		
Neo IT Solutions Ltd.		Comodo		✓ Trusted		
Festo Didactic SE		Comodo		✓ Trusted		
FTPPro.com		Comodo		✓ Trusted		
Timo Bingmann		Comodo		✓ Trusted		
Shearwell Data Ltd		Comodo		✓ Trusted		
Boyishsoft		Comodo		✓ Trusted		
Integrated Scuba Systems, Ilc		Comodo		✓ Trusted		
TeacherWeb, Inc.		Comodo		✓ Trusted		

- Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

#### 2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CCS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

#### 3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CCS checks that the .exe file that started the process is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

The selected vendor is added:

COMODO Creating Trust Online\*

File rating:	Unrecognized Select 🗸 🗸
File signed by vendors:	1 vendor(s) Add 🗸 🔨
Girlssoft Vendor Rating: <u>Any</u>	×

- **Vendor Rating** The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.
  - Example. If you select 'Trusted' here, then CCS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.

File rating:		Unrecognized Select	• •
File signed by v	endors:	1 vendor(s) Add	• •
Girlssoft Vendor Ratin	g: <u>Any</u>		×
	Any Trusted		
	Unrecognized Malicious		

• Repeat the process to add more vendors

#### Set the file age as filter criteria

• Click the 'Select' button in the 'File age' stripe.

COMODO Creating Trust Online\*

COMODO File Criteria ?	×
Please select the criteria to be applied.	
File location: Browse	
biowse	
File created by applications:     Any     Add     T	~
File started by processes:     Any     Add     *	~
File created by users: Any Add	~
File origin: Any Add 🔻	~
File rating: Any Select 🔻	~
File signed by vendors: Any Add 🗸	~
File age: Ary Select	>
COMODO File age: ? ×	
File creation date:	
Before 🔻 04/15/2019 👻 4:11:24 PM 🜩	
O File age:	
Less Than 🔻 1 📮 day(s) 💌	
OK CANCEL	

The 'File Age' dialog will appear. You can set the file age in two ways:

- File Creation Date To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- File age To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - Less Than CCS will check for reputation if a file is younger than the age you set here. Select
    the interval in hours or days from the first drop-down combo box and set hours or days in the
    second drop-down box. (Default and recommended = 1 hours)

COMODO Creating Trust Online\*

- **More Than** CCS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)
- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.

COMODO Manage Contained Program	?		×
Action Run Virtually			•
The selected containment action will be applied if file properties match	h the followin	g criteria	ə:
CRITERIA OPTIONS			
		Edit	
File Belongs to (File Group): Temporary Files			
File created by users: Guests			
File origin: Removable Media Internet			
File rating: Unrecognized			
File signed by vendors: Girlssoft Vendor Rating: Any			
ок		CANCEL	

#### **Step 3 - Select Options**

The next step is to choose additional options and restrictions on items contained by the rule.

• Click the 'Options' tab.

Creating Trust Online\*

COMODO Manage Contained Program	?		×
Action Run Virtually The selected containment action will be applied if file properties match the fol CRITERIA OPTIONS	lowing	criteria	•
<ul> <li>Log when this action is performed</li> <li>Set Restriction Level Partially Limited </li> <li>Limit maximum memory consumption to 1 MB</li> <li>Limit program execution time to 1 secs</li> </ul>			
ОК	G	ANCEL	

The options available depend on the 'Action' chosen in Step 1.

The 'Ignore' action has the following options:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS Containment logs.
- Don't apply the selected action to child processes Child processes are those started by the target application.
  - This option is disabled by default, so the ignore rule also applies to child processes.
  - If enabled, the ignore rule does not apply to child processes. Each child process will be inspected individually and all relevant rules applied.

The 'Run Restricted' and 'Run Virtually' actions have the following options:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS Containment logs
- Set Restriction Level When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
  - Partially Limited The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations

COMODO Creating Trust Online\*

like loading drivers or debugging other applications are also not allowed.(Default)

- Limited Only selected operating system resources can be accessed by the application. The
  application is not allowed to execute more than 10 processes at a time and is run without
  Administrator account privileges.
- **Restricted** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- Untrusted The application is not allowed to access any operating system resources. The
  application is not allowed to execute more than 10 processes at a time and is run with very limited
  access rights. Some applications that require user interaction may not work properly under this
  setting.
- Limit maximum memory consumption to Enter the memory consumption value in MB that the process should be allowed.
- Limit program execution time to Enter the maximum time in seconds the program should run. After the
  specified time, the program will be terminated.

The 'Block' action has the following options:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS Containment logs.
- Quarantine program If checked, the programs will be automatically quarantined. See Manage Quarantined Items for more information.
- Choose the options and click 'OK' to save them for the rule. The rule will be added and displayed in the list.

COMODO Advanced	Settings		? – 🗆 X
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Auto-Containm ✓ Enable Auto-Containm		
✓ HIPS	This option enables au policy defined below.	tomatic containment of executable file	s and scripts according to the
<ul> <li>Containment</li> <li>Containment Settings</li> </ul>	+ 🖌 Add Edit	* t I Remove Move Up Move Down	C Reset to Default
Auto-Containment	Action	O Target O Repu	Itation Q Enable Rule
Protected Objects	🗹 불 Run Virtually	Temporary Files Unre	cognized
Virtual Desktop	🗌 🥥 Block	All Applications Malic	ious
<ul> <li>Advanced Protection</li> </ul>	Block     Block	Suspicious Loca Any	
	□ → Ignore	Communication Trust	ed 💽
	□ → Ignore	Metro Apps Any	
	🗌 🛃 Run Virtually	All Applications Unre	cognized
	D Ø Block	Pseudo File Do Any	
		ОК	CANCEL

COMODO Creating Trust Online\*

You can move the rule up or down the list to change its priority.

#### Edit an Auto-Containment Rule

- Select a rule from the list in the Auto-Containment panel and click 'Edit' from the top.
- The edit procedure is similar to adding an auto-containment rule.
- Click 'OK' to save the rule changes.

**Important Note**: Please make sure auto-containment rules do not conflict. In the event of a conflict, the setting in the rule that is higher in the list prevails. The 'Reset to Default' button lets you restore the original rules.

### 6.6.3. Virtual Desktop Settings

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Virtual desktop settings let you set password protection, automatic login for specific users, and more.
- You can also configure desktop and start-menu shortcuts which will launch applications in the virtual desktop

#### Configure virtual desktop settings

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Virtual Desktop'

COMODO Advanced	l Settings ? — 🗆 🗙			
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Virtual Desktop			
<ul> <li>Firewall</li> </ul>	Request password when exiting Virtual Desktop <u>Create/Change password</u>			
V HIPS	Show disclaimer upon Virtual Desktop startup Edit Disclaimer			
— Containment	✓ Protect paused Virtual Desktop session with PIN			
Containment Settings	Duration of paused Virtual Desktop session before its automatic termination for the min(s)			
Auto-Containment	APPLICATIONS USERS			
Protected Objects				
Virtual Desktop	Applications quickly accessible via Virtual Desktop shortcuts or start menu:			
✓ File Rating	▲     Cr       Add     Remove       Remove     Default			
<ul> <li>Advanced Protection</li> </ul>	Application Q Desktop Start Menu			
	C:\Windows\explorer.exe			
	C:\Program Files\Internet Explorer\iexplore.exe			
	OK CANCEL			

The interface allows you to:

 $\sim$ 

\_ \_

### Comodo Client Security - User Guide

- Set an exit password for virtual desktop
- Configure 'Disclaimer' shown during startup of virtual desktop
- Secure virtual desktop sessions with a PIN
- Set time-out period for paused virtual desktop sessions
- Add applications to virtual desktop
- Set virtual desktop to start automatically when selected users / users in selected user group log-in
- **Request password when exiting Virtual Desktop** Create an 'exit' password for the virtual desktop. Users need to enter the password in order to close the virtual desktop.

сомо	DO Enter p	assword	×
Password:			
		ОК	CANCEL

This prevent users from closing the virtual desktop and accessing the host, potentially exposing the computer to danger. (*Default = Disabled*)

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Enable 'Request password when exiting Virtual Desktop'
- Click the '<u>Create/Change password</u>' link:

	Virtual Desktop
Req	uest password when exiting Virtual Desktop <u>Create/Change password</u>
	w disclaimer upon Virtual Desktop startup <u>Edit Disclaimer</u>
- a 17	
	COMODO Create/Change password ? ×
	Create/Change password
	Password:
	Retype:

Type a password that cannot easily be guessed.

COMODO Creating Trust Online\*

- It should be 8-16 characters long and contain a mix of upper case letters, lower case letters, numbers, and special characters.
- Confirm the password then click 'OK'.
- The validity of the password is 90 days. You need to reset the password when it expires.
- Show disclaimer upon Virtual Desktop startup Create a disclaimer which is shown when the virtual desktop starts. Users must accept the disclaimer before they can access the virtual desktop. Default = Enabled.

#### **Create Virtual Desktop disclaimer**

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Enable 'Show disclaimer upon Virtual Desktop startup'
- Click the 'Edit Disclaimer' link:

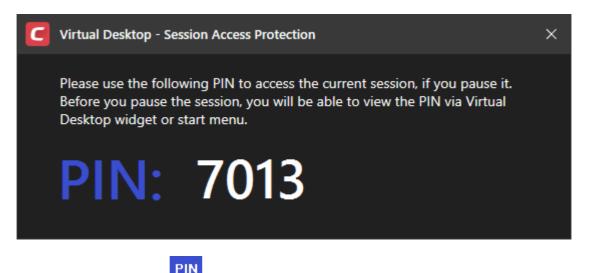
O Advanced	Settings	?	-		×
	Virtual Desktop				
	☐ Request password when exiting Virtual Desktop <u>Greate/Char</u> ✓ Show disclaimer upon Virtual Desktop startup <u>Edit Disclaimer</u>		assword	<u>t</u>	
	Protect paused Virtual Desktop session with PIN	_			
- Sottinger 1	Duration of paused Virtual Desktop session before its autom	atic	1	i m	in(c)
сомо	DO Edit Disclaimer		?		×
<inser< th=""><th>: disclaimer text here≻</th><th></th><th></th><th></th><th></th></inser<>	: disclaimer text here≻				
1	SAVE		C	ANCEL	

- Enter the disclaimer message and click 'Save'.
- The message is shown when the virtual desktop starts.
- Users should read the disclaimer and click 'Accept':

COMODO Creating Trust Online\*

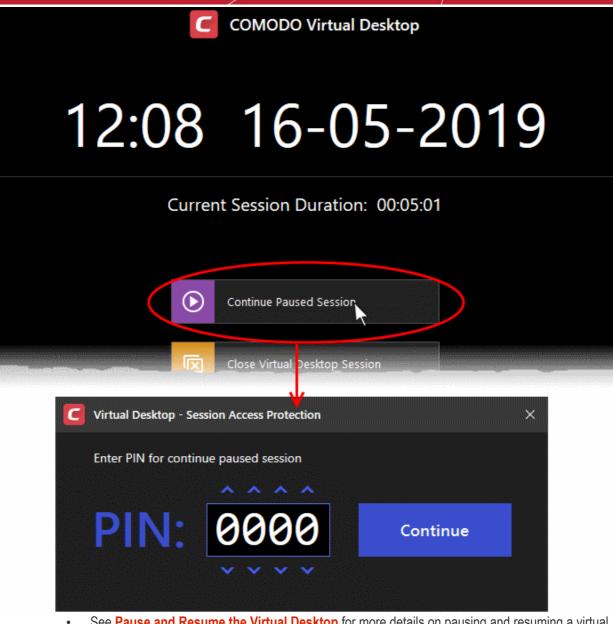
×	×
ılly	

- Protect paused Virtual Desktop session with a PIN Generates a session specific PIN number during virtual desktop startup. The PIN is required to resume the session from a paused state. This creates a second layer of authentication on top of the regular Windows username/password for any sensitive data in the virtual desktop. The feature is also useful on shared computers as it prevents other users from accessing the session. (*Default = Disabled*).
  - Select this option if you want to secure virtual desktop sessions with a PIN



- Click 'Show PIN'
   in the start menu to view the number at any time.
- The user needs to make a note of the PIN. If they pause the virtual desktop session they will need to enter the PIN to resume.

COMODO Creating Trust Online\*



See Pause and Resume the Virtual Desktop for more details on pausing and resuming a virtual desktop session

 Duration of paused Virtual Desktop session before its automatic termination - Set the maximum length of time a virtual desktop session can be left in paused state. The session gets automatically terminated when this period elapses. (*Default = Disabled*)

#### Add applications to virtual desktop

- The virtual desktop start menu has shortcuts for Windows explorer and your installed browsers.
- You can also add shortcuts in the virtual desktop for any other application.
- Alternatively, you can open any application inside the virtual desktop by navigating to the executable file.
- This section explains how to add and shortcuts for applications that you want to run inside the virtual desktop

#### Add application shortcuts and start menu items to virtual desktop

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Virtual Desktop'
- · Click 'Add' under 'Applications' in the 'Virtual Desktop' settings interface

COMODO Creating Trust Online\*

COMODO Advanced	Settings ? - □ ×
✓ General Settings	
✓ Antivirus	Virtual Desktop
✓ Firewall	Request password when exiting Virtual Desktop Create/Change password
✓ HIPS	Show disclaimer upon Virtual Desktop startup Edit Disclaimer
- Containment	Protect paused Virtual Desktop session with PIN
Containment Settings	Duration of paused Virtual Desktop session before its automatic termination
Auto-Containment	APPLICATIONS USERS
Protected Objects	
Virtual Desktop	Applications quickly accessible via Virtual Desktop shortcuts or start menu:
✓ File Rating	+ K C Add Remove Reset to Default
<ul> <li>Advanced Protection</li> </ul>	Applications Q Desktop Start Menu
	Running Process
	C:\Program Files\Internet Explorer\iexplore.exe
	OK CANCEL

You can add applications in two ways:

- Application Navigate to the location of the executable file for the application and select 'Open'
- **Running Processes** Select the process from the list of currently running processes, whose parent application is to be added click 'OK'.

COMODO Creating Trust Online\*

COMODO Browse for Processes	?	×
Application	PID	
ITSMAgent.exe	6652	X
🛛 🐂 explorer.exe	180	
✓	4264	
🕶 🐠 firefox.exe	6980	
4 🧕 firefox.exe	3176	
4 🐠 firefox.exe	252	
🔺 🕩 firefox.exe	1968	
I O browser_assistant.exe	4024	
🔺 📴 cis.exe	6120	
▲ 😡 MyWeather.exe	5016	
🔺 💹 Evernote.exe	7060	
4 🎕 LanTime.exe	1480	
📧 svchost.exe	6208	
O opera.exe	5976	
opera.exe	3248	
<ul> <li>opera_crashreporter.exe</li> </ul>	4436	
opera.exe	4372	•
	OK CANCEL	

#### The applications will be added to the list:

Applicat	tions quickly acce	essible via Virtual	Desktop short	cuts or start me	nu:
<b>∔</b> Add	X Remove	C) Reset to Default			
	Application		Q	Desktop	Start Men
	C:\Windows\expl	orer.exe			
	C:\Program Files\	Internet Explorer	iexplore.exe		
	C:\Program Files	(x86)\Google\Chr	ome\Applic		
	C:\Program Files	(x86)\MyFreeWea	ther\MyWe		

- Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut per application.
- Click 'OK' to save your settings
- · Click OK in the 'Advanced Settings' dialog for your changes to take effect

#### Add users who should log straight into the virtual desktop

• You can configure the virtual desktop to start automatically whenever certain users login to the system.

paration or paused virtual pesses of persion persion attomatic termination 1 🗘 min(s) tainment APPLICATIONS USERS Objects Users for whom Virtual Desktop will be launched as a primary working environment: ÷ Reset to Default otection User or Group Q Enable Guests D Alice CANCEL ок

#### This means the virtual desktop becomes the default operating environment for those users.

#### Add users

٠

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Virtual Desktop'
- Select the 'Users' tab
- Click 'Add'

COMODO Creating Trust Online

COMODO Creating Trust Online\*

at Settings	La termination	min(s)
ntainment	APPLICATIONS USERS	
d Objects		
	Users for whom Virtual Desktop will be launched as a prima	ry working environment:
	+ ★ C Add Madd Marting Remove Default	
rotection	User or Group	Q Enable
	Guests	
	Alice	
		DK CANCEL
		///
	Select User or Group	×
	Select this object type:	
	User, Group, or Built-in security principal	Object Types
	From this location:	
	DESKTOP-BGTT5H7	Locations
	Enter the object name to select ( <u>examples</u> ):	-
		Check Names
	Advanced OK	Cancel

- Select the users or user groups to whom you want this rule to apply.
  - Type the names of users or groups in the format <domain name>\<user/group name> or <user/group name>@<domain name>.
  - Alternatively, click 'Advanced' then 'Find Now' to locate specific users/user groups.
  - Click 'OK' to confirm.

•

COMODO Creating Trust Online\*

			1	
Select User or Gro	up			×
Select this object ty	/pe:			
User, Group, or Bu	Object Types			
From this location:				
DESKTOP-BGTT5	iH7		Locations	
Enter the object na	me to select ( <u>examples</u> ):			
			Check Name	s
Advanced	)	ОК	Cancel	
elect User or Gro Select this object ty	/ре:			
User, Group, or Bu	ilt-in security principal		Object 7	Types
From this location:				
DESKTOP-BGTT5	iH7		Locati	ons
Common Queries				
Name: S	itarts with 🖂			Colum
Description: S	itarts with $\sim$		کر 🗆	Find N
Disabled acc	ounts			Sto
Non expiring	password			
Days since last	logon: 🗸 🗸			R
Search results: 🛩			OK	Cano
Vame	In Folder			
Access Contr	DESKTOP-BGT			
Administrator	DESKTOP-BGT			
Administrators	DESKTOP-BGT			
Alice Backup Oper	DESKTOP-BGT DESKTOP-BGT			
Bob	DESKTOP-BGT			
Cryptographic	DESKTOP-BGT			
DefaultAccount	DESKTOP-BGT			
Contract Contract Device Owners	DESKTOP-BGT			
Distributed C	DESKTOP-BGT			

The user / user group will be added to the list.

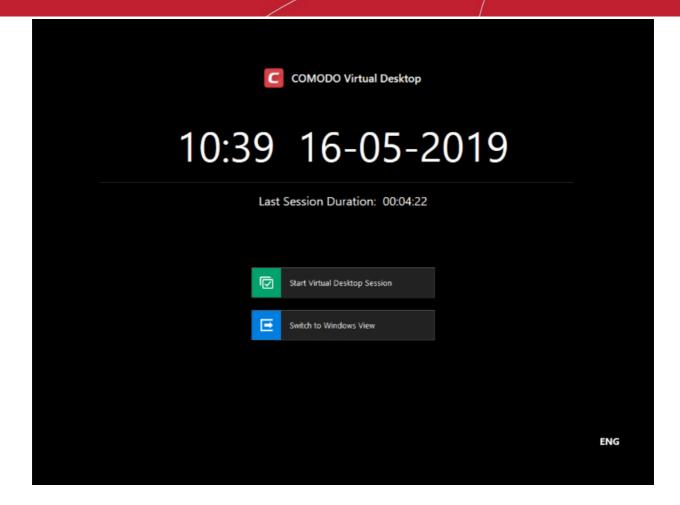
COMODO Creating Trust Online\*

inment	APPLICATIONS USERS	Trmit(5)
)bjects (top	Users for whom Virtual Desktop will be laund	hed as a primary working environment:
	<b>+ ≭ C</b> Add Remove Reset to Default	
ection	User or Group	Q Enable
	Guests	
	Alice	
	Bob	
		OK CANCEL

- Repeat the process to add more users.
- Click 'OK' to save your settings
- Click OK in the 'Advanced Settings' dialog for your changes to take effect

The virtual desktop starts automatically when the user signs-in to the computer.

COMODO Creating Trust Online\*



- The user can decide whether to continue with the virtual desktop or switch to the host OS.
- If so configured, users will need to provide a password to close the virtual desktop.

### 6.6.4. Containment - An Overview

- The container is an isolated operating environment for unknown and untrusted applications.
- Running an application in the container means that it cannot make changes to other processes, programs
  or data on your local computer. Applications in the container are executed under a carefully selected set of
  privileges and write to a virtual file system and registry instead of you real system.
- This delivers a smooth user experience by letting unknown applications run as normal while denying them the potential to cause damage.
- After an unknown application has been placed in the container, CCS also submits it to Valkyrie for behavior analysis. Valkyrie tests include:
  - Static analysis
  - Dynamic analysis
  - Valkyrie plugins and embedded detectors
  - Signature-based detection
  - Trusted vendor and certificate validation
  - Reputation system
  - Human expert analysis
  - If Valkyrie discovers that a file is malicious then it is added to the antivirus black list. The file is quarantined on the local machine and the user is alerted.
- Users can print documents from within the container. This is useful, for example, if a suspicious PDF has
  valid information that should be printed.

COMODO Creating Trust Online\*

By uniquely deploying 'containment as security', CCS offers improved security, fewer pop-ups and greater ease of use than ever before.

### 6.6.5. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CCS security inspections:
  - Antivirus scan
  - HIPS Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CCS (and therefore not scanned in the cloud) in the following ways:
  - Because it is on the local Comodo White List of known safe applications
  - Because the user has rated the file as 'Trusted' in the File List
  - Because the software publisher is rated as 'Trusted' in the Vendor List.
  - By the user granting the installer elevated privileges (CCS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CCS regards the installer and all files generated by the installer as safe)
- Additionally, a file is not sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See Active HIPS Rules for more details)
- Cloud Scanning

#### Step 1 - Comodo File Look-up Server (FLS)

- In order to try to establish whether a file is safe or not, CCS will first consult Comodo's File Look-Up Server (FLS) to check the latest signature databases:
  - A digital hash of the unrecognized process or file is created.
  - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures of the 'safe' files.
    - First, our servers check these hashes against the latest available black-list
    - If the hash is discovered on this blacklist then it is malware
    - The result is sent back to the local installation of CCS
  - If the hash is not on the latest black-list, it's signature is checked against the latest white-list
    - If the hash is discovered on this white-list then it is trusted
    - The result is sent back to local installation of CCS
    - The local white-list is updated
  - The FLS checks detailed above are near instantaneous.
  - If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'.

#### Step 2 - Vendor Rating

- If a file is still 'unrecognized' after FLS check up, CCS checks the rating of the software publisher.
  - 'Trusted' vendor rating CCS will award trusted status to the file.
  - 'Malicious' vendor rating CCS will award malicious status to the software file and place it in quarantine.
  - 'Unrecognized' vendor rating The file will keep its unknown status and is run in the container. The file is also sent to Valkyrie for analysis.

#### Step 3 - Valkyrie Analysis

 Applications that have neither file rating nor vendor rating are first contained then submitted to Valkyrie for analysis.

COMODO Creating Trust Online\*

- Unrecognized files uploaded to Valkyrie undergo a battery of static and dynamic analysis. At the end of the automated tests, files are analyzed by human experts for confirmation.
- Valkyrie returns its verdicts to CCS which will quarantine, allow or contain the file as appropriate.
- Click here to view Valkyrie online help guide

**Important Note:** In order for the software to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

- To allow communication with our FLSs:
  - IPs that need to be allowed:
    - 91.209.196.27
    - 91.209.196.28
    - 199.66.201.20
    - 199.66.201.21
    - 199.66.201.22
    - 199.66.201.25
    - 199.66.201.26
  - Ports that need to be allowed: 53 UDP and 80 TCP
  - Direction: Outgoing (Endpoints to FLSs)

### 6.7. File Rating Configuration

Click 'Settings' > 'File Rating' to open this interface.

- The file rating area lets you view and manage all trusted, malicious and unrecognized files.
- File ratings in CCS are obtained from our online file look-up service (FLS). This is a huge database of trust ratings of known files.
- When a file is first opened, CCS will consult the FLS to check the file's reputation on our global whitelist and blacklists.
- CCS will award 'Trusted' status to the file if:
  - The application is on our global whitelist of safe files.
  - The application has a 'Trusted' status in the CCS File List
  - The application is from a vendor rated as 'Trusted' in the Vendor List
- Trusted files are excluded from monitoring by HIPS reducing hardware and software resource use.
- Conversely, files which are on the blacklist of harmful files are given a status of 'Malicious'. These files are quarantined or deleted automatically.
- Files which are on neither the blacklist nor the whitelist are awarded 'Unrecognized' status.
- You can review unrecognized files in the File List interface ('Settings' > 'File Rating' > 'File List').
- You can also submit unknown files to Comodo for further analysis, or to run an on-demand file-lookup.

**Important Note**: In order to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

- FLS communication please allows the software to access the following IP addresses:
  - 91.209.196.27
  - 91.209.196.28

COMODO Creating Trust Online

- 199.66.201.20
- 199.66.201.21
- 199.66.201.22
- 199.66.201.25
- 199.66.201.26
- Allow ports 53 UDP and 80 TCP
- Direction: Outgoing (Endpoints to FLS)

The file ratings area lets you:

- Manually add files to the file list and assign them a rating.
- Submit unrecognized files for a file look-up, and view all files you have submitted previously.
- View and manage the vendor list, and assign trust ratings to vendors.
- Click 'Settings' on the CCS home-screen
- Click 'File Rating':

COMODO Advanced	Settings ? - □ ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>File Rating Settings</li> <li>File Groups</li> <li>File List</li> </ul>	Settings       ? - □ ×         File Rating Settings         ✓ Enable Cloud Lookup (Recommended)         △ Analyze unknown files in the cloud by uploading them for instant analysis (Privacy Policy)         ✓ Upload metadata of unknown files to the cloud         ✓ Do not show popup alerts         This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.         ✓ Rate applications according to their vendor rating
Submitted Files Vendor List ✓ Advanced Protection	<ul> <li>Trust files installed by trusted installers</li> <li>Detect potentially unwanted applications</li> <li>Automatically purge the file list from invalid records every 4 hour(s)</li> <li>The file list will be cleaned from records on files no longer existing on this computer. It will not affect records on quarantined files and files rated by administrators.</li> <li>Use proxy when performing cloud lookup</li> <li>Automatically scan unrecognized files and re-evaluate quarantined files at equal intervals Edit scan options</li> </ul>
	OK CANCEL

Click the following links to jump to the section you need help with:

- File Rating Settings Configure settings that govern the overall behavior of file rating.
- File Groups Create predefined groups of one or more file types.
- File List View, manage and investigate executable files on your computer and their current trust rating.
- Submitted Files View any files already submitted to Comodo for analysis.

COMODO Creating Trust Online\*

 Vendor List - View and manage the list of software publishers. Manually add vendors and assign trust ratings to them.

### 6.7.1. File Rating Settings

- Click 'Settings' > 'File Rating' > 'File Rating Settings'
- A file rating determines how CCS 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 container until they get rated as trusted or untrusted.
- The rating of a file can change over time, especially in the case of 'unknown' files. For example, an 'unknown' file might be re-classified as 'trusted' or 'untrusted' after it has been tested.
- You can also configure whether CCS should auto-upload unknown files to Comodo for analysis.

#### Open the 'File Rating Settings' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Rating Settings'

• General Settings   • Antivirus   • HIPS   • Containment   • File Rating   • File Rating   • File Rating Settings   • File Rating Settings   • File Rating Settings   • File Rating Settings   • Vulpoad metadata of unknown files to the cloud   • O not show popup alerts   • This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.   • Antivitus   • Antivitus   • Antivitus   • Antivitus   • List   • Submitted Files   • Vendor List   • Antivitus   • Antivitus   • Antivitus   • Antivitus   • Antivitus   • O protection   • Antivitus   • Antivitus   • O protection   • Antivitus   • Antivitus	COMODO Advanced	Settings ? - 🗆 🗙		
<ul> <li>File Rating</li> <li>Privacy Policy)</li> <li>File Rating</li> <li>Upload metadata of unknown files to the cloud</li> <li>File Rating Settings</li> <li>Do not show popup alerts</li> <li>This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.</li> <li>File List</li> <li>Submitted Files</li> <li>Vendor List</li> <li>Advanced Protection</li> <li>Automatically purge the file list from invalid records every 4          <ul> <li>hour(s) ▼</li> <li>The file list will be cleaned from records on files no longer existing on this computer. It will not affect records on quarantined files and files rated by administrators.</li> <li>Use proxy when performing cloud lookup</li> <li>Automatically scan unrecognized files and re-evaluate quarantined files at equal</li> </ul> </li> </ul>	✓ Antivirus	Enable Cloud Lookup (Recommended)		
File List	- File Rating	( <u>Privacy Policy</u> ) ✓ Upload metadata of unknown files to the cloud		
	File Groups       ✓ Do not show popup alerts         File Groups       This option, when enabled, automatically applies 'Block and Terminate' action to madetected by cloud scanning.         File List       ✓ Rate applications according to their vendor rating         Submitted Files       ✓ Trust files installed by trusted installers         Vendor List       ✓ Detect potentially unwanted applications         Advanced Protection       ✓ Automatically purge the file list from invalid records every 4 in hour(s)         The file list will be cleaned from records on files no longer existing on this computer will not affect records on quarantined files and files rated by administrators.         Use proxy when performing cloud lookup         Automatically scan unrecognized files and re-evaluate quarantined files at equations			

- Enable Cloud Lookup CCS checks a file's trust rating on our cloud severs as part of the real-time scan process.(*Default and recommended =Enabled*)
- Analyze unknown files in the cloud by uploading them for instant analysis CCS uploads files with an 'unknown' trust rating to Comodo for further analysis. Our experts will analyze the file, award it a trust rating, and add it to the global whitelist or blacklist as appropriate. (*Default = Disabled*)

COMODO Creating Trust Online\*

- Upload metadata of unknown files to the cloud Metadata is basic file information such as file source, author, date of creation and so on. If enabled, CCS will also send the file metadata when uploading unknown files to Comodo. (Default = Enabled)
- **Do not show popup alerts** Whether or not CCS should show an alert when malware is detected by the cloud scanner (FLS). (**Default = Enabled**)
  - Enabled No alerts are shown. This minimizes disturbances but at some loss of user awareness. CCS will automatically block and guarantine the threat.
  - **Disabled** A rating scanner alert is shown for malicious files.

COMODO Rating Scanner Alert	?
Policy.User@F@1	
Location:C:\Suspicious\AntiTest\AntiTest.exeMore information:Unavailable	
Clean (Recommended) Quarantines the file	
Ignore Ignores the alert and allows the file operation	$\sim$
	Show Activities

You can choose from these actions:

- Clean The program is blocked and quarantined
- **Ignore** Allows the file to run. Does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:

(!)	Ignore Ignores the alert and allows the file operation	
0	Ignore Once	
0	Ignore and Add to Exclusions	
0	Ignore and Report as False Alert	
		Show Activities

- Ignore Once The file is allowed to run this time, but it will still be flagged as a threat by future scans.
- Ignore and Add to Exclusions The file is allowed to run this time, and will not be flagged as a threat in future scans. The file is placed on the Exclusions list, meaning it is ignored

COMODO Creating Trust Online\*

permanently by the scanner.

- Ignore and Report as a False Alert The file is allowed to run this time, and submitted to Comodo for analysis. Select this option if you think the file is safe, and that CCS was wrong to flag it as a threat. Comodo will re-examine the file.
- Rate applications according to their vendor rating CCS will give files the same rating as the trust rating
  of the publisher (software creator). For example if the vendor is trusted, then all files created by the vendor
  will be trusted. (*Default =Enabled*)
  - The vendor is the software company who created and digitally signed the file.
  - You can view vendor trust ratings in 'Advanced Settings' > 'File Rating' > 'Vendor List'.
  - CCS ships with a list of vendors with 'Trusted' status. You can add new vendors to the list and set your own vendor ratings as required.
  - The vendor rating priority is shown below:
    - Admin
    - User
    - Comodo
  - Click the 'Vendor Rating' link to open the 'Vendor List' screen. See Vendor List for more details.
- Trust files installed by trusted installers CCS awards trusted status to files whose parent applications are listed in the 'Installer or Updater' rule in HIPS Rules. (*Default = Enabled*)
- Detect potentially unwanted applications (PUA) CCS scans will flag applications that:

(i) a user may or may not be aware is installed on their computer

(ii) may contain 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 that tells you the weather may also contain code that tracks your online activity (*Default = Enabled*).

- Automatically purge unrecognized files every NN hour(s) CCS periodically checks that all unrecognized files in the list are still installed at the path specified. If not, the file is removed from the list. Select the interval in hours from the drop-down box. (*Default = Enabled, 4 Hours*)
- Use proxy when performing Cloud Lookup CCS submits files to FLS for analysis through a proxy. The
  proxy server is same one that is defined for program and database updates.
  - See 'Configure Program and Virus Database Updates' for more details. (Default = Disabled)
- Automatically scan unrecognized files and re-evaluate quarantined files at equal intervals CCS can
  periodically re-scan unknown and quarantined files to check whether a new trust rating is available for
  them. (Default = Enabled and set for every 4 hours)
  - Click 'Edit Scan Options' to configure the scan settings and schedule.

? COMODO Scan × Unrecognized and Quarantined Files Scanning Scan Name: Define items to be scanned, scanning options and running schedule OPTIONS ITEMS SCHEDULE Profile Unrecognized Files Quarantined Files ОК CANCEL

- Scan Name The label of the scan. This is pre-configured and cannot be edited.
- **Items** The files that are scanned by the profile. 'Unrecognized' and 'Quarantined' files are the defaults. You cannot edit or add files to this profile.
- Scan Options Configure scan technologies, how to handle threats, and more. See Configure scan options for the profile in Scan Profiles for help with this.
- Schedule Specify the frequency of the automated scans. See Configure a scan schedule in Scan Profiles for help with this. (*Default = Every 4 hours*).
- Click 'OK' to save your changes
- Click 'OK' in the 'Advanced Settings' screen for your settings to take effect.

### 6.7.2. File Groups

- Click 'Settings' > 'File Rating' > 'File Groups'
- As the name suggests, a file group is a collection of one or more file types. For example, the 'Executables' group is a list of file types that can run code on your computer.
- Once created, file groups can be named as the target of a rule in other areas of CCS. This makes it easy to add an entire class of files to exclusions, HIPS rules, firewall rules, containment rules and more.
- CCS ships with a set of predefined file groups. You can also create your own groups and edit existing groups as required.

#### Open the 'File Groups' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Groups'

ting Trust Online

Creating Trust Online\*

COMODO Advance	d Settings ? — 🗆	×
<ul><li>General Settings</li><li>Antivirus</li></ul>	File Groups	
<ul><li>✓ HIPS</li><li>✓ Containment</li></ul>	🕂 🗶 🗱 💬 Add Edit Remove Purge	
- File Rating	File Groups	a ^
File Rating Settings	Executables	
File Groups	🗌 🗈 🗄 All Applications	
File List	🔲 🖽 Windows Updater Applications	
Submitted Files	🔲 🖻 🗄 Windows System Applications	
Vendor List	🗌 🗈 🗄 Windows Management	
<ul> <li>Advanced Protection</li> </ul>	🔲 🖽 3rd Party Protocol Drivers	
	🗌 🖻 🗄 Metro Apps	
	🗌 🖆 🗄 Email Clients	
	□ 🗈 🗄 File Archivers	
	OK CANCEL	

#### Search Option:

• Click the search icon at upper-right and enter the name of a file group in full or part.

#### Controls:

The buttons at the top provide the following options:

- Add Create a new file group. Add files, folders or running processes to an existing group.
- Edit Rename a group. Change the file path of items in a file group.
- **Remove** Delete a file group, or specific items in a group.
- **Purge** Runs a check to verify that all files in a group are actually installed at the path specified. If not, the file or file group is removed from the list.

See the following links if you need more help:

- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

#### **Create a File Group**

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File Groups'
- Click the 'Add' button and select 'New Group':

COMODO Creating Trust Online\*

File	Groups					
+ Add	🗶 Edit	X Remove	ච Purge			
New Gr Files Folders Runnin	Ð	5				Q 1
			roperty		?	×
	Choose File G My Confident	-				
				ОК	CANCEL	

• Create a label for the file group and click 'OK'.

The new group will be added and shown in the list:

COMODO Advanced	Settings	? – 🗆 X
✓ General Settings	File Groups	
✓ Antivirus		
✓ Firewall	+ 🗶 🗙 O	
✓ HIPS	Add Edit Remove Purge	
✓ Containment	File Groups	۹ ^
– File Rating	🔲 🗈 Email Clients	
File Rating Settings	🔲 🖻 🗄 Suspicious Locations	
File Groups	□ 🗄 🗄 Shared Spaces	
File List	□ 🗈 🗄 File Downloaders	
	🗌 🗈 🗄 Media Players	
<	My Confidential Files	
	ок	CANCEL

#### Add files or folder to a group

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File Groups'
- Select the group from the list

•

- Click the 'Add' button > Choose from 'Files', 'Folders' or 'Running Processes'
  - Add individual files or folders
    - Choose 'Files' or 'Folders' from the 'Add' drop-down menu.

General Settings				
Antivirus	File Groups			
Firewall	+ / ×	Ð		
HIPS	Add Edit Remove	Purge		
Containment	New Group			Q
· File Rating	Files Trans			
File Rating Setting	Running Processes			
File Katiliy Setting	s Locations			
File Groups	🔲 🖾 🖽 Shared Spaces			
File List				
🔄 Open			×	
Copen Look in	: 🔄 old man files 🗸 🗸	③	×	
	: old man files ~	<ul> <li>Image: Image: Im</li></ul>	X Type	
Look ir				
	Name	Date modified	Туре	
Look ir	Name BITStester give_a_dog_a_bone give_a_dog_a_bone	Date modified 25-02-2008 11:33	Type Compress OpenDoci Text Docu	
Look ir Quick access	Name BITStester give_a_dog_a_bone	Date modified 25-02-2008 11:33 10-06-2011 15:01	Type Compress OpenDoci	
Look ir	Name BITStester give_a_dog_a_bone give_a_dog_a_bone	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19	Type Compress OpenDoci Text Docu	
Look ir Quick access	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu	
Look ir Quick access	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00	Type Compress OpenDoci Text Docu Compress OpenDoci	
Look ir Quick access	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knack	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu	
Look in Quick access Desktop	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knack knack knick	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci	
Look in Quick access Desktop	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knack knick knick	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:18	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci Text Docu	
Look in Quick access Desktop	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knick knick paddy_whack	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci Text Docu OpenDoci	
Look in Quick access Desktop Libraries	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knick hnick paddy_whack paddy_whack	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:19	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci Text Docu OpenDoci Text Docu	
Look in Quick access Desktop Libraries This PC	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knick paddy_whack ProcX	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:19 14-02-2008 15:37	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci Text Docu OpenDoci Text Docu Compress	
Look in Quick access Desktop Libraries	Name BITStester give_a_dog_a_bone give_a_dog_a_bone keylogtest knack knack knick paddy_whack ProcX sss	Date modified 25-02-2008 11:33 10-06-2011 15:01 12-11-2010 12:19 01-02-2008 13:53 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:18 10-06-2011 15:00 12-11-2010 12:19 14-02-2008 15:37	Type Compress OpenDoci Text Docu Compress OpenDoci Text Docu OpenDoci Text Docu OpenDoci Text Docu OpenDoci Text Docu Compress Compress	

• Navigate to the file or folder you want to add to the group. Click 'OK'

COMODO Creating Trust Online\*

🗄 Media Players	
My Confidential Files	
— C:\old man files\give_a_dog_a_bone.exe	
— 📧 C:\old man files\knack.exe	
— 📧 C:\old man files\knick.exe	
C:\old man files\paddy_whack.exe	
	~
OK CANCEL	

Repeat the process to add more files or folders.

### Add an application from a running process

- Click the 'Add' button then 'Running Processes'
- This opens a list of processes currently running on your computer:

COMODO Creating Trust Online

+     ✓     ★     ↔       Add     Edit     Remove     Purge		
New Group	a	^
Files Folders e Downloaders		
Running Processes		
E Containment Folders		
	?	>
CHICDO BIOWSE IOI PIOCESSES	e Downloaders g Processes ers Containment Folders Containment Folders ? PID PID PID PID Cis.exe 4204 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4312 Cis.exe 4324 Cis.exe 4324 Cis.exe 4322 Cis.exe 4324 Cis.exe 4322 Cis.exe Cis.	
Application	PID	
	4204	1
	4712	
	2580	
▲ III taskhostw.exe	3932	
v svchost.exe	1008	
▲ 🖉 ctfmon.exe	3924	
svchost.exe	1168	
svchost.exe	108	
<ul> <li>svchost.exe</li> </ul>	260	
svchost.exe	1660 844	
svchost.exe		

- Select the desired process. The parent application of the process will be added to the group.
- Click 'OK'.

### Edit an item in the 'Files Groups' list

• Select the item from the list and click the 'Edit' button. The 'Edit property' dialog is shown:

Creating Trust Online\*

COMODO Edit property		?	×
Edit File Path C:\Windows\System32\RuntimeBroker.ex	xe		
	ОК	CANCEL	

• Edit the file path if required and click 'OK'.

### Delete a file group, or an individual file from a group

• To remove a file group, select it from the list and click the 'Remove' button.

	File Groups	
+ Ado	d Edit Remove Purge	
	File Groups Q	^
	🖾 🖽 Suspicious Locations	
	🗈 🗄 Shared Spaces	
	🗈 🗄 File Downloaders	
	🗈 🗄 Pseudo File Downloaders	
	File Archivers	
	🖾 🗄 Sandbox Folders	
	🖾 🗄 Browser Plugins	
	🗈 🗄 Media Players	
	🗈 🗄 My Confidential Files	~
	OK CANCEL	

- To remove an individual file from a group expand the group by clicking '+' at the left of the group, select the file to be removed and click the 'Remove' button.
- Alternatively, right-click on a file and choose remove from drop-down menu.

COMODO Creating Trust Online\*

### 6.7.3. File List

Click 'Settings' > 'File Rating' > 'File List'

The file list is an inventory of executable files and applications discovered on your computer. The list also shows the file vendor, the date the file was discovered, and the file's trust rating.

CCS rates files as:

- **Trusted** the file is safe to run outside the container.
- Unrecognized no trust-rating was found for the file, so it will be run in the container.
- Malicious the file is known malware and will be quarantined or deleted.

### **Trusted Files**

Files can be awarded a 'Trusted' status in the following ways:

- Cloud-based file lookup service (FLS) When a file is first opened, CCS will check the file's reputation on our global whitelist and blacklists. It will award trusted status if the file is on the global whitelist of safe files.
- Vendor rating The application is from a software publisher who has a 'Trusted' status in the Vendor List.
- Administrator rating Admins can elect to trust files on a local endpoints and networks. Only applies if
  your CCS installation is remotely managed by an administrator.
- User Rating You can manually assign a trusted rating to a file as follows:
  - Click 'Settings' > 'File Rating' > 'File List'
  - Select the target file then click the 'File Details' button
  - Click the 'File Rating' tab
  - Click the 'Rate Now' link
  - Set the rating as 'Trusted'
  - Click 'OK'
  - See change the file rating in File Details if you want more help on this.

### **Unrecognized Files**

- Once installed, HIPS monitors and verifies all file activity on your computer.
- Every new executable file is first scanned against the virus blacklist (known 'bad' files) and the file whitelist (known 'good' files).
- If the file is on neither list it is given an 'Unrecognized' file rating.
- Any executable that is modified is also given 'Unrecognized' status. This protects you against malware changing the behavior of a previously trusted application.

You can review pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be given a 'Trusted' rating. See 'Change the file rating' for more details. You can also submit files to Comodo for analysis. Experts at Comodo will test the files and add them to global white-list or black-list accordingly.

### **Malicious Files**

Files identified as malware are given a 'Malicious' rating, and are blocked and quarantined.

### Open the 'File List' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File List'

COMODO Creating Trust Online\*

COMODO Advanced	Settings	? — 🗆
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	File List View details and manage rating of known executables. Show files Executables  Quarantined and not quarantine	ed 🔻
<ul> <li>Containment</li> <li>File Rating</li> </ul>	🕂 🧟 🗰 Q 🗸	ビコ の t Exchange Purge
File Rating Settings	☐ ▼ File path Q Company Q First Observ	
File Groups	C:\Users\giri1\A Microsoft Cor 5/15/2019 1	1:02:50 A 🗸 <u>Trusted</u>
File List	C:\Users\giri1\A Microsoft Cor 5/15/2019 1	:04:53 PM 🗸 <u>Trusted</u>
Submitted Files	C:\Users\giri1\A Google LLC 5/16/2019 1	:36:36 PM 🗸 <u>Trusted</u>
Vendor List	C:\Suspicious\ Valeriy Sokolov 5/24/2019 1	2:42:26 PM ? Unrecognized
<ul> <li>Advanced Protection</li> </ul>	C:\Suspicious\w 5/24/2019 1	2:37:47 PM ? Unrecognized
	C:\Suspicious\h Threatstar B.V. 5/24/2019 1	2:37:15 PM 🗸 <u>Trusted</u>
	C:\Suspicious\A 5/24/2019 1	2:11:20 PM 🚷 Malicious
	C:\ProgramData Microsoft Cor 5/15/2019 1	0:55:52 A 🗸 <u>Trusted</u>

The file list shows applications and executable files discovered on your computer.

- File Path The location of the file on your computer
- · Company The software vendor that published/created the file
- First Observed Date and time at which the file was first discovered by CCS.
- File Rating Current trust rating of the file. The possible values are:
  - Trusted
  - Unrecognized
  - Malicious

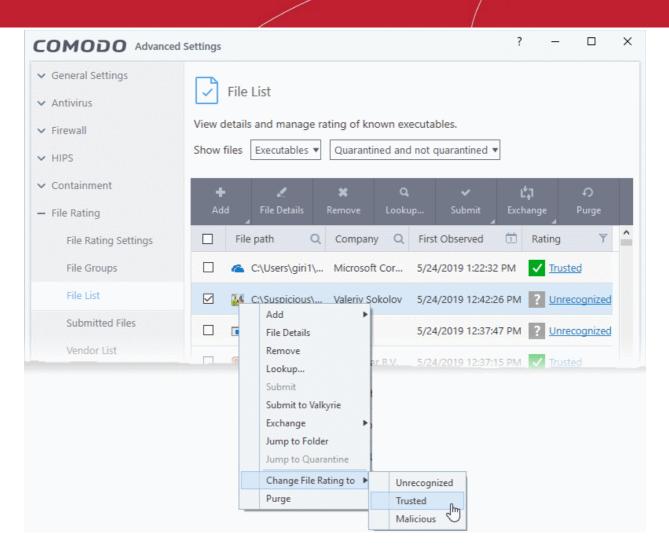
Files are rated based on the following, in order of priority:

- 1. Administrator rating Rating set by the administrator who remotely manages your CCS installation.
- 2. User rating A rating that you or another user awarded to a file.
- 3. FLS rating The rating of the file on Comodo's online file look-up service (FLS).

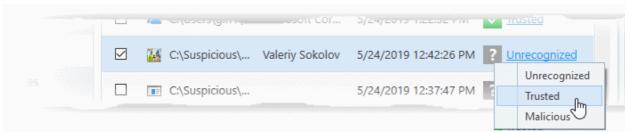
There are three ways you can set user rating for a file:

- 1. Right-click on a file in the file list
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Right-click on a file > Select 'Change File Rating to' > Choose a new rating:

COMODO



- 2. In the file rating column
- Click on the rating of a file in the 'Rating' column
- Choose a new rating from the options:



- 3. From the 'File Details' dialog
- Select a file in the file list
- Click the 'File Details' button at the top
- Click the 'File Rating' tab
- Click the 'Rate Now' link
- Set the rating as required
- Click 'OK'

#### **Context Sensitive Menu**

• Right-click on a file to open a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.

Creating Trust Online\*

O Advanced S	Settings					?	- 0	×
		List s and manage Executables	_		utables. not quarantined v	Ŧ		
	+ Add	File Details	X Remove	Q, Lookup	Submit	L <b>1</b> Exchange	€ Purge	
Settings	Fi	ile path	Q Compa	ny Q	First Observed	🗇 Rati	ng	<b>Y</b> ^
		C:\Suspicious\	h Threatst	tar B.V.	5/24/2019 12:37	7:15 PM 🗸	Trusted	
		C:\S Add			5/24/2019 12:37	7:47 PM ?	Unrecognized	₫
		Rem Lool Subr Subr Exch Jum	kup mit mit to Valkyrie lange p to Folder p to Quarantine nge File Rating		5/24/2019 12:42	2:26 PM <b>?</b>	Unrecognized	

- · Add Manually add a file to the list and specify its trust rating
- File Details View information about the selected item. You can also set the file rating from here.
- Remove Delete files from the list.
- Lookup Check the file-lookup server for more details about the file, including the latest trust rating.
- Submit to Valkyrie Upload an item to Valkyrie, Comodo's file analysis system.
- Exchange Consists of two options (Import and Export).
  - Import Add files to the list from an XML file
  - Export Save the current list as an XML file
- Jump to Folder Opens the folder containing the file in Windows Explorer.
- Jump to Quarantine Opens the 'Quarantine' interface of CCS to view or restore the file. Available only for items moved to quarantine. See Manage Quarantined Items for more details.
- Change File Rating to Set user defined trust rating to the file.
- Purge Check that all files in the list are still installed at the path specified. If not, the file is removed from the list.

### Sort, search and filter options

#### Sort option

 Click any column header to sort the items in alphabetical / ascending / descending order of entries in that column

COMODO Creating Trust Online\*

#### Search options

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and 'File rating'.

• Click the search icon at the far right in the 'File path' and/or 'Company' column header.

+ Add	File Details	X Remove	Q Lookup	Submit	<b>압</b> 귀 Exchange	Purge
	Search	x - Q	×	First Ob:	served 🗇	Rating

• Enter the file path and/or the name of company in part or full as per the selected criteria in the search field The result for the entered criteria will be listed automatically. Click the 'X' icon to clear the search criteria and display all the items again in the list.

#### **Filter options**

- The 'Show files' filters on the top lets you select whether you want to view only executables, non executables, or all files:
- The 'Show files' filters on the top lets you select whether you want to view only executables, non executables, or all files:

COMODO Advan	ced Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	File List				
✓ Firewall	View details and manage rating of known executables.	- 4 -			
✓ HIPS	Show files Executables V Quarantined and not quarantine	ed 🔻			
✓ Containment	+ Non-executa s a v	t:	1	ຄ	

- Select the file type from the drop-down on the left
- Select whether you want to view only items moved to quarantine, items not moved to quarantine, or all files:

COMODO Advanced	l Settings		?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	File List View details and manage ra Show files Executables 🔻	ting of known executables.				
		Quarantined Not quarantined Quarantined and not quarantined			^	

COMODO Creating Trust Online\*

- Only the items that meet the criteria chosen from the filters are shown in the file list.
- Click the calendar icon at the right of the 'First Observed' column
- Choose the time period you require
- This will show only those files discovered in the time-frame you set:

igs		File Details	Remove	Q. Lookup	Submit	Exchange	<b>ि</b> Purge	
		Search 🗙	- Q.S	earch 🗙	First Obs	erved 団	Rating	'
		C:\Windows\Sy	rs, 💿 (No fi	Itering)			✓ <u>Trusted</u>	
		C:\Windows\Sy	O Within			nour(s) 🔻	Trusted	
	<b>D</b> . 6						Tructor	
			O Curre	ent week				
			O Curre	ent month				
			O Within	n the period of				

Click the funnel icon at the right of the 'File Rating' column to filter files by rating:

	+) Purge	L <sub>∲</sub> I Exchange ⊿	Submit	Lookup	Remove	File Details	
1	Rating	erved 🗇	First Obs	earch 🗙		🗙 Search 🛛 🗙	
ed	Trust	9 1:06:53 PM	5/15/201	oft Windows	Microso	C:\Windows\Sys	
ognized							
ous	Malic						

#### **Control Buttons**

The buttons at the top provide the following options:

	+ Add	K. File Details	<b>X</b> Remove	Q. Lookup	. Submit	<b>Ľ‡</b> ] Exchang	Purge ⊿	
ngs	E F	File path 🛛 🤇	🔍 🔻 Compa	ny Q	First Observed	1	Rating	Y

- Add Manually add files to the 'File List' with user defined rating
- File Details View the information about the selected item. You can also set user defined rating to the selected file

#### COMODO Creating Trust Online\*

### Comodo Client Security - User Guide

- Remove Delete files from 'File List'.
- Lookup... Check the details of the selected file from the master Comodo safelist
- **Submit to Valkyrie** Uploads selected files to Valkyrie for behavior analysis. Valkyrie is Comodo's file testing and verdicting system.
- Exchange Consists of two options (Import and Export).
  - Import Fetch the files from a file list saved as an XML file
  - Export Save the current file list with existing ratings as an XML file
- **Purge** Runs a system check to verify that all the files for which the ratings are listed are actually installed on the host machine at the path specified. If not, the fie is removed from the list.

#### Manually add files to 'File list'

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Add' button at the top

+		×
Add 🛄	File Details	Remove
Files		Q
Folders		
Running	Processes	iles (x86)\
	C:\Program F	iles (x86)\

Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

You can add three types of items:

- Files Browse to the file you want to add and assign a rating.
- Folders Browse to the folder you want to add an assign a rating. All files in the folder will inherit the rating you gave to the folder.
- Running Processes Select a currently active process and assign a rating. The parent application of the
  process will be added to the file list with the rating you assign.

#### View the 'File Details' and change the rating

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select a file and click the 'File Details' button.

COMODO Creating Trust Online\*

File	List
View detail	s and manage rating of known executables.
Show files	Executables <b>v</b> Quarantined and not quarantined <b>v</b>
+	メ Q Y は、 の
Add	File Details Remove Lookup Submit Exchange Purge
E File	e path Q 🗸 Company Q First Observed 🛅 Rating 🍸 🏠
	C:\Suspicious\ Valeriy Sokolov 5/24/2019 12:42:26 PM 💽 Unrecognized
	C:\Suspicious\ Threatstar B.V. 5/24/2019 12:37:15 PM 🗸 <u>Trusted</u>
	V
	COMODO File Details ? ×
	OVERVIEW FILE RATING
	File Name: WorkingTimeManagerSetup.exe Jump to Folder
	File Rating: Unrecognized
	First Observed: 5/24/2019 12:42:26 PM
	Last Quarantined: (n/a)
	Certificate Signer: Valeriy Sokolov
	Origin: (unknown)
	Created by: System File Hash (SHA-1): 5C7EBFA561269F2AD4DE783B3281AF1AAE274B0E
	Reset COMODO Info
	OK CANCEL

**Tip**: Alternatively, right click on the selected file and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog has two tabs:

Overview

COMODO Creating Trust Online\*

#### • File Rating

### **Overview**

The 'Overview' tab shows general details such as the file rating, discovery date, hash value and publisher (signer):

OVERVIE	W FILE RATING
File Name: WorkingTime	-ManagerSetup.exe
File Rating:	Unrecognized
First Observed:	5/24/2019 12:42:26 PM
Last Quarantined:	(n/a)
Certificate Signer:	Valeriy Sokolov
Origin:	(unknown)
Created by:	System
File Hash (SHA-1):	5C7EBFA561269F2AD4DE783B3281AF1AAE274B0E
	Reset COMODO Info

- Click the file name to open the Windows 'File Properties' dialog.
- Click 'Jump to folder' to open the folder containing the file in Windows Explorer, with the respective file selected.
- Click 'Reset COMODO Info' to refresh the information from Comodo FLS database

### File Rating

• Shows the file's current trust rating from Comodo and lets you set your own rating:

COMODO Creating Trust Online\*

DMODO File Details	? ×
OVERVIEW	FILE RATING
Final Rating:	Unrecognized
Provider Date	File Rating
Administrator	? Unrecognized
User	? Rate Now
Comodo	? Unrecognized

**Note**: If your CCS installation is remotely managed by Endpoint Manager, your administrator's file rating for individual file will override your user file rating.

#### Change the user rating of the file

- Select the file from the 'File List' pane and click the 'File Details' button
- Click the 'File Rating' tab
- Click the 'Rate Now' link and choose the rating from the drop-down:

	e Details		? ×
OVERVIEW	_	FILE RA	TING
Final Rating:			Unrecognized
Provider	Date	File R	ating
Administrator		? เ	Inrecognized
User			tate Now
Comodo		?	Unrecognized Trusted Malicious
		ОК	CANCEL

The options available are:

- Trusted The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- **Unrecognized** The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- Malicious The file will be deleted or placed in quarantine and will not be allowed to run.
- Click 'OK' in the 'Files Details' dialog

Tip: Alternatively, right click on a file then choose 'Change File Rating to'

• Click 'OK' in the 'Advanced Settings' interface to save your settings.

#### Remove files from the file list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be removed
- Click the 'Remove' button at the top. The file(s) is / are only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a file then choose 'Remove' from context sensitive menu.

• Click 'OK' for your changes to take effect.

#### Perform an online lookup for files

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be checked from the 'File list' pane.

COMODO Creating Trust Online\*

• Click the 'Lookup...' button at the top from the 'File list' pane.

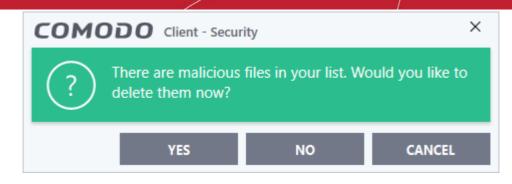
**Tip**: Alternatively, right click on a file then choose 'Lookup' from the context sensitive menu.

Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.

	Show files Executables  Quarant	tined and not quarantined 🔻
	+ 🧖 🗱 Add File Details Remove	Q ✓ Ľ₁ ↔ Lookup Submit Exchange Purge
tings	File path Q Comp.	any 🛛 First Observed 📋 Rating 🍸 ^
	C:\ProgramData Micros	soft Cor 5/15/2019 10:55:52 A 🗸 <u>Trusted</u>
	C:\Suspicious\A	5/24/2019 12:11:20 PM 🔗 Malicious
	🗹 🌋 C:\Suspicious\h Threat	star B.V. 5/24/2019 12:37:15 PM 🗸 <u>Trusted</u>
	C:\Suspicious\w	5/24/2019 12:37:47 PM ? Unrecognized
tion	🗹 🔣 C:\Suspicious\ Valeriy	Sokolov 5/24/2019 12:42:26 PM ? Unrecognized
	- CAllsore airitA - Google	e UC 5/16/2010 1/26/26 DM 🗸 Tructed
сомо		
100		rst.exe
File Name		Rating
WorkingT	imeManagerSetup.exe	? Unrecognized
wildfire-te	est-pe-file.exe	? Unrecognized
🎕 hmpalert-	test.exe	✓ Trusted
🛯 <u>AntiTest.e</u>	<u>xe</u>	() Bad - CloudScanner.Fls.File
× CLOSE		SEND TO BACKGROUND

If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.

COMODO Creating Trust Online\*



- Click 'Yes' to permanently delete the malicious file(s) from your computer.
- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. See the description of **changing the file rating** under the section **File Details** for more details.
- If no information is available, it will be indicated as 'Needs to be submitted' with a yellow icon. You can submit the file to Comodo for analysis from the dialog that appears on closing the 'Lookup' dialog. See **explanation below** for more details.

#### Manually submit files to Valkyrie

Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be submitted from the 'File List' pane.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

**Tip**: Alternatively, right click on a file then choose 'Submit to Valkyrie' from the menu.

You can view the list of files you submitted so far, from the **Submitted Files** panel.

#### Export and Import the File List

You can save the list of files with their currently assigned ratings to an XML file and store it in a safe place. This is useful to restore your list if you have to uninstall/reinstall CCS, or if you want to implement the same list on another machine that has CCS installed.

#### Export the File List

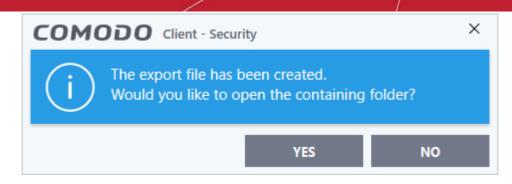
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Exchange' button at the top of the 'File List' pane then select 'Export' from the menu

**Tip**: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Export'

• Navigate to where you want to store the exported list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.

COMODO Creating Trust Online\*



### Import a saved file list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Exchange' button then select 'Import' from the menu

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Import'

• Navigate to the location of the XML file containing the file list and click 'Open'.

The 'File List' will be populated as per the imported 'File List'.

### 6.7.4. Submitted Files

- Click 'Settings' > 'File Rating' > 'Submitted Files'
- The 'Submitted Applications' area lets you review and manage the files that you have uploaded to Comodo Valkyrie for analysis.
- Valkyrie is Comodo's file testing and verdicting system.
- You can submit suspicious files, files with an 'unknown' trust rating, or false-positive files (those files you feel CCS has incorrectly identified as malware).
- After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.
- After manual classification by Valkyrie, they will be added to global white or black list accordingly.

### Open the 'Submitted Files' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'Submitted Files' on the left:

COMODO Creating Trust Online\*

COMODO Advance	d Settings	?			×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Submitted Files				
<ul><li>HIPS</li><li>Containment</li></ul>	業 わ Clean Refresh				
- File Rating	Path C	Submitted		Submittee	d As
File Rating Settings	E:\CCAV\10-08-18\unknown2.exe	10/10/2018 4:10	:50 PM	Automate	d Ar
File Groups	E:\CCAV\10-08-18\unknown1.exe	10/10/2018 5:27	:29 PM	Automate	d Ar
Submitted Files	E:\CCAV\Not yet tested\blueberry.exe	10/8/2018 11:22	20 AM	Automate	d Ar
Vendor List	E:\CCAV\10-08-18\unknown3.exe	10/10/2018 4:12	:45 PM	Automate	d Ar
✓ Advanced Protection	E:\CCAV\10-08-18\New folder\pathping.exe	10/11/2018 11:1	5:36	Automate	d Ar
	E:\CCAV\10-08-18\unknown4.exe	10/10/2018 4:25	:48 PM	Automate	d Ar
	<			) Privacy P	
		ок		CANCEL	

- Path The location of the file on your computer
- Submitted Date and time the file was uploaded for analysis.
- **Submitted As** The status under which the file was uploaded. Examples include 'automated' and 'contained'.
- **Cloud Service** The name of the Comodo cloud service to which the files were submitted. This is usually the Valkyrie analytic system operated by Comodo.

The buttons at the top provide the following options:

ĺ	Sub	mitted Fi	es
	X Clean	ච Refresh	
-	Path		Q

- Clean Clears the list
- Refresh Reloads the list to add items that are submitted recently

COMODO Creating Trust Online\*

### 6.7.5. Vendor List

• Click 'Settings' > 'File Rating' > 'Vendor List'

There are three ways that a file can be treated as safe in CCS:

- The file is on the Comodo safe list (a global white-list of trusted software)
- The user has assigned 'Trusted' rating to the file in the CCS file list ('Settings' > 'File Rating' > 'File List')
- The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file.

With regards to vendor settings, CCS handles unknown files as follows:

- The file is allowed to run normally if:
  - The vendor rating is 'Trusted' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**
- The file is run in the container if:
  - The vendor rating is 'Unrecognized' AND you have enabled 'Rate applications according to their vendor rating' in File Rating Settings
  - The vendor is not in the vendor list (regardless of whether you have enabled 'Rate applications according to their vendor rating')
- The file is blocked and quarantined if:
  - The vendor rating is 'Malicious' AND you have enabled 'Rate applications according to their vendor rating' in File Rating Settings

### Vendor List

- CCS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CCS allows unknown files which are digitally signed by one of these vendors to run.
- Click 'Settings' > 'File Rating' > 'Vendor List' to view this list of trusted vendors.
- You can also add new vendors, and change the rating of existing vendors. The vendor rating priority is as follows:
  - Admin
  - User
  - Comodo
- Software publishers can get themselves added to trusted vendors by contacting Comodo with their software details. Click here to read more about this.
  - Click here if you want to read background information on digitally signing software

### Open the 'Vendor List' interface

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List':

COMODO Creating Trust Online\*

<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Ver	ndor List						
<ul> <li>HIPS</li> <li>Containment</li> </ul>	+ Add	Vendor Details	X Remove	Q. Lookuş	)			
- File Rating		ndor	Q Rate	ed By 🌱	Last Modified	Ċ	Rating	Y
File Rating Settings	Be	ijing Huahong	Int Com	iodo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
File Groups		B S.p.A.	Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
File List	Ва	idu Online Net	two Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
Submitted Files	Bo	psoft (Zaozhu	ang Com	iodo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
Vendor List	C cs	@amedtec.de	Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
<ul> <li>Advanced Protection</li> </ul>		JRKIN ADDON	S C Com	iodo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
	Ef	icient Learning	Sy Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
	E Fin	e Senses Educ	ati Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	
		el(R) Software	De Com	odo	12/14/2018 1:2	2:04 PM	✓ <u>Trusted</u>	

The interface allows you to:

- Add a new vendor to the list
- · View details of vendors and assign user rating
- Perform an online lookup for vendors
- Remove vendors from the list

#### **Column Descriptions:**

- Vendor The name of the software publisher
- **Rated By** The entity that assigned the rating you see in the 'Rating' column. This can be 'Administrator', 'User' or 'Comodo' rating.
- Last Modified Date and time the rating was most recently updated.
- Rating Current trust rating of the vendor. The possible values are:
  - Trusted
  - Unrecognized
  - Malicious
  - Click on the rating to assign a new rating
  - CCS obeys vendor ratings with the following priority:
    - Admin rating
    - User rating
    - Comodo rating

There are three ways you can set a vendor rating:

COMODO Creating Trust Online\*

#### 1. Right-click on a vendor in the 'Vendor List'

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Right-click on a vendor > Select 'Change File Rating to' > Choose a new rating:

<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Vendor List	X Q	ıp	
✓ Firewall	+ / Add Detail	X Q	ıp	
	Add Vendo Detail	I Parrana Lasku	ıp	
✓ HIPS	Add Detail		ıp	
	. Contractory and			
✓ Containment	Vendor	Q Rated By	Last Modified	Rating 🍸 ^
— File Rating	] VideoIQ	Comodo	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
File Rating Settings	VideoLAN	Comodo	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
File Groups	] Videology	Add  Vendor Details	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
File List	] VideoMos	Remove Lookup	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
	VIDEOPAR	Change File Rating to 🕨	Unrecognized PPM	✓ <u>Trusted</u>
Vendor List	] Videoship <del>os</del>	Reset User Rating	Trustel Malicious	Trusted

#### 2. In the file rating column

- Click on the rating of a vendor in the 'Rating' column
- Choose a new rating from the options:

COMODO Advanced	d Settings		?	? – 🗆 ?
✓ General Settings				
✓ Antivirus	Vendor List			
✓ Firewall	+ 🖉	<b>*</b> Q		
✓ HIPS	Add Vendor Details		p	
✓ Containment	Vendor	Q Rated By	Last Modified	Rating 🍸
- File Rating	Videodesk SA	Comodo	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
File Rating Settings	VideoEgg	Comodo	4/11/2019 1:58:10 PM	✓ <u>Trusted</u>
File Groups	VideoIQ	User	4/11/2019 1:58:10 PM	2 Unrecognized
File List	VideoLAN	Comodo	4/11/2019 1:58:10 PM	Unrecognized Trusted
				Malicious

### 3. From the 'File Details' dialog

- Select a vendor in the file list
- Click the 'Vendor Details' button at the top
- Click the 'Vendor Rating' tab
- Click the 'Rate Now' link beside 'User'

COMODO Creating Trust Online\*

- Set the rating as required
- Click 'OK'

### **Context Sensitive Menu**

• Right-click on a vendor to open a context sensitive menu that allows you to view the 'Vendor Details' dialog, assign a rating to a vendor, add / remove vendors, and more.

A III	Vendor List							
+ Ad		<b>X</b> Remove	Q. Lookup	ı				
	Vendor	Q Rated By	y 🍸	Last Modified	1	Rating	Y	^
	VideoEgg	Comodo	)	4/11/2019 1:58:1	0 PM	✓ <u>Trusted</u>		
	VideoIQ	Add	Þ	4/12/2019 2:26:4	3 PM	✓ <u>Trusted</u>		
	VideoLAN	Vendor Details Remove Lookup		4/12/2019 2:26:4	3 PM	✓ <u>Trusted</u>		
		Change File Ratin Reset User Rating	-					

- Add Manually add a new vendor to the vendor list. You can select an executable file or a currently running
  process to add the publisher who signed that file to the list.
- Vendor Details View the information about the vendor. You can also assign user defined trust rating to the vendor
- Remove Delete the vendor from the list
- Lookup... Check details of the vendor from the master Comodo trusted vendor list
- Change File Rating to Set user defined trust rating to the vendor
- Reset User Rating Clear user rating and reinstate Comodo rating

#### Controls

The buttons at the top provide the following options:

COMODO Creating Trust Online\*

1	Vendor List						
+ Ade	d Vendor Details	XX Remove	Q Looku	p			
	Vendor	Q Rated E	}y ₹	Last Modified	Ť	Rating	Y
	Videodesk SA	Comode	0	4/11/2019 1:58:1	0 PM	✓ <u>Trusted</u>	
	VideoFaa	Comod	0	4/11/2019 1:58:1	0 PM	✓ <u>Trusted</u>	

- Add Manually add a new vendor to the list. You can add a vendor by simply selecting a file or a running process. CCS will extract the publisher who signed the file/process.
- Vendor Details View information about the selected vendor. You can also set your own trust rating for the vendor from here.
- Remove Delete selected vendors from the list. You can only remove user-added vendors.
- Lookup... Check details of a vendor on Comodo's online trusted vendor list

#### Sort, Search and Filter options

- · Click any column header to sort the list in order of the entries in that column
- Click the search icon in the 'Vendor' column header to look for specific vendors
- Click the calendar icon in the 'Last Modified' column header to filter vendors by date modified:

<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	5	Vendor List					
<ul> <li>Firewall</li> <li>HIPS</li> </ul>	+ Ado	Vendor Details	× Remo		<b>Q</b> Lookup	<b>)</b>	
✓ Containment		Vendor	Q R	ated By	7	Last Modified	
- File Rating		Beijing Huaho	(No filt	tering)			
File Rating Settings		ABB S.p.A.	<ul> <li>Within</li> <li>Exception</li> </ul>			1 + hour(s)	
File Groups		Baidu Online I	O Today				
			O Currer	nt week			-
			O Currer	n <mark>t mont</mark> h			
				the perio		05/27/2019	

Click the funnel icon in the 'Rated By' / 'Rating' columns to filter vendors by trust rating, and by who
assigned the rating:

COMODO Creating Trust Online\*

COMODO Adva	nced Settings					?
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Ven	dor List				
<ul><li>✓ Firewall</li><li>✓ HIPS</li></ul>	+ Add	Vendor Details	X Remove	<b>Q</b> Lookup		
✓ Containment	□ Ver	ndor	Q Rated E	By 💎	Last Modified	🗂 Ratir
<ul> <li>File Rating</li> </ul>	🗌 Beij	ing Huahong	In Admini		<b>5/15/2</b> 019 10:5	4:38 AM

### Add a new vendor to the list

- You can add vendors simply by browsing to a file they have digitally signed
- CCS will read the vendor's signature from the file and add them to the list
- You can then assign your own rating to the vendor

There are two ways to add vendors:

- Specify an executable file on your local drive
- Select a currently running process

#### Add a vendor by reading the vendor's signature from an executable

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a signed executable'
- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a signed executable'

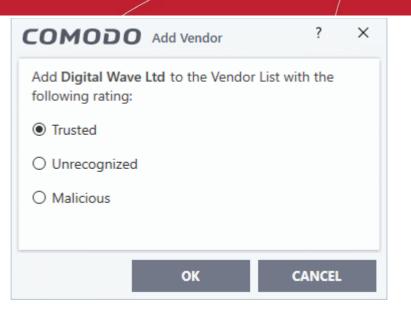
COMODO Creating Trust Online\*

OMODO Advance	d Settings		?
General Settings Antivirus	Vendor List		
Firewall HIPS	Add Vendor Remove	Q Lookup	
Containment File Rating	Read from a Running Cess	d By 🝸 Last Modifi odo 4/11/2019	
$\bigcirc$ Open $\leftarrow$ $\rightarrow$ $\land$ $\uparrow$ $\bigcirc$ « Lo	cal D > Program Files > 🗸 ඊ	Search Program Files	× م
Organize 🔻 New folde	er		
📃 Desktop 🛷 ^	Name	Date modified	Туре 🔨
👌 🦊 Downloads 🖈 🔤	Common Files	12-04-2018 05:08	File fol
🔮 Documents 🖈	соморо	11-04-2019 13:57	File fol
📰 Pictures 🛛 🖈	CUAssistant	12-04-2019 08:50	File fol
Music	internet explorer	12-04-2018 14:46	File fol
old man files	rempl	11-04-2019 17:05	File fol
	VideoLAN	12-04-2019 14:08	File fol
Suspicious	Windows Defender	12-04-2018 14:46	File fol
Videos	🣙 Windows Defender Advanced Threat	Pro 12-04-2018 14:51	File fol
💪 OneDrive	📙 Windows Mail	12-04-2018 05:08	File fol
	📙 Windows Media Player	12-04-2018 14:46	File fol
This PC	📙 Windows Multimedia Platform	12-04-2018 05:08	File fol
💣 Network	📙 windows nt	12-04-2018 05:08	File fol 🗸
~	<		>
File <u>n</u>	ame: 🔍 🗸	Executable Files (*.exe, *.e	dll, *.or ~
		<u>O</u> pen <mark>▼</mark> C	ancel

• Navigate to the executable file whose publisher you want to add to the vendor list and click 'Open'.

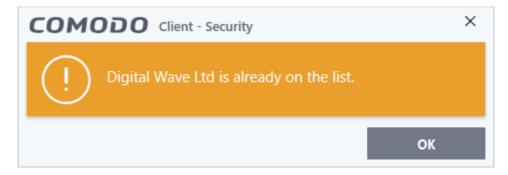
CCS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, you can add the vendor to the list by assigning your trust rating'.

COMODO Creating Trust Online\*

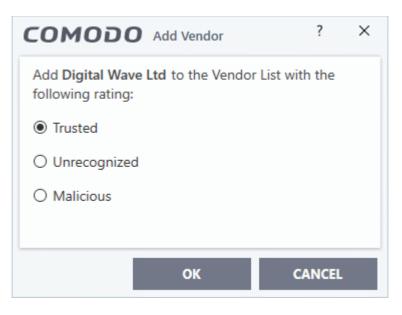


- Choose your rating and click 'OK'
- The vendor will be added to the list with your rating.

If the vendor is already on the list you will be notified:



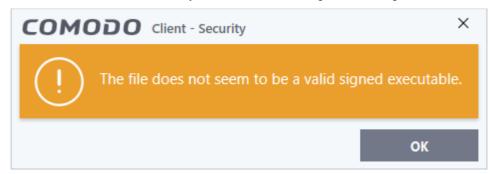
You can assign your own rating to the existing vendor:



- Choose your rating and click 'OK'
- The user rating for the vendor will be assigned as you set.
- If CCS cannot verify that the software certificate is signed by a Trusted CA then it does not add the software

COMODO Creating Trust Online\*

vendor to the vendor list. In this case, you can see the following error message.



### Add a trusted vendor from a currently running process

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a Running Process'
- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a Running Process'

COMODO Creating Trust Online\*

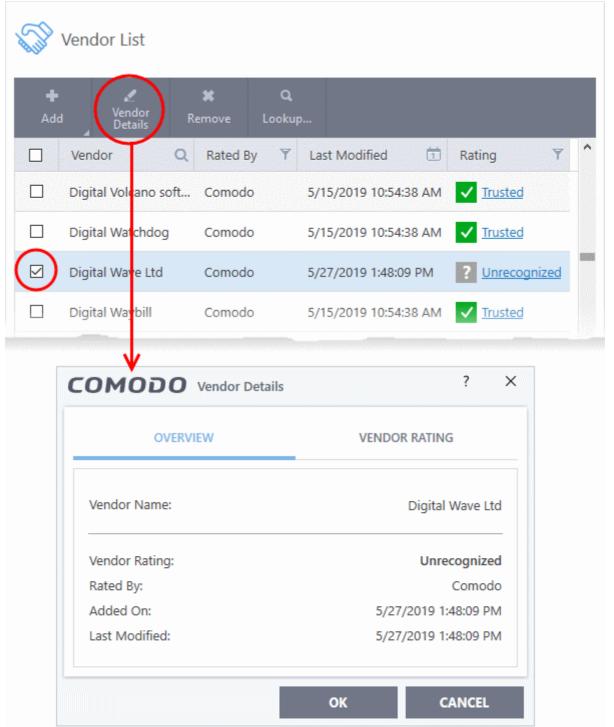
ieneral Settings Vendor List		
irewall 🔶 🗶 🗶	٩	
HPS Add Vendor Remove	Lookup	
Containment	3y 🍸 Last Modified	İ Ra
ile Rating	o 5/15/2019 10:54:38	
File Rating Settings ABB S. A Comod	o 5/15/2019 10:54:3	8 AM 🗸
	?	×
Application	PID	
▲ III csrss.exe	528	^
▼ III winlogon.exe	592	
fontdrvhost.exe	724	
▲ 📑 dwm.exe	932	
▼ 🐂 explorer.exe	3580	
▲ 🖶 MSASCuiL.exe	5920	
✓ O browser_assistant.exe	6104	
✓ i WmiPrvSE.exe	5464	
✓ I svchost.exe	1580	
✓ conhost.exe	2336	
✓ I CpmService.exe	2292	
🔻 🔽 cis.exe	3160	
▼ 🧧 cis.exe	5536	
∠ 🔄 cis.exe	3864	
	3012	
▲ Image: a taskhostw.exe		
<ul> <li>Image: Test test test test test test test test</li></ul>	5840	

- Select the signed executable that you want to trust and click the 'OK' button.
- Comodo Client Security performs the same certificate check as described above. If the parent application of
  the selected process is signed, you will be able to assign a rating and add the vendor as described above.

#### View details of vendors and assign user rating

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select a vendor and click the 'Vendor Details' button
- · Alternatively right-click on a vendor and select 'Vendor Details'

COMODO Creating Trust Online\*



The 'Vendor Details' dialog will open. The dialog has two tabs:

- Overview
- Vendor Rating

#### Overview

The 'Overview' tab shows general details such as the vendor name, Comodo assigned rating, when the vendor was added and more:

COMODO Creating Trust Online\*

OMODO Vendor Details	?
OVERVIEW	VENDOR RATING
Vendor Name:	Digital Wave Ltd
Vendor Rating:	Unrecognized
Rated By:	Comodo
Added On:	5/27/2019 1:48:09 PM
Last Modified:	5/27/2019 1:48:09 PM
	OK CANCEL

#### **Vendor Rating**

The 'Vendor Rating' tab shows the vendor's current trust rating from Comodo and your admin and lets you set your own rating:

OVERVIEV	V	VENDOR RATING
Vendor Rating:		Unrecognized
Provider	Date	Vendor Rating
Administrator		? Unrecognized
User		? Rate Now
Comodo	5/27/2019 1:48:09 PM	? Unrecognized

### Change the user rating of the file

- Select the vendor from the 'Vendor List' pane and click the 'Vendor Details' button
- Click the 'Vendor Rating' tab from the 'Vendor Details' pane

Creating Trust Online\*

•	Click the 'Rate No	w' link beside	'User' and	I choose the	rating from	m the drop	-down
---	--------------------	----------------	------------	--------------	-------------	------------	-------

OVERVIEW		VENDOR RATING
Vendor Rating:		Unrecognized
Provider	Date	Vendor Rating
Administrator		? Unrecognized
User		Rate Now
Comodo	5/27/2019 1:48:09 PM	? Trusted Malicious

- Click 'OK'
- The trust rating of the vendor will be updated with the user rating in the 'Vendor List' interface.
- · You can change the rating for the vendor at anytime by following the same process

Tip: Alternatively, right click on a selected vendor, then choose 'Change File Rating to' from context sensitive menu and select the rating.

Click 'OK' in the 'Advanced Settings' interface to save your settings.

#### Perform an online lookup for vendors

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Look Up...' button
- · Alternatively right-click on a vendor and select 'Look up...'

Comodo servers will be contacted immediately to conduct a search of Comodo's trusted vendor list database to check if any information is available about the vendor in question and the results will be displayed.

COMODO Creating Trust Online\*

COMODO Advanced	Settings	?
✓ General Settings	Vendor List	
✓ Antivirus	Vendor List	
✓ Firewall	+ 🗶 🗶 ۹	
✓ HIPS	Add Vendor Remove Lookup	
✓ Containment	□ Vendor Q Rated By ▼ Last Modified □	
- File Rating	☑ Via-Vox Ltd Comodo 4/11/2019 1:58:10 PM	
File Rating Settings	✓ Viber Media Inc. Comodo 4/11/2019 1:58:10 PM	
File Groups	Viber Media S.à r.l. Comodo 4/11/2019 1:58:10 PM	
File List		
COMODO Lookup	? - □	×
100% via-vos	x Ltd	
Vendor	Rating	
Viber Media Inc.	🧭 Trusted	
Via-Vox Ltd	🧭 Trusted	
× CLOSE	SEND TO BACKGROU	JND

### Remove vendors from the list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Remove' button
- Alternatively right-click on a vendor and select 'Remove'

### Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

- i. **Content Source**: The software they are downloading and are about to install *really comes from the publisher that signed it.*
- ii. **Content Integrity**: That the software they are downloading and are about to install *has not be modified or corrupted since it was signed.*

In short, users benefit if software is digitally signed because they know who published the software and that the code

COMODO Creating Trust Online\*

hasn't been tampered with. They know they are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the vendor list.

However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Sectigo', 'Identrust' and 'Digicert' are examples of trusted CA's authorized to counter-sign 3rd party software. The counter-signature is critical to the trust process, so a CA only counter-signs a certificate after conducting strict background checks on the vendor.

If a file is signed by a vendor with 'Trusted' rating in the vendor list and the user has 'Rate applications according to their vendor rating' in the 'File rating Settings' then it will be automatically trusted by Comodo Client Security.

One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main executable for Comodo Client Security is called 'cis.exe', which has been counter-signed by Sectigo certificate authority.

- In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with. They know they are downloading and installing the genuine software.
- The 'Vendors' that digitally sign their software are the software publishers. These are the company names
  you see listed in the vendor list
- However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Certificate Authority' (CA).
- 'Sectigo CA Limited' and 'Verisign' are two example CAs who are authorized to counter-sign 3rd party software.
- The counter-signature is critical to the trust process. A CA only counter-signs a certificate after it has conducted detailed background checks on the publisher.
- One of the methods of identifying whether an executable file has been digitally signed is by checking the properties of the .exe file in question.
- For example, the main program executable for Comodo Client Security is called 'cis.exe' and has been digitally signed.
  - Browse to the (default) installation directory of Comodo Client Security.
  - Right click on the file cis.exe.
  - Select 'Properties' from the menu.
  - Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software as shown below:

COMODO Creating Trust Online\*

cis Properties				$\times$
Security	Details		Previous Versions	
	patibility 🤇	Comodo	Digital Signatures	;
Signature list				
Name of signer:	Digest algorit	hm Times	tamp	
Comodo Security				
Comodo Security	/ sha256	Tuesd	lay, November	
			Details	
	ОК	Ca	ancel Apply	

Click the 'Details' button to view certificate details. Click the 'View Certificate' button to inspect the actual code signing certificate. (see below).

gital Signature Details	? ×	Certificate
ieneral Advanced Digital Signature Informatio This digital signature is OK.	n	General Details Certification Path
Signer information Name: Comodo Security So E-mail: Not available	olutions, Inc	This certificate is intended for the following purpose(s): • Ensures software came from software publisher • Protects software from alteration after publication
Signing time: Tuesday, Novembe	vr 8, 2016 10:52:03 M View Certificate	* Refer to the certification authority's statement for details.  Issued to: Comodo Security Solutions, Inc
Countersignatures           Name of signer:         E-mail address:           COMODO SHA-2         Not available	Timestamp Tuesday, November	Issued by: COMODO RSA Extended Validation Code Signing CA Valid from 1/11/2016 to 1/11/2018
	Details	Install Certificate Issuer Statement
	OK	ОК

COMODO Creating Trust Online\*

It should be noted that the example above is a special case in that Comodo, as creator of 'cis.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different.

### The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Vendor List' with 'Trusted' status that is shipped with Comodo Client Security. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the vendor list, CCS automatically trusts the software and does not generate any warnings or alerts on installation or use of the software.

The vendors have to apply for inclusion in the vendors list through the sign-up form at http://internetsecurity.comodo.com/trustedvendor/signup.php and make sure that the software can be downloaded by our technicians. Our technicians check whether:

- The software is signed with a valid code signing certificate from a trusted CA;
- The software does not contain any threats that harm a user's PC;

... before adding it to the default vendor list of the next release of CCS.

More details are available at .http://internetsecurity.comodo.com/trustedvendor/overview.php.

### 6.8. Advanced Protection

The 'Advanced Protection' section allows you to:

- Configure the VirusScope component
- · Specify items you want to exclude from detection during a virus scan
- · Specify types of external devices are to allowed / blocked
- Configure heuristic command line analysis and embedded code detection on files that can execute code
- Configure miscellaneous settings.

### Open the 'Advanced Protection' area

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' on the left:

COMODO Creating Trust Online\*

COMODO Advanced Settings		?	- 0	×
<ul><li>General Settings</li><li>Antivirus</li></ul>	VirusScope			
✓ Firewall	Enable VirusScope			
✓ HIPS	This option enables VirusScope subsystem which dynamica processes and keeps a record of their activities.	ally analyzes the be	havior of runnin	ng
✓ Containment	Do not show popup alerts			
✓ File Rating	This option, when enabled, automatically quarantines deter activities.	cted threats and re	verses their	
- Advanced Protection	Monitor only the applications in the container			
VirusScope	This option applies VirusScope monitoring only to applicat Virtually or Run Restricted.	ions in the contain	er that are Run	
Scan Exclusions Device Control	Manage the status of the recognizers installed on this com	puter:		
Script Analysis	Name	Version	Status	
Miscellaneous	recognizerCryptolocker.dll	1.16.0.587		
	recognizer_v11.2.0.7313.dll	11.2.0.7313		
		ОК	CANCEL	

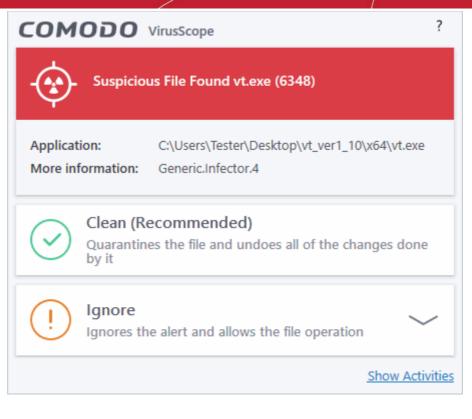
Click the following links to jump to the section you need help with:

- VirusScope Settings Configure VirusScope behavior
- Scan Exclusions Add and manage items that should be ignored during a scan
- Device Control Settings Manage types of external devices like USB drives, and printers that can connect to and are to be blocked
- Script Analysis Manage heuristic command line analysis and embedded code detection
- Miscellaneous Settings Exclude files from buffer overflow monitoring, configure browser alerts, and more

### 6.8.1. VirusScope Settings

- Click 'Settings' > 'Advanced Protection' > 'VirusScope'
- VirusScope monitors the activities of processes running on your computer and alerts you if they take actions that could threaten your privacy or security.
- VirusScope also allows you to reverse the actions of software without blocking the software itself. This
  provides more flexibility over legitimate software which requires certain actions to be implemented in order
  to run correctly.
- VirusScope alerts give you the opportunity to quarantine the process & reverse its changes, or to let the process go ahead.
- Be especially wary if a VirusScope alert appears 'out-of-the-blue' when you have not made any recent changes to your computer.

COMODO Creating Trust Online



#### Open the 'VirusScope' settings section:

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'VirusScope':

COMODO Advanc	ed Settings	?	- 🗆 X
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	VirusScope		
<ul><li>Firewall</li><li>HIPS</li></ul>	Enable VirusScope This option enables VirusScope subsystem which processes and keeps a record of their activities.	dynamically analyzes the be	havior of running
<ul> <li>Containment</li> <li>File Rating</li> </ul>	Do not show popup alerts This option, when enabled, automatically guarant	tines detected threats and re	everses their
Advanced Protection     VirusScope	activities.  Monitor only the applications in the container This option applies VirusScope monitoring only t	o applications in the contain	er that are Run
Scan Exclusions	Virtually or Run Restricted. Manage the status of the recognizers installed on		
Script Analysis	Name	Version	Status
Miscellaneous	recognizerCryptolocker.dll	1.16.0.587	
	recognizer_v11.2.0.7313.dll	11.2.0.7313	
		ок	CANCEL

### VirusScope Settings

VirusScope monitors running processes and alerts you to suspicious activity. You then have the option to quarantine the suspicious file and undo its activities.

- Enable VirusScope Activate VirusScope. If enabled, VirusScope monitors the activities of running
  processes and generates alerts if suspicious activity is detected. (*Default = Enabled*)
- **Do not show pop-up alerts** Whether CCS should show an alert if VirusScope detects suspicious activity. (*Default = Disabled*)
  - If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.
- Monitor only applications in the container VirusScope only tracks the activities of processes that a
  running in the container. It will not track processes directly running on the host (*Default = Enabled*)
- Applications can be made to run in the container in two ways:
  - Run a program in the container on a 'one-off' basis. See Run an Application in the Container for more details.
  - Create a rule to auto-contain programs that match certain criteria. See **Auto-Containment Rules** for more details.

### Manage the status of recognizers

- VirusScope detects zero-day malware by analyzing the behavior and actions of an application.
- If the detected behavior corresponds to that of known malware, then VirusScope will generate an alert which allows you to quarantine the application and reverse any changes that it made.
- A 'recognizer' file contains the sets of behaviors that VirusScope needs to look out for.
- If you disable a recognizer, VirusScope will no longer show an alert if an application exhibits behavior described by the recognizer.
- We recommend most users to leave the 'Status' of recognizers at their default settings.
- Advanced users, however, may want to try disabling recognizers if they are experiencing a large number of VirusScope false positives.

### 6.8.2. Scan Exclusions

- Click 'Settings' > 'Advanced Protection' > 'Scan Exclusions'
- The 'Scan Exclusions' panel shows files and paths which you have chosen to skip during a virus scan.
- CCS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.
- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.

### Open the 'Scan Exclusions' panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'

COMODO Creating Trust Online\*

COMODO Advanced	Settings	?	-		×
✓ General Settings	Scan Exclusions				
✓ Antivirus					
✓ Firewall	EXCLUDED PATHS EXCLUDED APPLICATIONS				
✓ HIPS					
✓ Containment	The virus scanner is going to skip or exclude the files and folders defined the scan. This setting applies to realtime as well as manual and schedule			perform	ing
✓ File Rating	+ / ×				
- Advanced Protection	Add Edit Remove				
VirusScope	Path				Q
Scan Exclusions					
Device Control	C:\Program Files\COMODO\COMODO Internet Security\*				
Script Analysis	□ <sup>®</sup> %WINDIR%\Prefetch\*.pf				
Miscellaneous					
	ок		CÆ	NCEL	

The 'Scan Exclusions' panel has two tabs:

- Excluded Paths A list of paths/folders/files on your computer which are excluded from real-time, ondemand and scheduled antivirus scans. See 'Exclude Drives/Folders/Files from all types of scans' for more details.
- Excluded Applications A list of applications which are excluded from real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus 'Scan Results', or by clicking 'Ignore' at an Antivirus Alert, or by excluding it manually. Note excluded items are skipped by the real-time scanner but will be scanned during on-demand scans. See 'Exclude Programs/Applications from real-time scans' for more details.

### Exclude Drives/Folders/Files from all types of scans

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click the 'Add' button:

COMODO Creating Trust Online\*

Exclusions	
EXCLUDED PATHS EXCLUDED APPLICATIONS	
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.	
(+) < *	
Add Edit Remove	
File Groups 🕨	Q
Files	
Folders	

You can add a:

- File Group
- Drive partition/Folder

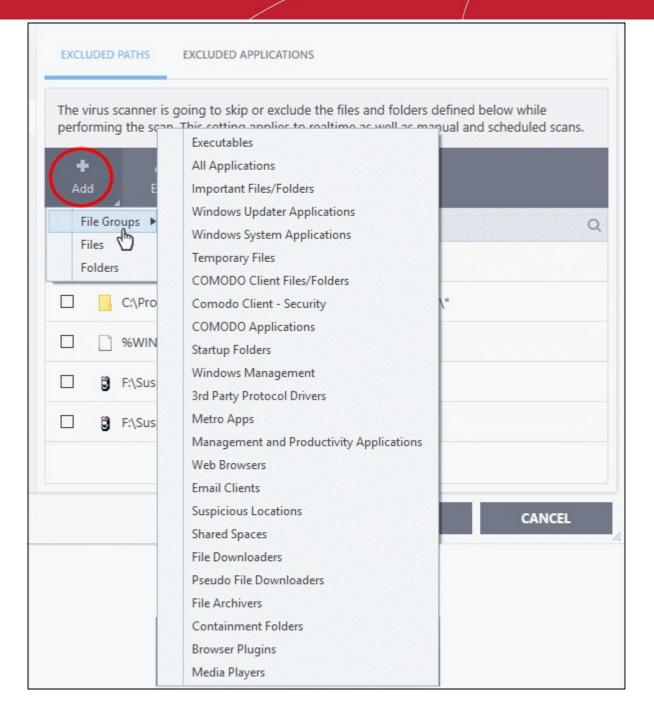
or

• Individual file

### Add a File Group

- Choose 'File Groups' to exclude a pre-set category of files or folders. This provides a convenient way to apply a generic ruleset to important files and folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl \*\cmd.exe, \*.bat, \*.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications' and 'Start Up Folders'.

Creating Trust Online\*



- CCS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > 'File Groups'.
- You can also add new file groups as required. See File Groups for more details.

#### Add new file groups to exclusions

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Click 'Add' > 'File Groups'
- Select the target file group from the list:

COMODO Creating Trust Online\*

Exclusions
EXCLUDED PATHS EXCLUDED APPLICATIONS
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.
+ X X Add Edit Remove
D Path Q
?:\\$Recycle.Bin\*
C:\Program Files\COMODO\COMODO Internet Security\*
%WINDIR%\Prefetch\*.pf
F:\Suspicious files\All_tests\IE-KillConnectionsTab.exe
F:\Suspicious files\All_tests\IE-KillProgramsTab.exe
Executables
OK CANCEL

- Repeat the process to add more file groups.
- Items added to the 'Excluded Paths' will be omitted from all types of future Antivirus scans.

#### Add a Drive Partition/Folder

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click 'Add' > 'Folders'
- Navigate to the drive partition or folder you want to add to excluded paths and click 'OK'.

COMODO Creating Trust Online\*

Exclusion	IS
EXCLUDED PATHS	EXCLUDED APPLICATIONS
	can. This setting applies to realtime as well as manual and scheduled scan Browse For Folder X
Path	> 27bfd58d8041e362ace9d55f66a6c7cd > 42c676a6b6641a60136a8a
?:\\$	A108f5ccd23e7699919f       5905a983d5cda5888543       51582d02ddd39d740379
□ <u></u> %w	All tests     CCAV
□ ĝ F:\S	CCAV_configs
🗆 🎒 F:\S	Make New Folder OK Cancel
Execu	tables
	OK CANCEL

The folder/partition will be added to the list of excluded items:

COMODO Creating Trust Online\*

Exclusions
EXCLUDED PATHS EXCLUDED APPLICATIONS
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.
+ 🗶 🗱 Add Edit Remove
Path Q
?:\\$Recycle.Bin\*
C:\Program Files\COMODO\COMODO Internet Security\*
%WINDIR%\Prefetch\*.pf
F:\CCS Logs\*
OK CANCEL

• Repeat the process to add more folders. Items added to 'Excluded Paths' will be omitted from all types of antivirus scans in future.

### Add an individual file

You can specify individual files as excluded path.

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click 'Add' > 'Files'
- Navigate to the file you want to add to excluded paths and click 'OK'.

COMODO Creating Trust Online\*

٢	Exclusions		
EXCLU	IDED PATHS E	CLUDED APPLICATIONS	
		ng to skip or exclude the files and folders defi is setting applies to realtime as well as manua	
+ Ada	لاً الم Edit	* Remove	
Fi	les	*	Q
	G Open	•	
	Look in:	🕌 My Downloads 👻	G 🏂 📂 🎞 -
	(Ha	Name	Date modified Type
	Recent Places	📢 DTLiteInstaller	11/2/2016 8:38 AM Applicatic
	Desktop		
	Libraries		
	Computer		
	(interview of the second secon	File name: DTLiteInstaller	- Open
		Files of type: All Files (*.*)	Cancel

The file will be added to excluded paths:

•

COMODO Creating Trust Online\*

Exclusions
EXCLUDED PATHS EXCLUDED APPLICATIONS
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.
<ul> <li>▲</li> <li>Add</li> <li>Edit</li> <li>Remove</li> </ul>
Path Q
F:\CCS Logs\*
C:\My Downloads\DTLiteInstaller.exe
OK CANCEL

- Repeat the process to add more paths.
- Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

### Edit the path of an added item

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Select the target item and click 'Edit':

COMODO Creating Trust Online\*

Exclusions
EXCLUDED PATHS EXCLUDED APPLICATIONS
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.
+ Add Edit Remove
<ul> <li>Path</li> <li>F:\CCS Logs\*</li> </ul>
C:\My Downloads\DTLiteInstaller.exe
COMODO Edit property ? X
Edit File Path C:\My Downloads\DTLiteInstaller.exe
OK CANCEL
OK CANCEL

• Modify the file-path as required and click 'OK'.

### Remove an item from 'Excluded Paths'

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Select the target item and click 'Remove':

COMODO Creating Trust Online\*

Exclusions	
EXCLUDED PATHS EXCLUDED APPLICATIONS	
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.	
+        Add     Edit       Remove	
Path Q	
C+CCS Logs\*	
C:\My Downloads\DTLiteInstaller.exe	
OK CANCEL	/1.

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

### **Exclude Programs/Applications from Real-time Scans**

- The 'Excluded Applications' screen lets you specify programs which should be skipped by real-time virus scans.
- Applications which you chose to '**Ignore**' in an antivirus alert or in the **Scan Results** window are automatically added to this list.
- You can manually add and remove programs to/from the list as required

Open 'Excluded Applications' pane

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab:

COMODO Creating Trust Online\*

COMODO Advance	d Settings	?	-		×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>Containment</li> </ul>	Scan Exclusions EXCLUDED PATHS EXCLUDED APPLICATIONS				
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	This setting applies to realtime scanning only. The realtime scan system activity (e.g. file/folder creation, etc.) from the applicatio			all file	
VirusScope	🕂 🧟 🗱 Add Edit Remove				
Scan Exclusions	Applications				Q
Device Control Script Analysis Miscellaneous	%SystemRoot%\System32\SearchIndexer.exe				
	ок		c	ANCEL	

### Add an item to excluded applications

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab
- Click 'Add' at the top of the 'Excluded Applications' pane.

COMODO Creating Trust Online\*

l Settings			?	-		
Excl	usions					
EXCLUDED	PATHS E	XCLUDED APPLICATIONS				
		realtime scanning only. T			all file	
		realtime scanning only. The figure of the fi			all file	
					all file	

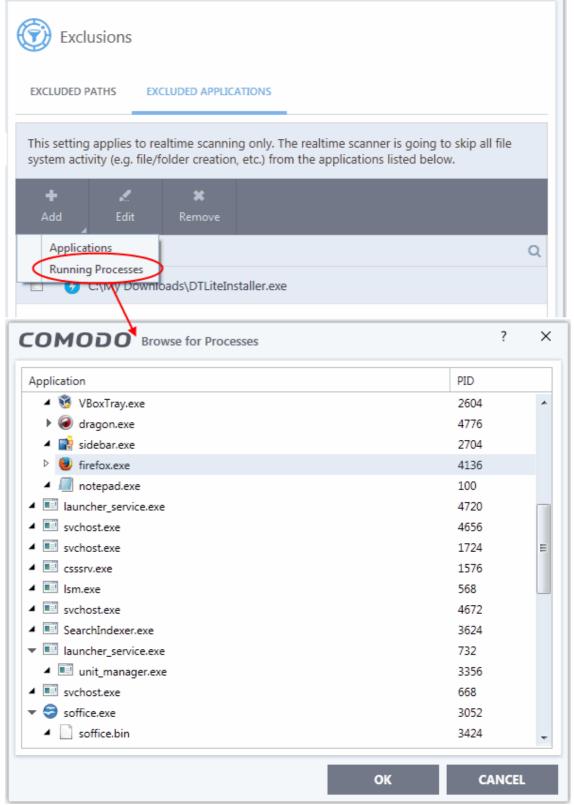
You can choose to add an applications by:

- Selecting it from the running processes This option allows you to choose the target application from the list of processes that are currently running on your PC.
- **Browsing your computer for the application** This option is the easiest for most users and simply allows you to browse to the files which you want to exclude.

### Add an application from a running processes

• Choose 'Running Processes' from the 'Add' drop-down

COMODO Creating Trust Online\*



A list of currently running processes in your computer will be displayed:

Select the process whose target application you wish to exclude and click 'OK':

The application will be added to 'Excluded Applications'.

#### Browse to the Application

•

Choose 'Applications' from the 'Add' drop-down

COMODO Creating Trust Online\*

Exclusion Exclusion	ons			
EXCLUDED PATH	S EXCLUDED	APPLICATIONS		
		canning only. The realtime scar eation, etc.) from the application		all file
+ Add	Edit Rem			
Applications Running Pro				Q
G Open	4			<b>—</b>
Look in:	🌗 My Download	s 🗸	G 🜶 📂 🛄 -	
Ca	Name	~	Date modified	Туре
Recent Places	😡 DTLiteInstall	er	11/2/2016 8:38 AM	Applicatic
Desktop				
Libraries				
Computer				
Network	File name:	DTLiteInstaller		Open
	Files of type:	Applications (*.exe)	-	Cancel

• Navigate to the file you want to exclude and click 'Open'.

COMODO Creating Trust Online\*

Excl	usions			
EXCLUDED F	ATHS EX	CLUDED APPLIC	ATIONS	
			ng only. The realtime scanner is going to skip all file a, etc.) from the applications listed below.	
		*		
Add	Edit	Remove		
A	Edit	Remove		Q
Apr	olications	Remove oads\DTLiteIn:	staller.exe	Q

• Repeat the process to add more items. Excluded items will be skipped from future real-time scans.

### Edit the path of the application added to 'Excluded Applications'

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab

- Select the application and click 'Edit' at the top.
- Make required changes to the file path in the 'Edit Property' dialog.

COMODO Creating Trust Online\*

Scan Exclu	usions			
EXCLUDED PATHS	EXCLUDED APPLICATIONS			
	s to realtime scanning only Ider creation, etc.) from th			ile system
+ Add Ed	it Remove			
Application	15			Q
System	mRoot%\System32\Search	Indexer.exe		
🗹 🗑 C:\Prog	ram Files (x86)\Evernote\E	vernote\Evernote.exe		
сок	1000 Edit proper	ty	?	×
Edit Fil				
	gram Files (x86)\Evernote\	Evernote\Evernote.exe		
		ОК	CANCEL	

• Click 'OK' to save your changes

### Remove an item from the Excluded Applications

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab
- Select the item and click 'Remove' at the top:

COMODO Creating Trust Online\*

П

Exclusions	
EXCLUDED PATHS EXCLUDED APPLICATIONS	
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.	
+ Add Edit Remove	
☑ Applications	Q
C:\My Downloads\DTLiteInstaller.exe	

• Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

### 6.8.3. Device Control Settings

- Click 'Settings' > 'Advanced Protection' > 'Device Control'
- The 'Device Control' panel lets you specify types of external devices that are to be blocked and define
   exclusions to it

### **Open the Device Control panel**

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'

COMODO Creating Trust Online\*

✓ General Settings Device Control			
<ul> <li>Antivirus</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> <li>VirusScope</li> <li>Scan Exclusions</li> <li>Device Control</li> <li>Use this table to manage the list of devices to which you view</li> </ul>	or enabled	ves,	
Script Analysis   Miscellaneous     Device     Ide	entification		

- Enable Device Control Activate the device control functionality to selectively prohibit access to external devices. You should specify devices to be banned in the 'Blocked Devices' pane. (Default = Enabled)
- Log Detected Devices CCS logs events like connection attempts of external devices (Default = Enabled)
- Show Notifications when devices are being disabled or enabled CCS displays an alert whenever an external device is connected or disconnected.(*Default = Disabled*)
- Blocked Devices List of external device classes which are not allowed to connect to the endpoint. Example classes include 'USB Storage Devices', 'CD/DVD Drives', 'BlueTooth Devices' and 'Firewire Devices'.
- **Exclusions** Add exceptions to a blocked class. For example, if you wish block the class 'USB Devices' but wish to allow access for your company's authentication tokens, then you should add those USB tokens as exceptions.

Click the following links for more information on blocked devices and exclusions:

- Block devices
- Specify exclusions

### **Block Devices**

You can specify devices to be blocked in three ways:

- Select device classes
- Select from currently connected devices

COMODO Creating Trust Online\*

### • Specify custom devices

#### Block a device class

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button
- Click 'Add device class' from the options:

COMODO Advance	ed Settings ? - $\Box$ ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> </ul>	Device Control
✓ Containment	This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, serial and parallel ports.
✓ File Rating	Log detected devices
- Advanced Protection	Show notifications when devices are being disabled or enabled
VirusScope	BLOCKED DEVICES EXCLUSIONS
Scan Exclusions	
Device Control	Use this table to manage the list of devices to which you want to block access.
Script Analysis	Add Edit Remove
Miscellaneous	Add device class Q Identification Add existing device Add custom device
	OK CANCEL

- Choose the device class you wish to block.
  - For example, to block all USB devices that are plugged to your computer, select "Portable devices" from the list
  - If you want to exclude any specific device from this class, enter the device name in the exclusion list.

COMODO Creating Trust Online\*

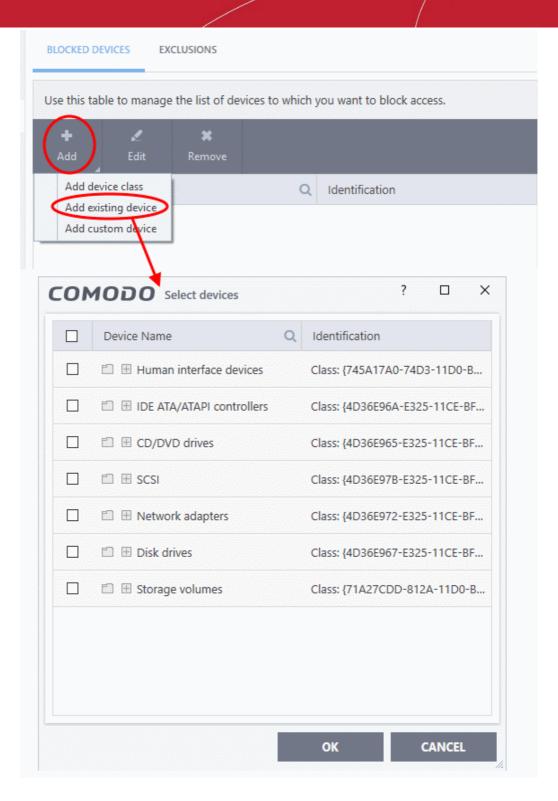
CON	<b>10D0</b> Select device classes	? 🗆	>
	Device Class Q	Identification	-
	SCSI	Class: {4D36E97B-E325-11CE-B	
	Modems	Class: {4D36E96D-E325-11CE-B	
	Smart card readers	Class: {50DD5230-BA8A-11D1	
	Ports	Class: {4D36E978-E325-11CE-B	
	Network adapters	Class: {4D36E972-E325-11CE-B	
	Biometric	Class: {53D29EF7-377C-4D14-8	
	Disk drives	Class: {4D36E967-E325-11CE-B	
	Storage volumes	Class: {71A27CDD-812A-11D0	
	Portable devices	Class: {EEC5AD98-8080-425F-9	
			~
		OK CANCEL	

- Select the device(s) you wish to block
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

### Select devices from currently connected devices

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button
- · Click 'Add existing device' from the options

COMODO Creating Trust Online\*



- Choose the device class you wish to block. For example, Network adaptor devices, CD/DVD drives, Storage devices or Disk drives.
- · Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to block
- Click 'OK' and again click 'OK' in the 'Device Control' panel to save your settings.

### Specify a custom devices to be blocked

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button

na Trust Onlin

se this table to manage	the list of devices to	which you	want to blo	ck acces	is.	
+ Add Edit	<b>XX</b> Remove					
Add device class		Q Id	lentification			
Add existing device	ces	Cl	ass: {8A63A	D27-0C	07-4F43-B8	E1-07.
USB Input Device		U	SB\VID_80EI	E&PID_0	021\5&18F	54CB
сомо	DO Add custom	device		?	×	
Enter device	ID (e.g. USBSTOR*)				1CE	L

Enter the device ID and click 'OK' •

### Specify exclusions

The 'Exclusions' tab lets you allow access to specific devices that fall within a blocked device class.

You can specify the exceptions in two ways:

- Select from currently connected devices •
- Specify a custom device •

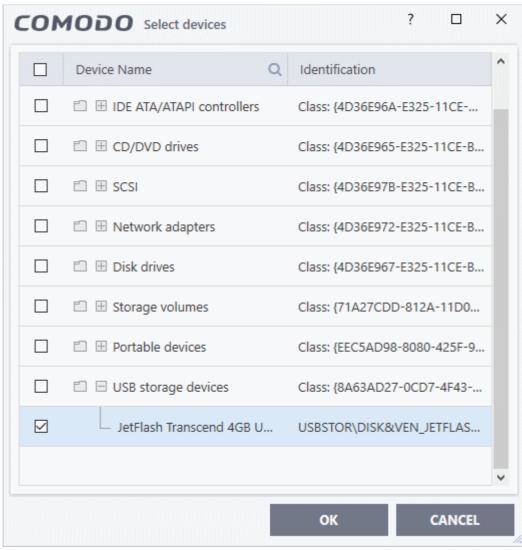
#### Add exclusions from currently connected devices

You need to add the device to the exclusion list before blocking the device class.

- Make sure the external device is connected to the computer •
- Click 'Settings' on the CCS home screen •
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button .

COMODO Creating Trust Online\*

• Select 'Add existing device' from the options



COMODO Creating Trust Online\*

- Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to exclude
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

#### Add custom device to be excluded

- You can also add exclusions by specifying the device lds.
- For example, you want to block all USB storage devices apart from the type of SANDISK devices used by your company, you could specify a device exclusion ID of 'USBSTOR\DISK&VEN\_SANDISK\4C5310\*'.
- You can also use the wildcard character ' \* ' to cover a range of devices

#### Specify custom devices to be excluded

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button
- Select 'Add custom device' from the options

Use this table to	manage the list of	devices to which ye	ou want to allow access.	
+ Add	🗶 🗱 Edit Remove			
Add existing Add custom		Q	Identification	
	<b>COMODO</b> nter device ID (e.g		ce ?	×

- Enter the unique device identifier in the 'Device ID' field, for example to exclude all USB storage devices whose device IDs start with "4C5310", you could enter: USBSTOR\DISK&VEN\_SANDISK\4C5310\*
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

### 6.8.4. Script Analysis Settings

- Click 'Settings' > 'Advanced Protection' > 'Script Analysis'
- The script analysis settings panel lets you:

COMODO Creating Trust Online\*

- Configure heuristic command line analysis for applications in real-time
- Configure heuristic command line analysis for auto-run entries. Auto-run entries include Windows services, auto-start items and scheduled tasks.

**Background note**: 'Heuristics' is a technology which analyzes a file to see if it contains code typical of a virus. Heuristics is about detecting 'virus-like' traits in a file. This helps to identify previously unknown (new) viruses.

### Open the 'Script Analysis' settings panel

- · Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Script Analysis'

	d Settings	? – 🗆	×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Script Analysis Perform Script Analysis (Recommended) Limit the total size of saved detected scripts to 100 When reaching the set limit, the older records will be deleted to RUNTIME DETECTION AUTORUNS SCAN	KB o free up space.	
Advanced Protection     VirusScope     Scan Exclusions     Device Control     Script Analysis	Manage the list of applications for which you would like to perfore execution.	rm script analysis before	
Miscellaneous	Application Q       Heuristic Command-Line Analysis       E         Number of the second	Embedded Code Detection	*
	ОК	CANCEL	

- Perform Script Analysis (Recommended) Enable / disable script analysis of managed applications (Default = Enabled)
  - Limit the total size of saved detected scripts to 'N' KB CCS stores the list of executing scripts that
    are run by the managed applications for analysis. This options allows you to specify the total size of the
    stored scripts. When the set limit is reached, the older scripts are deleted automatically.

The interface has two tabs:

- Runtime Detection
- Autoruns Scans

#### **Runtime Detection**

CCS performs heuristic analysis on certain programs because they are capable of executing code. Example programs are wscript.exe, cmd.exe, java.exe and javaw.exe. Example code includes Visual Basic scripts and Java

applications.

- For example, the program wscript.exe can be made to execute Visual Basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'.
- If this option is selected, CCS detects c:\tests\test.vbs from the command-line and applies all security
  checks based on this file. If test.vbs attempts to connect to the internet, for example, the alert will state
  'test.vbs' is attempting to connect to the internet
- If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the internet'.
- Relevant settings are applied to the scripts. For example, if a script is detected by the containment module, then auto-containment rules are applied. Each module (AV, FW, VirusScope and so on) that detects a script will apply its appropriate settings.

COMODO Advanc	ed Settings	? – 🗆	×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Script Analysis  Perform Script Analysis (Recommended) Limit the total size of saved detected scripts to 100 KB When reaching the set limit, the older records will be deleted to free up space RUNTIME DETECTION AUTORUNS SCAN		
VirusScope Scan Exclusions	Manage the list of applications for which you would like to perform script analys	is based on containment rules.	
Device Control	Application Q Heuristic Command-Line Analysis Em	bedded Code Detection	^
Script Analysis	*\winhlp32.exe		
Miscellaneous	"\WScript.exe		
	🗆 *\cscript.exe 💽 🖸		
	□ *\mshta.exe		
			~
		OK CANCEL	

Runtime Detection - Column Descriptions				
Column Header	Description			
Application	Names of existing applications covered by this rule			
Heuristic Command-Line Analysis	Enable or disable command line tracking			
Embedded Code Detection	Enable or disable embedded code tracking			

### Manually add a new application to the list for analysis

Click 'Add' at the top

COMODO

COMODO Creating Trust Online\*

+ Add	ی۔ Edit	XX Remove	Co Reset to Default
Add a new application Applications Running Processes		Heuris	tic Command-Line Ar
	*\WScript.exe		
· · · · · · · · · · · · · · · · · · ·	*\cscript.exe		

You can add an application by following methods:

- Add a new application
- Add a current application
- Add application from the currently running processes

### Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Enter the file path in the 'Edit Property' dialog and click 'OK'

+ 🦨 Edit	Remove Reset to Default	
Add a new application	Heuristic Command-Line Analysis	Embedded Code Detection
Applications Running Processes		
*\WScript.exe		0
сомо	DO Edit property	? ×
Edit applicatio	on's name	
*\bat.exe		

The application will be added and displayed in the list.

COMODO Creating Trust Online

+ Add	ي Edit	🗶 Remove	CF Reset to Default		
	Application	Q Heur	istic Command-Line Analysis	Embedded Code Detection	
	*\pythonw.exe		0		
	*\autoit3.exe		2		
	*\autoit3_x64.exe		2		
	*\bat.exe		0		

• Click "OK" to apply your settings

### Add a current application

- · Click 'Add' then 'Applications' from the drop-down
- · Navigate to the file you want to add in the 'Open' dialog and click 'Open'
- The file will be added to the list
- Click "OK" to apply your settings

#### Add a currently running processes

- Choose 'Running Process' from the 'Add' drop-down
- A list of currently running processes in your computer will be displayed
- Select the process whose parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list
  - Use the slider beside the applications to enable/disable them for analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list and choose 'Remove' at the top.
  - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

#### Autoruns Scans

- Add and manage applications for which you want to perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.
- CCS ships with a list of predefined applications for which it performs heuristic analysis on programs that are capable of executing code.
- The applications added here are applicable for the settings in:
  - 'Scan Options' > 'Apply this action to suspicious autorun processes' (monitors only during on-

COMODO Creating Trust Online\*

#### demand scans)

 'Advanced Settings' > 'Miscellaneous' > 'Apply the selected action to unrecognized autorun entries related to new/modified registry items' (monitors constantly)

#### Open the 'Autoruns Scans' interface

- Click 'Settings' on the CCS home screen.
- Click 'Advanced Protection' > 'Script Analysis'

	ed Settings	?	- 0	×		
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Script Analysis					
<ul> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> </ul>	Perform Script Analysis (Recommended)     Limit the total size of saved detected scripts to 100 KB     When reaching the set limit, the older records will be deleted to free up space.     RUNTIME DETECTION AUTORUNS SCAN					
Advanced Protection     VirusScope     Scan Exclusions	Manage the list of applications for which you would like to perform script analysis autostart items and scheduled tasks.	to protect Windo	ws services,			
Device Control	Application     Q     Heuristic Command-Line Analysis     Em       *\winhlp32.exe     •     •       *\WScript.exe     •     •       *\cscript.exe     •     •	bedded Code Det	ection			
		ок	CANCE	L		

Autroruns Scans - Column Descriptions					
Column Header	Description				
Application	Names of existing applications covered by this rule				
Heuristic Command-Line Analysis	Enable or disable command line tracking				
Embedded Code Detection	Enable or disable embedded code tracking				

#### To manually add a new application to the list for analysis

• Click 'Add' at the top

COMODO Creating Trust Online\*

+     *     C       Add     Edit     Remove     Reset to Default       Add a new application     Heuristic Command-Line Analysis       Applications     Image: Command-Line Analysis       Running Processes     Image: Command-Line Analysis		-	list of applica ms and scheo		ich you would	l like to perform
Applications	A	<b>F</b> dd	🗶 Edit	🗱 Remove		
		Applicati	ons	A Heuris	stic Command	d-Line Analysis

You can add an application by following methods:

- Add a new application
- Add a current application
- Add application from the currently running processes

#### Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Enter the file path in the 'Edit Property' dialog and click 'OK'

RUNTIME DETECTION	AUTORUNS SCAN	
Manage the list of a autostart items and	oplications for which you would like to perform scr scheduled tasks.	ipt analysis to protect Windows services,
+ Add Edit	<b>≭ C</b> Remove Reset to Default	
Add a new applications Running Processe		Embedded Code Detection
*\WScript.ex	COMODO Edit property	? ×
*\cscript.exe	Add a new application *\bat.exe	
		OK CANCEL

The application will be added and displayed in the list.

COMODO

+ Add	۲. Edit	🗱 Remove	Cr Reset to Default		
_ App	lication	Q Heuris	stic Command-Line Analysis	Embedded Code Detection	
*\po	wershell_ise	e.exe	)		
×\reg	gasm.exe				
*\ba	t.exe		)		

Click "OK" to apply your settings

### Add an application

- Click 'Add' then 'Applications' from the drop-down
- Navigate to the executable file you want to add in the 'Open' dialog and click 'Open'
- The file will be added to the list
- Click "OK" to apply your settings

### Add a currently running process

- Choose 'Running Process' from the 'Add' drop-down
- A list of currently running processes in your computer will be displayed
- Select the process whose parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list
  - Use the slider beside the applications to enable/disable them for analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list and choose 'Remove' at the top.
  - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

### 6.8.5. Miscellaneous Settings

- Click 'Settings' > 'Advanced Protection' > 'Script Analysis'
- The miscellaneous settings panel lets you:
  - · Configure protection against shellcode injections (buffer overflow attacks)
  - Skip automatic cleanup of suspicious certificates.
  - Specify what actions are taken if CCS detects unrecognized auto-start entries or scheduled tasks

COMODO Creating Trust Online\*

#### Open the 'Miscellaneous' settings interface:

- Click 'Settings' on the CCS home
- Click 'Advanced Protection' > 'Miscellaneous'

COMODO Advanced	Settings ? - □ ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection         <ul> <li>VirusScope</li> <li>Scan Exclusions</li> <li>Device Control</li> <li>Script Analysis</li> </ul> </li> </ul>	<ul> <li>Miscellaneous</li> <li>Don't detect shellcode injections in these applications</li> <li>Do not automatically clean up suspicious certificates</li> <li>Apply the selected action to unrecognized autorun entries related to new/modified registry items:</li> <li>Ignore </li> <li>When this option is enabled, the registry will be monitored for modifications and the selected action will be applied to detected unrecognized Windows services, autostart entries or scheduled tasks.</li> </ul>
Miscellaneous	OK CANCEL

This interface allows you to:

- Disable shellcode injection detection for certain applications
- · Define actions to be taken on unrecognized auto-start entries/scheduled tasks
- · Skip automatically clean-up of suspicious certificates

#### Disable shellcode injection detection

By default, protection against shellcode injection is enabled for all applications on your computer. Use this setting to define applications which you **do not** want to monitor for shellcode injections.

#### Background:

- Shellcode injection is a malicious technique which allows an attacker to cause a buffer overflow on your system.
- A buffer is an area of memory designed to hold a specific amount of data. A buffer overflow occurs when a process stores data beyond the boundaries of this fixed-length buffer.
- The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.
- Malware can deliberately cause buffer overflows in order to run malicious code or make the program operate incorrectly.

COMODO Creating Trust Online\*

#### Exclude certain applications from shellcode injection protection

- Make sure 'Don't detect shellcode injections in these applications' is enabled then click the 'these applications' link. The 'Manage Exclusions' dialog appears.
- Click the 'Add' button at the top

You can add items by selecting the required option from the drop-down:

сомор	Advanced Settin	ıgs	
	dia	Miscellaneous Don't detect shellcode injections in thes ge Exclusions ?	
✓ Conf ✓ File I Add	e Edit	x A Remove Purge	es related to new, for modifications a or scheduled task
V Fil	le Groups les olders unning Processes	ExecutablesAll ApplicationsWindows Updater ApplicationsWindows System ApplicationsWindows Management3rd Party Protocol DriversMetro AppsEmail ClientsFile ArchiversTemporary FilesShared SpacesFile DownloadersSuspicious LocationsContainment FoldersWeb BrowsersBrowser Plugins	

- File Groups Select a category of pre-set files or folders. For example, 'Executables' lets you create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, \*cmd.exe \*.bat, \*.cmd. Other categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc. See File Groups, for more details on file groups.
- Running Processes Select an application or executable from the processes that are currently running on your PC.
- Folders Specify a folder on your computer to include all files in the folder to the exclusions .
- Files Select a specific executable file you wish to add to the exclusions.

Click 'OK' to implement your settings.

#### Do not automatically cleanup suspicious certificates

COMODO Creating Trust Online\*

- Choose whether or not to delete any root certificates that were not signed by a trusted certificate authority.
- By default, CCS warns you if any fake root certificates are found in your browsers but does not delete them.
- Disable this option if you want CCS to delete those fake certificates whenever they are found

#### **Background:**

- SSL certificates are used by websites to encrypt the connection between your browser and the website.
- This ensures nobody can intercept the traffic sent between you and the website. All information sent from your browser to the site is private. This is especially important for sensitive transactions like online payments, where you send your credit card information over the internet.
- You can tell a site is using an SSL certificate by the padlock icon in the browser address bar. You will also notice that the website address begins with https:// (the 's' stands for 'secure').
- SSL certificates are issued to website owners by an organization known as a 'Certificate Authority' (CA). The certificate authority checks the applicant, the website owner, is a legitimate business before they will issue a certificate to them.
- Root certificates are embedded in your browser and are used to check that the SSL certificate used by a
  website is legitimate. That it was indeed signed by a certificate authority.
- A fake root certificate would, therefore, bypass this check of legitimacy. It could tell you to trust a website run by a hacker.
- CCS detects whether you have any fake root certificates in your browser and warns you if you do. Disable this option if you also want CCS to delete fake root certificates automatically.

#### Define actions to be taken on unrecognized auto-start entries/scheduled tasks

- Apply the selected action to unrecognized autorun entries related to new / modified registry items -Specify what CCS should do if applications added to Script Analysis > Autoruns Scans try to create or modify one of the following registry items:
  - Windows services
  - Auto-start entries
  - Scheduled tasks

The available options are:

- Ignore CCS does not take any action (*Default*)
- Terminate CCS stops the process / service
- **Terminate and Disable** Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- Quarantine and Disable The application is quarantined and the corresponding auto-start entry is removed. In the case of a service, CCS disables the service.

#### Background:

- CCS can perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.
- CCS ships with a list of predefined applications for which it performs heuristic analysis on programs that are capable of executing code.
- You can also add programs for which you want CCS to perform heuristics analysis in 'Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autoruns Scan'. See Autoruns Scans in Script Analysis Settings for more details on this.
- Click 'OK' to save your settings.

# Appendix 1 - CCS How to... Tutorials

The 'How To...' section of the guide contains guidance on key tasks in Comodo Client Security. Use the links below to go to each tutorial's page.

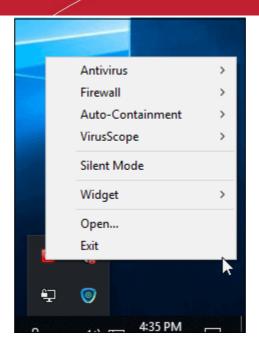
#### How to ...:

- Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily How to quickly enable or disable various CCS modules.
- Setup the Firewall for maximum security and usability How to set up a secure connection to the internet
- Block Internet Access while allowing local network (LAN) Access Configure the firewall to only allow intranet/LAN connections while blocking the internet
- Set up HIPS for Maximum Security and Usability How to set up the host intrusion protection system for the optimum balance between security and usability
- Create Rules to Auto-Contain Applications How to set auto-containment rules for maximum security
   against untrusted applications
- Run an instant Antivirus scan on selected items Run a manual scan on selected folders/files to check for viruses and other malware
- Create an Antivirus scan schedule Set up antivirus scans to automatically run at specific times.
- Run an untrusted program inside the container Launch programs that you do not trust inside the container to eliminate the possibility of them causing damage to your computer.
- Run Browsers inside the Container Run your browser inside the container when you plan to visit
   untrusted websites
- Restore incorrectly quarantined item(s) Restore files and executables that had been moved to quarantine by mistake
- Submit quarantined items to Comodo for analysis Send suspicious files/executables to Comodo for analysis
- Enable file sharing applications like BitTorrent and Emule Configure firewall for file sharing through popular software
- Block any downloads of a specific file type Configure HIPS to block downloads of files of a specific type
- Disable Auto-Containment on a Per-application Basis Exclude specific files or file types from the autocontainment process
- Switch Off Automatic Antivirus Updates Stop automatic virus updates
- Suppress alerts when playing games Switch off CCS pop-up alerts to avoid interruptions while playing games
- Control External Device Accessibility Restrict access to external devices such as USB pen drive on the endpoints.

# Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily

• Right-click on the CCS tray icon to quickly switch Antivirus, Firewall, Auto-Containment or VirusScope on or off:

COMODO Creating Trust Online



### Antivirus

- 1. Right-click on the system tray icon
- 2. Move your mouse over 'Antivirus'

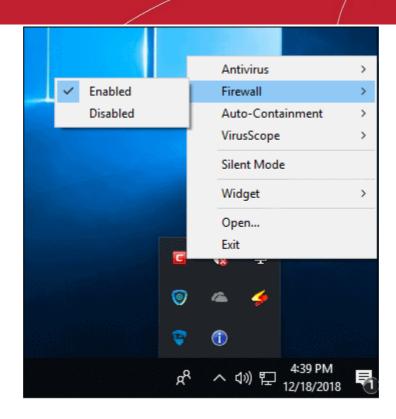
			State State
✓ Enabled		Antivirus	>
Disabled		Firewall	>
		Auto-Containment	>
		VirusScope	>
		Silent Mode	
		Widget	>
		Open	
	-	Exit	
	G	* <b>T</b>	
	0	le 🍝	
	Ŷ		
	RA	へ (い) に 4:37 PM 12/18/2018	$\Box$

3. Choose 'Enabled' or 'Disabled' as required You can also set security level in **the Home Screen**.

#### Firewall

- 1. Right-click on the system tray icon
- 2. Move your mouse over 'Firewall'
- 3. Choose 'Enabled' or 'Disabled' as required

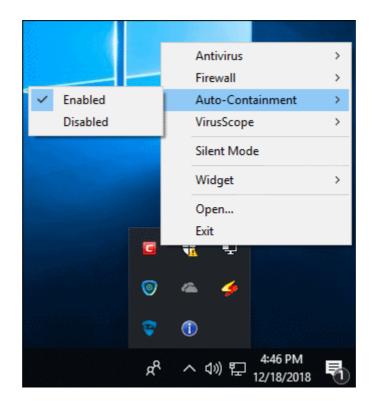
COMODO Creating Trust Online\*



You can also set security level in the Home Screen.

#### **Auto-Containment**

- 1. Right-click on the system tray icon
- 2. Move your mouse over 'Auto-Containment'

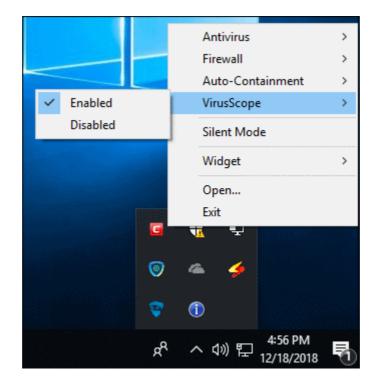


3. Choose 'Enabled' or 'Disabled' as required

You can also set security level in the Home Screen.

VirusScope

- 1. Right-click on the system tray icon
- 2. Move your mouse over 'VirusScope'



3. Choose 'Enabled' or 'Disabled' as required

You can also set security level from the Home Screen.

### Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the internet.

### **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. Click 'Tasks' > 'Firewall Tasks'
- 2. Click 'Stealth Ports'

COMODO Creating Trust Online

COMODO Creating Trust Online\*

	<b>COMODO</b> Stealth Ports Ports allow your computer to communistealthing them, you may configure this	? × icate with other computers in a network. By s computer's visibility to others.
GENERAL TASKS FIREWA	Block Incoming Connect Block all incoming connection	c <b>tions</b> ons and make this PC invisible to all
Block Applicati Block an applicati	showing popup alerts	tions ake this PC invisible on a case basis by BIOCK all network activity to any
Stealth Ports Manage this P PC's.	C's network visibility from other	View Connections View applications which are contra- internet.
		internet.

3. Select 'Block Incoming Connections' to make your computer's ports are invisible to all networks

### Click here for more information about port stealthing

#### **Network Zone Settings**

'Network Zones' settings allow you to configure the protection level for connections to a router/home network (this is usually done **automatically** for you).

#### View the configurations

- 1. Click 'Settings' at the top of the CCS home screen
- 2. Select 'Firewall' > 'Network Zones'
- 3. Click 'Network Zones' tab in the 'Network Zones' interface

COMODO Creating Trust Online\*

COMODO Client - So	ecurity 11	- ×
品 tasks 🔅 settings		
COMODO Advanced	Settings ? —	
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Network Zones	
- Firewall	Enable automatic detection of private networks	
Firewall Settings	Do not show popup alerts and treat location as	
Application Rules	The following network zones are defined on this computer:	
Global Rules	NETWORK ZONES BLOCKED ZONES	
Rulesets Network Zones	+ 2 ¥ Add Edit Remove	
Portsets	Zone Name	Q
<ul> <li>✓ HIPS</li> <li>✓ Containment</li> </ul>	🕅 🗈 🗄 Loopback Zone	
<ul> <li>File Rating</li> </ul>	🗐 🗄 Work #1	
<ul> <li>Advanced Protection</li> </ul>		
	ОК СА	NCEL

- 4. Inspect the 'Loopback zone' and 'Local Area Network #1' (exact name may vary) 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'.

### Click here for more details on network zones settings

### **Firewall Settings**

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

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

COMODO Creating Trust Online\*

COMODO Client - Se	curity 11	- ×
용 tasks (ô) settings	>	
		<b>I</b> Ø
	Scan	View Quarantine
COMODO Advanced	Settings	? – 🗆 ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Firewall Settings	
Firewall Settings Application Rules Global Rules	Image: Second stress       Image: Second stress         Image: Second	

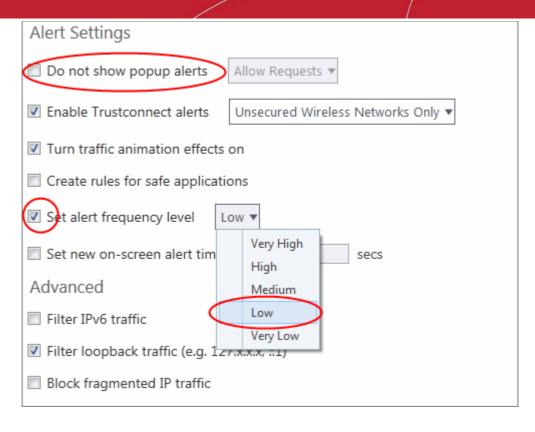
**Safe Mode**: While filtering network traffic, the firewall will automatically create rules which allow traffic for application components certified as 'Safe' by Comodo. For non-certified, new, applications, you will receive an alert whenever that application attempts to access the network. Should you 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.

COMODO Creating Trust Online\*



#### **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 down your
    download time.
- · Select 'Do Protocol Analysis' checkbox to detect fake packets used in denial of service attacks
- Select 'Enable anti-ARP spoofing'

Advanced
Filter IPv6 traffic
Filter loopback traffic (e.g. 127.x.x.x, ::1)
Block fragmented IP traffic
Do protocol analysis
Enable anti-ARP spoofing

COMODO Creating Trust Online\*

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

#### Click here for more details on the firewall settings

#### 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 the 'Application Rules'

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Firewall > 'Application Rules'

COMODO Client - Security 11			
🔠 tasks 🔅 settings			
COMODO Advanced S	iettings ? —		
<ul><li>General Settings</li><li>Antivirus</li></ul>	Application Rules		
- Firewall	The following firewall application rules are active on this computer.		
Firewall Settings Application Rules	+     .     ★     I     ↓     ↓       Add     Edit     Remove     Move Up     Move Down     Purge		
Global Rules	Application Q Treat as	۹ 🔶	
Rulesets	🔲 🗉 🗄 C:\Program Files\COMODO\GeekBuddy\launc Custom		
Network Zones	📃 🕘 🖯 C:\Program Files\Mozilla Firefox\firefox.exe Custom		
Portsets	Allow All Incoming and Outgoing Requests		
✓ HIPS	Custom		
✓ Containment	Allow System To Send Requests If The Tar	E	
✓ File Rating	Allow System To Receive Requests If The		
✓ Advanced Protection	COMODO Internet Security     Outgoing Only		
	E Windows Updater Applications     Custom		
	Allow IP Out From MAC Any To MAC Any		
		•	
	ОК СА	ANCEL	

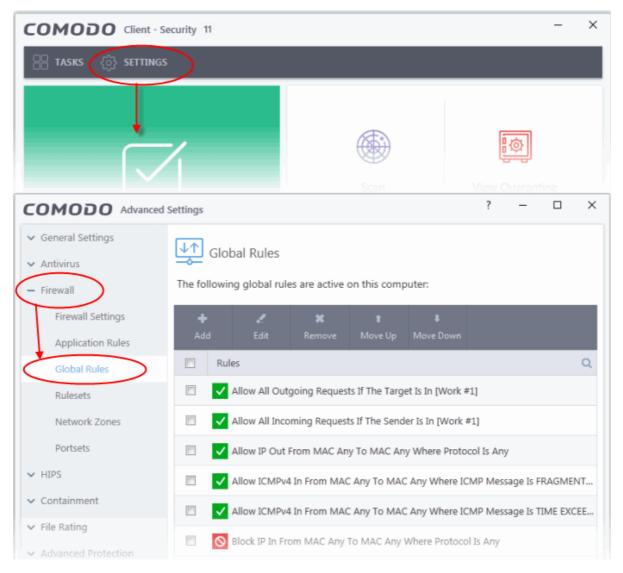
COMODO Creating Trust Online\*

- 3. Click 'Add' to create a new application rule
- 4. Select a rule and click 'Edit' to edit the rules for a specific application manually or click 'Remove' to remove them
- 5. Click 'OK' for your settings to take effect

#### Click here for more details on application rules

#### View the Global Rules

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Firewall' > 'Global Rules'



- 3. Click 'Add' to create a new global rule
- 4. Select a rule and click 'Edit' to edit the a rule manually or click 'Remove' to remove them
- 5. Click 'OK' for your settings to take effect

#### Click here for more details on global rules

#### **View Predefined Firewall rulesets**

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Firewall' > 'Rulesets'

COMODO Creating Trust Online\*

COMODO Client - Se	ecurity 11	-	- ×
문 tasks (ô settings			
COMODO Advanced	Settings	? — [	×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	Rulesets The following rulesets are defined on this computer:		
Firewall Settings Application Rules	+ X X Add Edit Remove		
Global Rules	Ruleset Name		Q
Rulesets	Web Browser		
Network Zones	Email Client		
Portsets	FTP Client		
✓ HIPS	Allowed Application		
✓ Containment	Blocked Application		
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>	Outgoing Only		

- 3. Click 'Add' to create a new ruleset
- 4. Select a ruleset and click 'Edit' to edit the rules manually or click 'Remove' to remove them
- 5. Click 'OK' for your settings to take effect

Note: You need not make your own rulesets, the defaults are usually enough.

Click here for more details on pre-defined firewall rulesets

# Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure the firewall to block internet access while allowing connections to an internal network (intranet or LAN).

Example scenarios:

- In your network at home, you want your child's computer to connect to other computers at home but disable their internet access for safety reasons
- In a company network, you want employee computers to connect to your network but disable internet access for bandwidth reasons

COMODO Creating Trust Online\*

You need to create a global firewall rule to block internet access while allowing internal connections.

### Create the global rule

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Firewall' > 'Global Rules'

COMODO Client - Se	curity 11							-	$\times$
🔠 tasks 🏠 settings	>								
	/			Scan		Į.	<b>Ø</b>		
COMODO Advanced S	Settings					?	-		$\times$
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> </ul>	-0-	obal Rules ing global rul	es are active	on this com	outer:				
Firewall Settings Application Rules	+ Add	۲. Edit	<b>X</b> Remove	t Move Up	<b>↓</b> Move Down				
Global Rules	E Ru	iles							Q
Rulesets		Allow All Out	going Reques	ts If The Targ	et Is In [Work #	¥1]			
Network Zones		Allow All Inco	oming Reques	ts If The Send	ler Is In [Work	#1]			
Portsets		Allow IP Out	From MAC Ar	iy To MAC An	y Where Proto	col Is Any	/		
✓ HIPS		Allow ICMPv4	4 In From MAG	C Any To MAG	C Any Where IC	CMP Mess	sage Is Ff	RAGMEI	NT
✓ Containment		Allow ICMPv4	4 In From MAG	C Any To MAG	C Any Where IC	MP Mess	sage Is TI	IME EXC	EE
<ul> <li>File Rating</li> <li>Advanced Protection</li> </ul>		Block IP In Fr	om MAC Any	To MAC Any	Where Protoco	ol Is Any			

3. Choose 'Add' from the options at the top.

COMODO Creating Trust Online\*

Antivirus	Global Rules	
Firewall	The following global rules are active on this computer:	
Firewall Settings Application Rules	+ X X t + Add Edit Remove Move Up Move Down	
Global Rules	Rules	
Rulesets	Allow All Outgoing Requests If The Target Is In [Work #1]	
сомодо	Firewall Rule ?	×
Action:	Allow   Log as firewall event if this rule is fired	
Protocol:	IP 💌	
Direction:	Out •	
Description	Allow Lan and block internet	
SOURCE ADDRESS	DESTINATION ADDRESS IP DETAILS	
Exclude (i.e. N	DESTINATION ADDRESS IP DETAILS	

- 4. Choose the following options from the respective drop-downs:
  - Action = 'Block';
  - Protocol = 'IP';
  - Direction = 'Out'.
- 5. Enter a description for the new rule in the 'Description' text box.
- 6. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter the IP address of the computer in the IP text box.
- 7. Click the 'Destination Address' tab, choose 'Network Zone' from the 'Type' drop-down and choose your local area network from the 'Zone' drop-down.

COMODO Creating Trust Online\*

сомодо	Firewall Rule ?	×
Action:	Allow   Log as firewall event if this rule is fired	
Protocol:	IP 🔹	
Direction:	Out 🔻	
Description	Allow Lan and block internet	
SOURCE ADDRESS	DESTINATION ADDRESS IP DETAILS	
Тур		
Zon	Loopback Zone Loopback Zone Work #1	
	OK CANC	EL

8. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.

SOURCE ADDRESS	DESTINATION ADDRESS	IP DETAILS
IP Protocol:	Any Custom Any TCP UDP ICMPv4 IGMP Raw IP PUP GGP GRE RSVP	• OK CANCEL
	ICMPv6	

COMODO Creating Trust Online\*

- 9. Click 'OK'. The created policy will be added to the list of 'Global Rules'.
- 10. Select the rule and click the 'Move Up' button until the rule is in first position:

COMODO Advance	ed Settings ? — 🗆 🗙
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Global Rules
<ul> <li>Firewall</li> <li>Firewall Settings</li> <li>Application Rules</li> </ul>	+ * t + Add Edit Remove Move Up Move Down
Global Rules Rulesets	Rules     Q       Image: Constraint of the second se
Network Zones	Allow All Outgoing Requests If The Target Is In [Work #1]
Portsets ✓ HIPS	Allow All Incoming Requests If The Sender Is In [Work #1]     Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
<ul> <li>Containment</li> <li>File Rating</li> </ul>	Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGMENT     Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE
✓ Advanced Protection	<ul> <li>Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE</li> <li>Block IP In From MAC Any To MAC Any Where Protocol Is Any</li> </ul>
	OK CANCEL

11. Click 'OK' for your configuration to take effect.

Your firewall is now configured to allow access to the internal network but to block internet access.

COMODO Creating Trust Online\*

### Set up HIPS for Maximum Security and Usability

This page explains how to configure the host intrusion prevention system (HIPS) to provide maximum security against malware and hackers.

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'HIPS' > 'HIPS Settings'
- 3. Select 'Enable HIPS'

COMODO Client -	Security 11			_	×
🔠 tasks 🏠 setting	s				
	7	Scan	View Quar	] antine	
COMODO Advance	d Settings		? –		×
<ul><li>General Settings</li><li>Antivirus</li></ul>	HIPS Settings				
<ul> <li>Firewall</li> <li>HIPS</li> </ul>	Paranoid Mode Monit				
HIPS Settings HIPS Rules		st Intrusion Protection System tivities to protect the comput Allow Requests 🔻			5
Rulesets Protected Objects	<ul> <li>Set popup alerts to verbos</li> <li>Create rules for safe applic</li> </ul>				

4. Choose 'Safe Mode' from the drop-down.

### **Monitoring Settings**

1. Click the 'Monitoring Settings' link in the 'HIPS Settings' interface

Creating Trust Online\*

HIPS Settings	
✓ Enable HIPS	
Safe Mode Mor	nitoring Settings
	he Host Intrusion Protection System, the component that monitor em activities to protect the computer against malware actions.
	ettings ?
Activities to Monitor	
Interprocess Memory Access	es Process Execution
☑ Windows/WinEvent Hooks	☑ Window Messages
Device Driver Installations	DNS/RPC Client Service
Processes' Terminations	
Objects to Monitor Agains	t Modifications
Protected COM Interfaces	Protected Registry Keys
Protected Files/Folders	
Objects to Monitor Agains	t Direct Access
Physical Memory	☑ Disks
Computer Monitor	🗹 Keyboard

2. Make sure that all the check boxes are selected then click 'OK'

### **Advanced Settings**

1. Enable the following settings in the 'Advanced' area of the HIPS Settings interface:

Advanced
Enable adaptive mode under low system resources
Block all unknown requests when the application is not running
Enable enhanced protection mode (Requires a system restart)

 Enable 'Block all unknown requests if the application is not running' (Optional) - Selecting this option blocks all unknown execution requests if Comodo Client Security 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 CCS security settings, then it is 'OK' to leave this box unchecked.

COMODO Creating Trust Online\*

- Select 'Enable enhanced protection mode (Requires a system restart)' If you are using a 64-bit system, in
  order to maximize the security, it is important to enable this mode to activate additional host intrusion
  prevention techniques in HIPS 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 CCS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS functionality.

#### Click here for more details on HIPS Settings

### Create Rules to Auto-Contain Applications

- Click 'Settings' > 'Containment' > 'Auto-Containment'
- Auto-containment rules let you define which types of files should automatically run in the container.
- You can contain files based on various criteria, including location and file source.
- A contained application has much less opportunity to damage your computer because it runs isolated from your operating system and your files.
- CCS ships with some pre-defined rules configured to provide maximum protection for your system. Click here to check whether these rules meet your needs before creating a custom rule.
- The rest of this tutorial explains how to create a custom auto-containment rule.

### Create auto-containment rules

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Containment' > 'Auto-Containment'
- 3. Make sure 'Enable Auto-Containment' is selected
- 4. Click 'Add'

COMODO Creating Trust Online\*

COMODO Client - Security	11						-	×
🔠 TASKS 🔅 SETTINGS								
			Scan		View	نې Ouarant	ine	
COMODO Advanced Settings					?	-		×
<ul> <li>✓ General Settings</li> <li>✓ Antivirus</li> </ul>	Auto-Containm	ient						
✓ Firewall	able Auto-Contain his option enables au policy defined below.		tainment of e	xecutable fil	es and scri	pts accord	ding to t	he
- Containment Containment Settings Auto-Containment	ed Edit	X Remove Q Tar	t Move Up rget	Move Dow	Dela	to ult	e Rule	*
✓ File Rating	🔝 Run Virtually	6	C:\Program I	il Any				
COMODO Manage Co	ontained Program				?		×	
Action Run Virtually						•	•	
The selected containment action	on will be applied	l if file pro	perties mat	ch the fol	owing c	riteria:		
CRITERIA OPTIONS								
					Edi	it		
No criteria selected								
			ок		CA	NCEL		

The add rule screen contains two tabs:

- Criteria Define the conditions of the rule.
- Options Configure additional actions like logging, memory usage and time restrictions.

There are three steps:

- Step 1 Choose the action
- Step 2 Select the rule targets
- Step 3 Choose additional options

COMODO Creating Trust Online\*

### Step 1 - Choose the action

The setting in the action drop-down combined with the restriction level in the options tab determine the privileges of an auto-contained application. These items specify what right the application has to access other processes and hardware resources.

сом	COMODO Manage Contained Program			
Action	Run Virtually			$\bigcirc$
	Run Restricted			$\forall$
The select	Run Virtually Block			
CRITERIA				

Choose one of the following actions:

- **Run Virtually** The application will run in a virtual environment, completely isolated from your operating system and the rest of your files.
- **Run Restricted** The application is allowed limited access to operating system resources. The application is not allowed to execute more than 10 processes at a time. Some applications, like games, may not work properly under this setting.
- Block The application is not allowed to run at all.
- Ignore The application is not contained. It is allowed to run as normal on your computer.

### Step 2 - Select the rule targets

- Next, select the types of files which will be covered by your rule.
- You can add rule filters so the rule only applies to specific types of file.
  - For example, you can specify 'All executables' as the target and add a filter so it only affects executables downloaded from the internet.
  - Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target and 'File created by specific user' as the filter criteria.

#### Select targets and filters

- Click the 'Criteria' tab.
- Click the 'Edit' button at the far right:

COMODO Creating Trust Online\*

COMODO Manage Contained Program	?		×
Action Run Virtually			Ŧ
The selected containment action will be applied if file properties match the follo	owing	criteria	:
CRITERIA OPTIONS			
	E	dit	$\triangleright$
No criteria selected			38
COMODO File Criteria ?		×	
Please select the criteria to be applied.			
File location:			
В	rowse	•	
File created by applications: Any Ad	d 🔻	^	
File started by processes: Any Ad	d 🔻	$\checkmark$	
File created by users: Any Ad	d	$\sim$	
File origin: Any Ad	d 🔻	$\sim$	
File rating: Any Sele	ct 🔻	$\sim$	
File signed by vendors: Any Ad	d 🔻	$\sim$	
File age: Any Sele	ct	$\checkmark$	
ок с			

Next:

- Select the target
- Configure the filters

COMODO Creating Trust Online\*

### Select the target

• Click the browse button next to the file location field:

COMODO File Criteria		?	×
Please select the criteria to be applied.			
File location:		Browse	•
File created by applications:	Any	Files Runk File G	g Processes
		Folde File H	r

Select one of the following target types:

- Files Add individual files as the target.
- **Running Processes** Add any process that is currently running on your computer. This targets the parent application of the process.
- File Groups Add a predefined file group as the target. For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- Folder Add a directory or drive as the target. All files in the target folder are covered by the rule.
- File Hash Add a file's hash value as the target of the rule. A hash value is a number derived from the file itself, which uniquely identifies and represents the file. It is extremely unlikely that two files can ever generate the same hash value. The rule will apply to the target file, even if the file name changes.
- Process Hash Add a processes hash value as the target of the rule. Please see description above if required.

#### Add an individual File

• Choose 'Files' from the 'Browse' drop-down.

COMODO Creating Trust Online

сомодо	File Cri	teria		? ×		
Please select the c	riteria to	be applied.				
File location:						
				Browse		
File created by app	olications		Any	Files		
				Runt g Processes		
	in the second			Folder		
				File Hash		
				Process Hash		
					<u></u>	
🔄 Open					×	
← → • ↑ 📙 •	« Progra	m Files (x86) > Cuckoo	ٽ ~	Search Cuckoo	م	
Organize 🔻 New	folder				- 🔟 🕐	
💪 OneDrive	1	Name ^	Date modified	Туре	Size	
💻 This PC		Converters	5/28/2018 1:51 P	M File folder		
3D Objects	10.000	Cuckoo_music	5/28/2018 1:39 P	M Application	1 KB	
Desktop		🖏 helper	5/28/2018 12:03	PM Application	875 KB	
Documents						
Downloads						
Music						
Pictures						
Videos						
Local Disk (C:)						
👝 New Volume (E	:)					
	~					
	File name	Cuckoo_music	~	Executable Files (*	.exe, *.dll, *.or ~	
		[				
				<u>O</u> pen  ▼	Cancel	

- Navigate to the target file and click open
- The file will be added as the target and run as per the action chosen in Step 1.

COMODO Creating Trust Online\*

COMODO File Criteria		?		×
Please select the criteria to be applied.				
File location:				
C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe		Bro	owse	•
File created by applications:	Any	Add	•	^
File started by processes:	Any	Add	•	~
File created by users:	Any	Add		V
File origin:	Any	Add	T	$\sim$
File rating:	Any	Selec	t 🔻	v
File signed by vendors:	Any	Add	T	$\checkmark$
File age:	Any	Selec	t	$\checkmark$
ок			NCEL	

- Click 'OK' if you don't want to specify any filters or options.
- If required ,you can **configure filter criteria and file rating** and **options** for the rule.

### Add a currently running process

• Choose 'Running Processes' from the drop-down:

COMODO Creating Trust Online\*

Please select the criteria to be applied.	
File location:	
	Browse 🔻
	Files
File created by applications:	Any Running Processe
	Folder
	File Hash
	Process Hash
COMODO Browse for Processes	? ×
Application	PID
LEI KUNTIMEBROKER.exe	3904
fontdrvhost.exe	724
svchost.exe	1592
ctfmon.exe	3184
svchost.exe	1112
RmmService.exe	2188
	3248
	5004
🔺 🧐 VBoxTray.exe	
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> </ul>	4916
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> </ul>	4916 1968
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>Mspaint.exe</li> </ul>	
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>mspaint.exe</li> <li>System</li> </ul>	1968
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>Mspaint.exe</li> </ul>	1968 4328
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>mspaint.exe</li> <li>System</li> <li>smss.exe</li> </ul>	1968 4328 4
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>Imspaint.exe</li> <li>System</li> <li>smss.exe</li> <li>svchost.exe</li> </ul>	1968 4328 4 320
<ul> <li>MSASCuiLexe</li> <li>OneDrive.exe</li> <li>Imspaint.exe</li> <li>System</li> </ul>	1968 4328 4 320 1060
<ul> <li>VBoxTray.exe</li> <li>MSASCuiL.exe</li> <li>OneDrive.exe</li> <li>mspaint.exe</li> <li>System</li> <li>smss.exe</li> <li>swchost.exe</li> <li>VBoxService.exe</li> </ul>	1968 4328 4 320 1060 8

- Select the process belonging to the parent application you want to add and click 'OK'.
- The parent application of the process will be added as the target.

COMODO Creating Trust Online\*

COMODO File Criteria	?		×
Please select the criteria to be applied.			
File location:			
C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe		Browse	•
File created by applications: Any	/	Add 🔻	^
File started by processes: An	у	Add 🔻	~
File created by users: An	y	Add	$\sim$
File origin: An	y	Add 🔻	$\sim$
File rating: An	y 🔤	Select 🔻	$\sim$
File signed by vendors: An	y	Add 🔻	~
File age: An	y	Select	~
ОК		CANCE	L

- Click 'OK' if you don't want to specify any filters or options.
- If required ,you can configure filter criteria and file rating and options for the rule.

### Add a file group

- Choose 'File Groups' from the drop-down.
  - For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- Select the file group you want to target with the rule:

COMODO Creating Trust Online

COMODO File Criteria	?	×
Please select the criteria to be applied.		Executables
File location:		All Applications
	Browse	
	Files	Windows System Applications
File created by applications:		ng Processes Windows Management
the decide of opprovide of	- North	roups 3rd Party Protocol Drivers
	Folder	
	File H	
		ss Hash File Archivers
	Proce	Temporary Files
		File Downloaders
		Suspicious Locations
File started by processes:	Any Add 🔻	Containment Folders
File created by users:	Any Add	Pseudo File Downloaders
rile created by users.	Any Add	Important Files/Folders
File origin:	Any Add 🗸	V Web Browsers
elle antione	Colort -	Browser Plugins
File rating:	Any Select 🔻	Management and Productivity Applications
File signed by vendors:	Any Add 🗸	V Media Players
		COMODO Client - Security
ile age:	Any Select	COMODO Client - Security Manager
		COMODO Client Files/Folders
	OK CANCEL	COMODO Client - Communication
		Startup Folders
		exclusive
		exclusion
		malware
		firewall event
		Antivirus Exclusion
		HIPS exclusion1
		Shared Spaces

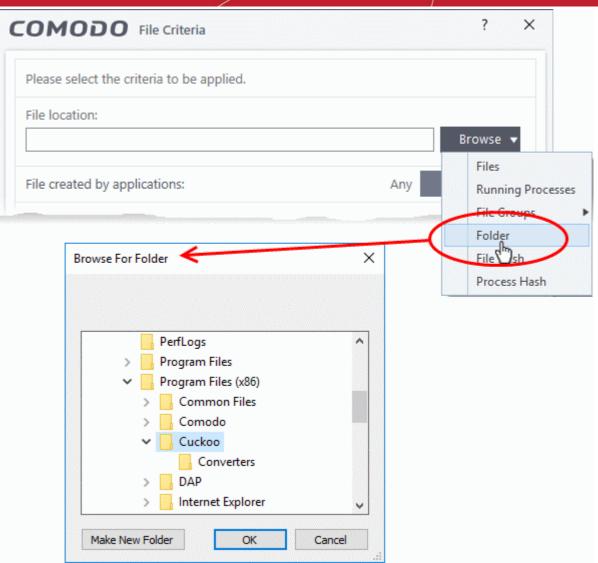
• Click 'OK' if you don't want to specify any filters or options.

• If required, you can configure filter criteria and file rating and options for the rule.

### Add a folder/drive partition

• Choose 'Folder' from the 'Browse' drop-down.

COMODO Creating Trust Online\*



- Navigate to the drive partition or folder you want to add as target and click 'OK'
- Click 'OK', if you don't want to specify any filters or options.
- If required you can configure filter criteria and file rating and Options for the rule.

### Add a file using its hash value

• Choose 'File Hash' from the drop-down.

COMODO

сомодо	) File (	Criteria		? ×	
Please select the o	criteria	to be applied.			
File location:					
File created by ap	plicatio	ons:	Any	Browse ▼ Files Running Processes File Groups Folder File Hash Process Hash	•
	« Pro <u>c</u> v folder	yram Files (x86) → Cuckoo →	ڻ ~	Search Cuckoo	× م
OneDrive	^	Name	Date modified	Туре	Size
_		Converters	5/28/2018 1:51 P	M File folder	
This PC		Cuckoo_music	5/28/2018 1:39 P	M Application	1 KB
3D Objects Desktop		🖏 helper	5/28/2018 12:03	PM Application	875 KB
Documents					
Downloads					
Music					
Pictures					
Videos					
Local Disk (C:)					
🚃 New Volume (I	E:)				
- M.L	Ť				
	File <u>n</u> ar	ne: Cuckoo_music	~	Executable Files (*.	exe, *.dll, *.or ~
				<u>O</u> pen   <del>▼</del>	Cancel

- Navigate to the file whose hash value you want to add as target and click 'Open'
- Click 'OK', if you don't want to specify any filters or options.
- If required you can **configure filter criteria and file rating** and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

#### Add an application from a running process based on its hash value

• Choose 'Process Hash' from the drop-down.

COMODO Creating Trust Online\*

COMODO File Criteria		? X	
Please select the criteria to be applied.			
File location:			
		Browse 🔻	
File created by applications:	Any	Files Running Proce File Groups Folder File Hash	sses
	5	Process Hash	>
COMODO Browse for Processes		?	×
Application		PID	
▲ 📝 ctfmon.exe		3184	^
✓ sychost.exe		1112	
<ul> <li>RmmService.exe</li> </ul>		2188	
🔻 🐂 explorer.exe		3248	
✓ Image: A state of the sta		5004	
▲ 🖶 MSASCuiL.exe		4916	
🖌 🦳 OneDrive.exe		1968	
🖌 🚳 mspaint.exe		4328	
▼ System		4	
smss.exe		320	
svchost.exe		1060	
4 🥸 VBoxService.exe		8	
Cuckoo_music.exe		732	
▲ 📧 svchost.exe		1600	
🖌 📇 SearchIndexer.exe		936	
<ul> <li>WmiPrvSE.exe</li> </ul>		4984	
🖌 😨 ITSMAaent.exe		2004	~
	ОК	CANCEL	

- Select the process, to add the hash value of its parent application to target and click 'OK' from the 'Browse for Process' dialog.
- Click 'OK', if you don't want to specify any filters or options.
- If required you can **configure filter criteria and file rating** and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.

COMODO

• CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

### **Configure Filter Criteria and File Rating**

You can apply an action to a file if it meets certain criteria.

The available filter criteria are:

- By application that created the file
- By process that created the file
- By user that created the file
- By file origin
- By file rating
- By vendor who signed the file
- By file age

#### Auto-contain a file if it was created by a specific application

- This will apply the rule to a file based on its parent application.
- You can also specify the file rating of the parent application. The rule will then only contain a file if the parent app has a certain trust rating.

Specify parent applications:

• Click the add button in the 'File created by applications' stripe:

COMODO File Criteria	?		×
Please select the criteria to be applied.			
File Belongs to (File Group):			
Temporary Files		Browse	•
File created by applications:	AIV A	Add 🔻	
		Files Run Øg P	rocesses
		File Group	IS
		Folder File Hash	
		Process H	ash

- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.
- · Click the 'Any' link beside 'File Rating' and select the file rating of the source

Creating Trust Online\*

сомо	<b>DO</b> File Criteria			?		×
Please sele	ect the criteria to be app	lied.				
File Belong	gs to (File Group):					
Temporal	ry Files				Browse	•
File created	d by applications:	1	process(es)	A	dd 🔻	^
Executat File Rati	<u> </u>				:	×
	Any					
	Trusted					
	Unrecognized	and a state of the second state of the				
	Malicious 🖑					

• Repeat the process to add more applications or groups/folders.

#### Auto-contain a file if it was launched by a specific process

- This will apply the rule to a file based on its based on its parent process.
- You can also specify:
  - The trust rating of the parent process. The rule will then only contain a file if the parent process has a certain trust rating.
  - The number of levels in the process chain that should be inspected.

#### Specify source process:

• Click the 'Add' button in the 'File started processes' stripe:

OMODO File Criteria	? 🗆 X
Please select the criteria to be applied.	
File Belongs to (File Group):	
Temporary Files	Browse 🔻
File created by applications:	Any Add 🗸 🗸
File started by processes:	Any Add 🗸 🔨
	Files
	Running Processe
	File Groops
	Folder
	File Hash
	Process Hash

- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.
- · Click the 'Any' link beside 'File Rating' and select the file rating of the source

ed by processe	1 process(es)	Add 🔻	1
wnloaders ting: <u>Any</u>			×
nit Any Truste Unrec Malici	rocesses in the process chain to	1	
	zed		

• 'Limit number of parent processes in the process chain to' - Specify how far up the process tree CCS should check. 1 = will only check the trust rating of the file's parent process. 2 = will check the trust rating of the parent process and the grand-parent process. Etc.

File created by applications:	Any	Add	<b>•</b> •
File started by processes:	1 process(es)	Add	<b>·</b> ^
File Downloaders			×
File Rating: <u>Any</u>			~
☑ Limit number of parent process	ses in the process chain to	3 📫	>

Repeat the process to add more processes

### Auto-contain a file created by specific users

• Click the 'Add' button in the 'File created by users' stripe.

ating Trust Onlin

COMODO Creating Trust Online\*

Please select the criteria to be applied.	
File Belongs to (File Group):	
Temporary Files	Bro
ile created by applications:	Any Add
File started by processes:	Any Add
File created by users:	Any Add
Select User or Group	
Select User or Group Select this object type: User, Group, or Built-in security principal	
Select this object type:	
Select this object type: User, Group, or Built-in security principal	
Select this object type: User, Group, or Built-in security principal From this location:	Object Types
Select this object type: User, Group, or Built-in security principal From this location: DESKTOP-FKQF9QT	Object Types
Select this object type: User, Group, or Built-in security principal From this location: DESKTOP-FKQF9QT	Object Types

- Enter the names of the users you want to add in the large text box.
- Name format = <domain name>\<user/group name>, or <user/group name>@<domain name>.
- Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm your choice.

COMODO Creating Trust Online\*

Coloct this object t	hee:			
Select this object t User Group or B	type: uilt-in security principal		Object Types	
			Object Types	
From this location: DESKTOP-1N2U			Landbara	
DESITIOF*11V20	550		Locations	
Enter the object na	ame to select ( <u>examples</u> ):			
			Check Names	
	< · · · · · · · · · · · · · · · · · · ·			
Advanced		ОК	Cancel	
1				
elect User or Gr	0.00			
elect User or Gro	oab			
Select this object t	lype:			
User, Group, or B	uilt-in security principal		Object Typ	
From this location:				
DESKTOP-1N2U	S38		Locations	
C				
Common Queries	3			
Name:	Starts with 🖂			
Description	Ch			
Description:	Starts with 🖂			
Disabled ac	counts			
Non expiring	g password			
Days since last	t logon:			
2 290 01100 1201				
			014	
Search results:			ОК	
	In Folder		ОК	
Name			ОК	
Name Distributed C Event Log Re			ОК	
Everyone	DESKTOP-1N2 DESKTOP-1N2		OK	
Vame Distributed C Event Log Re Everyone Guest	DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2		ОК	
Vame Distributed C Event Log Re Everyone Guest Guests	DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2		ОК	
Vame Distributed C Event Log Re Everyone Guest Guests Hyper-V Admi	DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2		OK	
Name Distributed C Event Log Re Everyone Guest Guests Hyper-V Admi IIS_IUSRS	DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2		ОК	
Vame Distributed C Event Log Re Everyone Guest Guests Hyper-V Admi IIS_IUSRS infra	DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2 DESKTOP-1N2		OK	

The user will be added to the list.

Creating Trust Online\*

COMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files		ĺ	Browse	T
File created by applications:	Any	Ac	ld 🔻	$\sim$
File started by processes:	Any	Ad	ld 🔻	$\sim$
File created by users:	1 user(s)	Ac	ld	^
Guests				×

• Repeat the process to add more users.

### Auto-contain a file if it was downloaded/copied from a specific source

• Click the 'Add' button in the 'File origin' stripe.

COMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files			Browse	•
File created by applications:	Any	Ac	ld 🔻	$\sim$
File started by processes:	Any	Ac	ld 🔻	$\sim$
File created by users:	1 user(s)	Ac	ld	$\sim$
File origin:	Any	Ac	ld 🔻	^
		h	nternet	
			le Val	ole Med

- Choose the source from the options:
  - Internet Apply the rule to files that were downloaded from the internet.
  - **Removable Media** Apply the rule to items copied to your computer from removable storage devices.
  - Intranet Apply the rule to files downloaded from the local intranet.
- Repeat the process to add more sources

### Select file rating as filter criteria

COMODO

COMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files		В	rowse	•
File created by applications:	Any	Ado	l 🔻	$\checkmark$
File started by processes:	Any	Ado	l 🔻	$\checkmark$
File created by users:	1 user(s)	Ado	ł	$\checkmark$
File origin:	2 origin(s)	Ado	l 🔻	$\checkmark$
File rating:	Any	Sele	ct 🔻	^
		Tri	usted	
		Ur	recogi	nized

- Trusted A file will have a trusted rating if:
  - The file is on the Comodo whitelist of safe files
  - The file is signed by a vendor who has a trusted rating in 'Settings' > 'File Rating' > 'Vendor List'
  - The file was installed by trusted installer
  - The user has given the file a trusted rating in 'Settings' > 'File Rating' > 'File List'
  - See File Rating Settings for more information.
- Malware The file has a trust rating of 'Malicious'.
- **Unrecognized** Any file that does not have a 'Trusted' or 'Malicious' rating is classed as 'Unrecognized'. Although these files may not turn out to be malicious, Comodo auto-contains these files until we have established their true trust rating.

### Auto-contain a file based on software vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.
- You can also specify the trust rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

Choose vendors:

• Click the 'Add' button in the 'File signed by vendors' stripe.

COMODO Creating Trust Online\*

COMODO File Criteria		?		×
Please select the criteria to be applied.				
File Belongs to (File Group):				
Temporary Files		В	rowse	•
File created by applications:	Any	Ado	d 🔻	$\mathbf{v}$
File started by processes:	Any	Ado	d 🔻	$\sim$
File created by users:	1 user(s)	Ado	d	$\sim$
File origin:	2 origin(s)	Ado	d 🔻	$\mathbf{v}$
File rating:	Unrecognized	Sele	ct 🔻	$\mathbf{v}$
File signed by vendors:	Any	Ado راس	d 🔻	^
		V Ve Fil	le Sign	rom Vendo er Process Sig

There are three ways you can add a vendor:

### 1. Directly select a vendor

- Choose 'Vendor from a Vendor List' from the drop-down
- The 'Add Vendor' dialog opens with a list of vendors in the Vendor List

Creating Trust Online\*

Vendor	Q	Rated By	Ţ	Rating	Ţ	1
Itannex B.V.		Comodo		✓ Trusted		
Neo IT Solutions Ltd.		Comodo		✓ Trusted		
Festo Didactic SE		Comodo		✓ Trusted		
FTPPro.com		Comodo		✓ Trusted		
Timo Bingmann		Comodo		✓ Trusted		
Shearwell Data Ltd		Comodo		✓ Trusted		
Boyishsoft		Comodo		✓ Trusted		
Integrated Scuba Systems, IIc		Comodo		✓ Trusted		
TeacherWeb, Inc.		Comodo		✓ Trusted		

- · Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

### 2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CCS identifies the vendor of the file and adds the to the rule.
- The rule will apply to files digitally signed by the vendor.

### 3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CCS identifies the vendor of the process and adds the to the rule.
- The rule will apply to files digitally signed by the vendor.

The selected vendor is added:

Creating Trust Online\*

File rating:	Unrecognized Select 🗸 🗸
File signed by vendors:	1 vendor(s) Add 🗸 🔨
Girlssoft Vendor Rating: <u>Any</u>	×

- **Vendor Rating** The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.
  - Example. If you select 'Trusted' here, then CCS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.

File rating:		Unrecognized Select	• •
File signed by ve	endors:	1 vendor(s) Add	<b>·</b> ^
Girlssoft Vendor Rating	g: <u>Any</u>		×
	Any Trusted Unrecognized Malicious		

• Repeat the process to add more vendors

### Set the file age as filter criteria

• Click the 'Select' button in the 'File age' stripe.

COMODO Creating Trust Online\*

COMODO File Criteria	? 🗆 X
Please select the criteria to be applied.	
File location:	Browse 🔻
	Browse 🗸
File created by applications:	Any Add 🔻 🗸
File started by processes:	Any Add 🔻 🗸
File created by users:	Any Add 🗸
File origin:	Any Add 🗸 🗸
File rating:	Any Select 🔻 🗸
File signed by vendors:	Any Add 🗸 🗸
File age:	Ary Select
COMODO File age:	? ×
<ul> <li>File creation date:</li> <li>Before</li></ul>	
Before V 04/15/2019 V 4:11:24 PM V	
O File age: Less Than ▼ 1   day(s) ▼	
ОК	CANCEL

You can set the file age in two ways:

- File Creation Date To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- File age To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - Less Than CCS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

COMODO Creating Trust Online\*

- **More Than** CCS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)
- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.

сомор	Manage Contained Program		?		×
Action Run Vi	rtually				•
The selected con	tainment action will be applied if file prope	erties match the fo	llowing	g criteria	:
CRITERIA O	PTIONS				
				Edit	
File Belongs to Temporary Fi					
File created by Guests	users:				
File origin: Removable M Internet	1edia				
File rating: Unrecognized	d				
File signed by v Girlssoft Vendor Ratin					
		ОК		CANCEL	

### Step 3 - Select the Options

•

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

• Click the 'Options' tab.

Creating Trust Online\*

COMODO Manage Contained Program	?		×
Action Run Virtually The selected containment action will be applied if file properties match the fol	llowing	criteria	•
CRITERIA OPTIONS			
Log when this action is performed			
Set Restriction Level Partially Limited V			
□ Limit maximum memory consumption to 1 ▲ MB			
Limit program execution time to 1 secs			
ок	C	ANCEL	

The options will be displayed, depending on the 'Action' chosen in Step 1.

The options available for 'Ignore' action are:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS containment logs.
- Don't apply the selected action to child processes Child processes are the processes launched by the
  application. CCS treats all child processes as individual processes and forces them to run as per the file
  rating and the containment rules.
  - By default, this option is not enabled and the 'Ignore' rule will also apply to child process of the target application(s).
  - If this option is enabled then the 'Ignore' rule will be applied only to the target application. Any child processes will be checked and containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

The options available for 'Run Restricted' and 'Run Virtually' actions are:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS containment logs.
- Set Restriction Level When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
  - Partially Limited The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. (*Default*)
  - Limited Only selected operating system resources can be accessed by the application. The

application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.

- Restricted The application is allowed to access very few operating system resources. The application
  is not allowed to execute more than 10 processes at a time and is run with very limited access rights.
  Some applications, like computer games, may not work properly under this setting.
- **Untrusted** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
- Limit maximum memory consumption to Enter the memory consumption value in MB that the process should be allowed.
- Limit program execution time to Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For 'Block' action, the following options are available:

- Log when this action is performed Whenever this rule is applied for the action, it will be added to CCS containment logs.
- Quarantine program If checked, the programs will be automatically quarantined. See Manage Quarantined Items for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.

COMODO Advanced	Settings		? – 🗆 ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> </ul>	Auto-Containme Enable Auto-Containme This option enables autor policy defined below.		iles and scripts according to the
— Containment	+ 2	X I I	c.
Containment Settings	Add Edit	Remove Move Up Move Dov	wn Default
Auto-Containment	Action	Q Target Q Re	putation Q Enable Rule
Protected Objects	🗹 🛓 Run Virtually	🖺 Temporary Files Un	recognized
Virtual Desktop	🗌 🖉 Block	All Applications Ma	ilicious
✓ File Rating	🗌 🥥 Block	🖺 Suspicious Loca An	y 💽
<ul> <li>Advanced Protection</li> </ul>	🗌 🥝 Block	🖺 Containment Fo An	y 💽
	□ → Ignore	Communication Tru	isted
	□ → Ignore	Metro Apps Ang	y 💽
	🗌 🛃 Run Virtually	All Applications Un	recognized
	🗌 🥥 Block	Pseudo File Do An	у 💽
		ок	CANCEL

COMODO Creating Trust Online\*

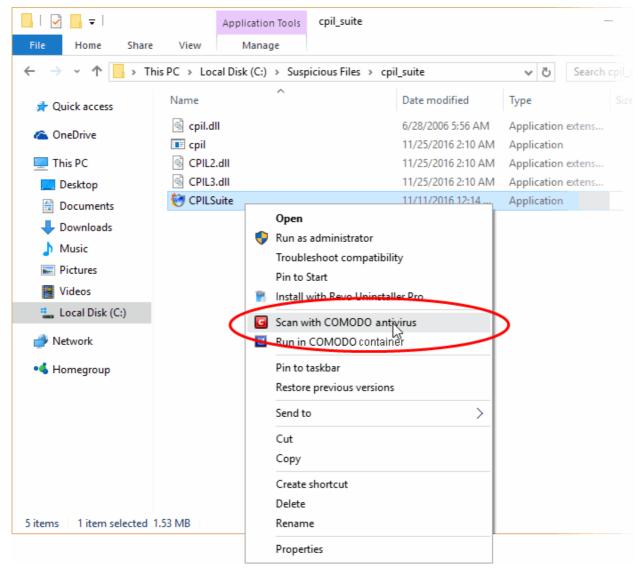
**Important Note:** Please make sure the auto-containment rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail. You can restore the rules to default rules at any time by clicking the 'Reset to Default' button at the top.

### 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 the item and select 'Scan with COMODO Antivirus' from the context sensitive 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.

Click 'Settings' > 'Antivirus' > 'Scans', then open the 'Full Scan' profile to view these thresholds.

Scan results an	e shown when the scan finishes:						
	can			?	—		×
100%	TASK: C:\Old Man Apps\poison1\haza STATUS: Scan Finished ELAPSED TIME: 00:00:07	rd.bin					
THREAT(S) FOUND	e:1 🛞 SKIPPED FILES: 0						
Threat Name		Q	Action	Clean		•	
Malware@#3fxg8e8	df3its						
C:\Old Man A	Apps\poison1\hazard.bin		🗸 Clea	an		•	
CLOSE	puter if no threats are found at the en	d of the sca	an	APPLY	SELECTE	D ACTIO	NS

Click here for more details to take action on the infected item(s).

### Create an Antivirus Scan Schedule

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'
- 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.

### Create a scan schedule

- 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:

COMODO Creating Trust Online\*

COMOL	O Scan			? ×
	Quick Scan cans commonly infected a	reas and memor	у.	LAST SCAN: 29-05-2019
X6	<b>Custom Scan</b> can files and folders or rur	n custom scan pr	ofiles.	~
	older Scan elect and scan a folder.			
	ile Scan elect and scan a file.			
	fore Scan Options			
		Ð		
	un custom scan profiles.	. <sup>™</sup>		? - □
R	un custom scan profiles.			? – 🗆
COMODO Adva	anced Settings	V		
COMODO Adva General Settings Antivirus	anced Settings Cons This page allows you to	add, remove an		
COMODO Adva General Settings Antivirus Realtime Scan Scans	anced Settings Consection Consect	add, remove an Remove	d edit scan profile	s and scheduled sca
COMODO Adva General Settings Antivirus Realtime Scan Scans	anced Settings Cons This page allows you to	add, remove an		

Tip: You can also get to this screen by clicking 'Settings' > 'Antivirus' > 'Scans'.

• Click 'Add' to create a new custom scan profile.

COMODO Creating Trust Online\*

сомо									×
Scan Name:	Old man do	ocuments							
Define items		l, scanning op SCHEDULE	tions and run	ning schedule					
[ <b>∔</b> Add Files	Add Folder	🖾 Add Area	X Remove						
Pro	file								
						ОК	C	ANCEL	

First, create a name for the profile. The next steps are:

- Select the items to be scan
- Configure scan options for the profile (optional)
- Configure a scan schedule (optional)

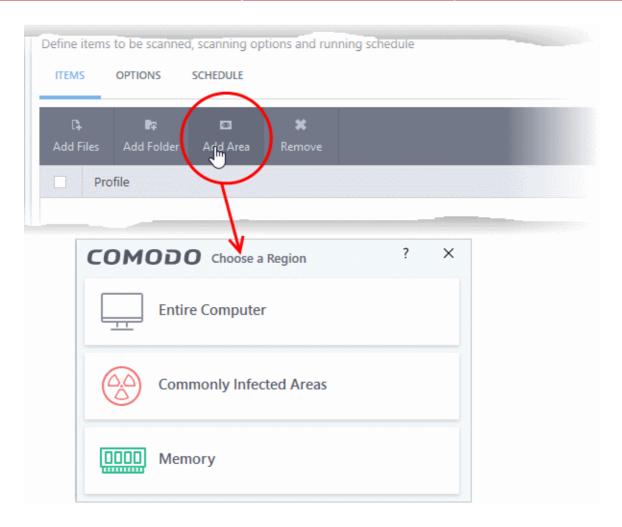
### Select items to scan

• 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' and 'System Memory'. See screenshot below:

COMODO Creating Trust Online\*



• Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

### **Configure scan options**

· Click 'Options' at the top of the 'Scan' interface

COMODO Creating Trust Online\*

can Name:	
Define items	to be scanned, scanning options and running schedule
ITEMS	OPTIONS SCHEDULE
🗹 Decompi	ess and scan compressed files
This optio	n allows scanner to decompress archive files e.gzip, .rar, etc. during scanning
Use cloue	d while scanning
This optio	n allows scanner to connect to cloud to query file ratings
Automat	cally clean threats  Quarantine Threats
When the	threats are identified, perform the selected action automatically
Show sca	n results window
	n enables to view results of scans launched as per schedule or from the management portal, as well as e media scans.
🗹 Use heur	istics scanning Low 🔻
Use the se	elected level of sensitivity while scanning heuristically
🗹 Limit ma	kimum file size to 40 MB
While sca	nning, if a file size is larger than specified, it is not scanned
Run this	scan with Background 🔻
Priority of	scanner determines how much of the computer resources are used among other tasks
🗹 Update v	irus database before running
This optio	n makes sure the database is updated before running the scan
Detect p	otentially unwanted applications
Potentially download	y unwanted applications are programs that are unwanted despite the possibility that users consented to them.
Apply thi	s action to suspicious autorun processes Terminate and Disable 💌
	ed action will be automatically applied if unrecognized Windows services, autostart entries or I tasks are detected.
Limit scan t	ime of a single file to 9 📄 min(s)
When the	set time limit is reached, the file will be skipped and antivirus will proceed scanning other files.
	OK CANCEL
	OK CANCEL

- Use cloud while scanning Improves accuracy by augmenting the local scan with an online lookup of Compdeia latest view database. This means CCS can datest the latest malware even if your.
- up of Comodo's latest virus database. This means CCS can detect the latest malware even if your virus database is out-dated. (*Default = Disabled*).
- Automatically clean threats Select whether or not CCS should automatically remove any malware found by the scan. (*Default = Enabled*).

- Disabled = Results are shown at the end of the scan with a list of any identified threats. You
  can manually deal with each threat in the results screen. See Process Infected Files for
  guidance on manually handling detected threats.
- **Enabled** = Threats are handled automatically. Choose the action that CCS should automatically take:
  - Quarantine Threats Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See 'Manage Quarantined Items' for more details.
  - Disinfect Threats If a disinfection routine exists, CCS will remove the virus and keep the original file. If not, the file will be quarantined. (*Default*)
- Show scan results window You will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.
- Use heuristic scanning Select whether or not heuristic techniques should be used in scans on this profile. You can also set the heuristic sensitivity level. (*Default = Enabled*).

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

If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

• Low - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

Despite the name, this setting combines a very high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (*Default*)

- **Medium** Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.
- Limit maximum file size to Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (*Default = 40 MB*).
- Run this scan with If enabled, you can set the priority of scans on this profile The available
  options are:
  - High
  - Normal
  - Low
  - Background
  - Disabled = The scan will be run in the background (Default)
- Update virus database before running CCS checks for and downloads the latest virus signatures before starting a scan. (*Default = Enabled*).
- Detect potentially unwanted applications The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility 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 your activity on the internet. (Default = Enabled).
- Apply this action to suspicious autorun processes Specify how CCS should handle unrecognized auto-run items, Windows services and scheduled tasks.
  - Ignore The item is allowed to run (Default)
  - Terminate CCS stops the process / service

COMODO Creating Trust Online\*

- **Terminate and Disable** Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- Quarantine and Disable Auto-run processes are quarantined and the corresponding autorun entry removed. In the case of a service, CCS disables the service.

Note 1 - This setting only protects the registry during the on-demand scan itself. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

See Miscellaneous Settings for more details

Note 2 - CCS runs script analysis on certain applications to protect their registry records. You can manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See 'Autorun Scans' in Script Analysis Settings for more details.
- **Limit scan time of a single file to** Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

#### Schedule the scan

• Click 'Schedule' at the top of the 'Scan' interface

COMODO Scan	?		×
Scan Name:			
Define items to be scanned, scanning options and running schedule			
ITEMS OPTIONS SCHEDULE			
Frequency:			^
Do not schedule this task			
O Every few hours			
O Every Day			
O Every Week			
O Every Month			
Additional Options			
Run only when computer is not running on battery			
Run only when computer is IDLE			
Turn off computer if no threats are found at the end of the scan			
Run during Windows Automatic Maintenance			~
ок		CANCEL	

- Do not schedule this task The scan profile is created but not run automatically. The profile will be available for on-demand scans.
- Every few hours Run the scan at the frequency set in 'Repeat scan every NN hour(s)'
- Every Day Run the scan every day at the time specified in the 'Start Time' field.

- Every Week Run the scan on the days specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- Every Month Run the scan on the dates specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery** The scan only runs when the computer is plugged into the power supply. This is useful when you are using a laptop or other mobile device.
- Run only when computer is IDLE The scan only runs if the computer is in an idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan** Will turn off your computer if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Automatic Maintenance** Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.

The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See **Automatically Clean Threats**.

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

• Click 'OK' to save the profile.

The profile will be available for deployment in future.

		add, remove	and edit sca	n profiles and scheduled sc	ans.
+ Add	2 Edit	🗱 Remove			
	Name		Action	Last Scan	Status
	Full Scan		<u>Scan</u>	12/11/2018 5:44:22 PM	
	Quick Scan		<u>Scan</u>	12/11/2018 2:15:38 PM	
	suspicious		Scan	Never	
	This page	Add Cedit Name Full Scan Quick Scan	This page allows you to add, remove          +       &       *       Remove         Add       Edit       Remove         Image: Search and the	This page allows you to add, remove and edit sca Add Edit Remove Name Action Full Scan Scan Quick Scan	This page allows you to add, remove and edit scan profiles and scheduled so         Add       Edit       Remove         Name       Action       Last Scan         Full Scan       Scan       12/11/2018 5:44:22 PM         Quick Scan       Scan       12/11/2018 2:15:38 PM

COMODO Creating Trust Online\*

### Run Untrusted Programs inside the Container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'
  - Choose the program you want to run
  - Click 'Open'
- CCS 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. The following image shows how a 'virtual' shortcut will appear on your desktop:

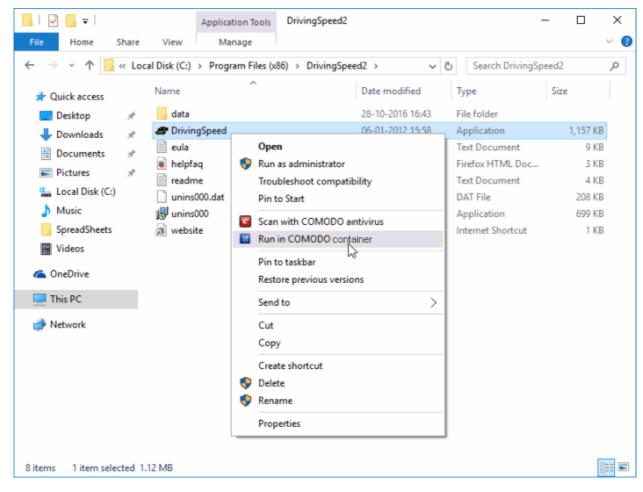


Use any of the following methods to run a program in the container:

- 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:



COMODO Creating Trust Online\*

### The 'Containment Tasks' interface

- 1. Click 'Tasks' > 'Containment Tasks'
- 2. Click the 'Run Virtual' tile

COMODO Client - Secu	rity 11		
K HOME {} SETTINGS			
Secure   All system	s are active and running		
GENERAL TASKS FIREWALL TA	SKS CONTAINMENT TASKS	ADVANCED TASKS	
		Copen Shared System Open the storage	
shortcuts from them	n on the desktop.	and real application	
$rac{1}{2}$ Reset the Contain		lal	? ×
		e the container isolated from the m making permanent changes to	
	Choose and Run Select an application	) on and run it inside the container	
	Create a virtual desktop shor	tcut	

- 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.

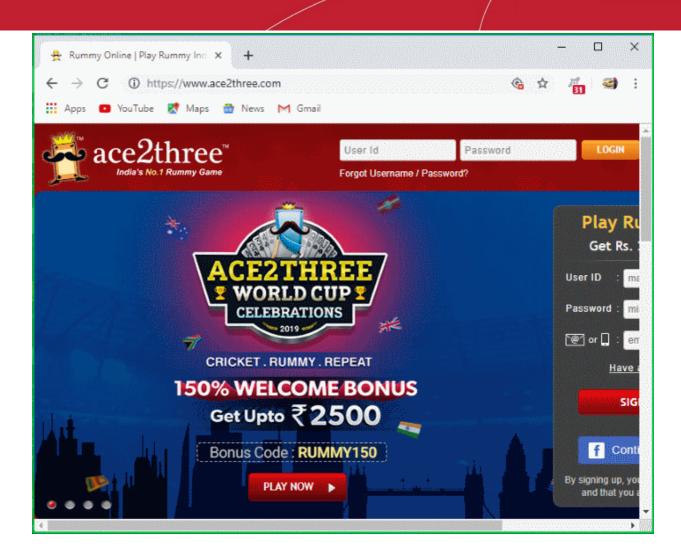
#### Run browsers in container

The CCS widget contains shortcuts to run your browsers in the container:

сомодо								
۵	Secure							
۲ <sup>.</sup> [	. <u>.</u> 0	79						
() 🛞								
e	0	3						
	$\sim$							

- Click a browser icon to start the browser inside the container
- The green border indicates that the browser is in the container:

Creating Trust Online\*



### Run Browsers Inside the Container

- This topic explains how to run your internet browser inside the container.
- Surfing the internet from within the container is the same as normal, with the benefit that any malicious files you inadvertently download cannot damage your real computer.
- You can also create a desktop shortcut to run the browser inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



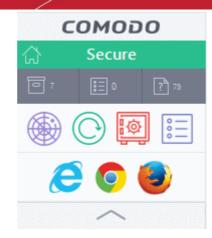
There are two ways to run a browser in the container:

- From the desktop widget
- From the 'Containment Tasks' area

Start a browser from the desktop widget

• The CCS widget contains shortcuts to run your browsers in the container:

COMODO Creating Trust Online\*



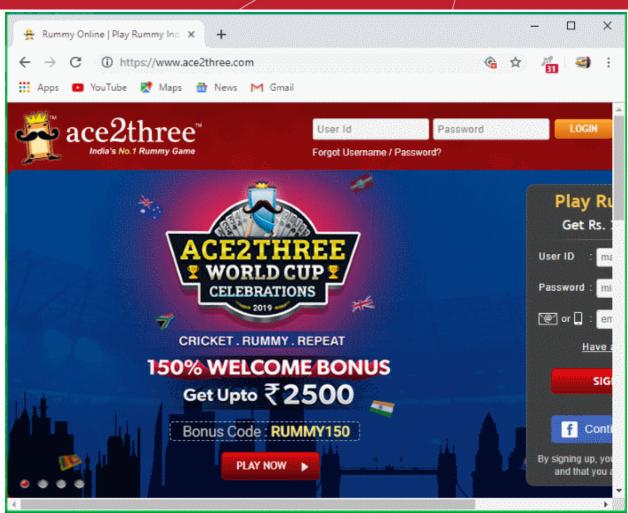
### Start a browser from the 'Containment Tasks' interface

- 1. Click 'Tasks' > 'Containment Tasks'
- 2. Click 'Run Virtual'

COMODO Client - Security 11	
< HOME {ତ୍ରି SETTINGS	
Secure   All systems are active and runni	ng
GENERAL TASKS FIREWALL TASKS CONTAINMENT	TASKS ADVANCED TASKS
Run Virtual Run applications in the container and cr shortcuts for them on the desktop.	reate Copen Shared Spanned Spa
	Run Virtual ? X
	ations inside the container isolated from the rest of the ent them from making permanent changes to the system.
	e and Run an application and run it inside the container.
Create a virtual d	esktop shortcut

- 3. Click 'Choose and Run' then navigate to the install location of the browser. Select the .exe file of the browser.
- 4. Select 'Create a virtual desktop shortcut' to quickly run the application in the container in future.

The browser will run with a green border around it, indicating that it is contained:



### **Restore Incorrectly Quarantined Items**

This page explains how to restore an item from quarantine. You may want to do this if

- You think CCS has incorrectly classed it as malicious (a false positive)
- It was manually moved to quarantine by mistake

### Restore an item from quarantine

- Click 'Tasks' > 'General Tasks'
- Click 'View Quarantine'

COMODO Creating Trust Online\*

<mark>( HOME</mark> {ွှိ	SETTINGS								
🗹 Secure	All syste	ems are active	and running						
GENERAL TASKS	FIREWAL	L TASKS CO	NTAINMENT TAS	KS ADVAN	CED TASKS				Q
Scan		er for viruses ar	nd spyware.	Ø Vie	w Quarantin w and manage nner.		arantin	ed by vi	rus
		o check for proc	rap and virus						
сомод	<b>O</b> Quara	antine			n en	?	_		×
+	0	G	0	~					
+ Add	<b>⊘</b> Delete	Restore	<b>⊘</b> Delete All	Submit					
					C	Q Date/	Time		c ^
Add		Restore Q	Delete All	Submit	e-Samples-mas			8:15 PM	
Add	Delete	Restore Q n0jxmvk	Delete All Location	Submit		i 5/29/2	2019 3:5	8:15 PM	1
Add Item Malwa	Delete are@#jgft8m	Restore Q n0jxmvk oklh7gw	Delete All Location () C:\Suspice	Submit cious\Malwar	e-Samples-mas	5/29/2 5/29/2	2019 3:5 2019 3:5		1
Add Item       Item       Malwa       Malwa       Malwa	Delete are@#jgft8m are@#vigyad	Restore Q n0jxmvk oklh7gw oklh7gw	Delete All Location (@ C:\Suspice (@ C:\Suspice (@ C:\Suspice	Submit cious\Malwar cious\Malwar	e-Samples-mas e-Samples-mas	5/29/2 5/29/2 5/29/2	2019 3:5 2019 3:5 2019 3:5	8:07 PM	1
Add Item Item Malwa Malwa Malwa Malwa	Delete are@#jgft8m are@#vigyad are@#vigyad	Restore Q n0jxmvk oklh7gw oklh7gw euxrw2dy	Delete All Location O C:\Suspice O C:\Suspice O C:\Suspice O C:\Suspice	Submit cious\Malwar cious\Malwar cious\Malwar	e-Samples-mas e-Samples-mas e-Samples-mas	5/29/2 5/29/2 5/29/2 5/29/2	2019 3:5 2019 3:5 2019 3:5 2019 3:5	8:07 PM	
Add Item Item Malwa Malwa Malwa Malwa Malwa	Delete are@#jgft8m are@#vigyad are@#vigyad are@#1ienpo	Restore Q n0jxmvk oklh7gw oklh7gw euxrw2dy 8l4kcvjrs	Delete All Location (i) C:\Suspice (i) C:\Suspice (i) C:\Suspice (i) C:\Suspice (i) C:\Suspice	Submit cious\Malwar cious\Malwar cious\Malwar cious\820075 cious\AntiTes	e-Samples-mas e-Samples-mas e-Samples-mas 5cbedd6f15eec	5/29/2 5/29/2 5/29/2 5/29/2 5/29/2	2019 3:5 2019 3:5 2019 3:5 2019 3:5 2019 3:5	8:07 PM 8:02 PM 7:40 PM	

- Select the item(s) you wish to move out of quarantine and click the 'Restore' button.
- You will then be asked if you wish to create an exclusion for the file so that it will not be flagged by future antivirus scans:

Creating Trust Online\*

COMODO Quarantine		?	-		×
Item Q Location	Q	Date/	/Time		Ť.
Generic.Infector.4		4/10/	2017 6:2	20:16 AN	1
COMODO Client - Security  Would you like to add these files to your antiexcluded files too?	ivirus	×			
YES	NO				
RE	FRES	н		CLOSE	

- 'Yes' The items will be restored to their original locations and added to the antivirus exclusion list. The restored files will be skipped in future AV scans.
- 'No' The items will be restored to their original locations but may still be flagged by future AC scans.
- Click 'Close' to exit.

See Manage Quarantined Items and Submit Quarantined Items to Comodo for Analysis for more information on this topic.

### Submit Quarantined Items to Comodo Valkyrie for Analysis

- You can send quarantined items to Valkyrie for analysis. You may want to do this if you think the item is a false positive it was incorrectly flagged as malicious by CCS.
- Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.
- If the submitted item is found to be a false positive, it will be added to the Comodo white-list.
- If it is found to be malware, it will be added to the virus black-list.
- Submitting files helps Comodo enhance its virus signature database and benefits millions of CCS users. See **Quarantined Items** for more detailed information on the quarantine system.

### Submit quarantined items

- Click 'Tasks' > 'General Tasks'
- Click 'View Quarantine'

COMODO Creating Trust Online\*

C	COMODO Quarantine							?	-		×
	+ Ado		<b>⊘</b> Delete	<b>C</b> Restore	<b>⊘</b> Delete All	✔ Submit					
		Item		Q	Location		Q	Date/	Time		
		User	Item		E:\CCAV	\11-10-18\br	utus.exe	2/20/2	2019 12:	:04:01 PN	N
		Appli	cation.Win3	2.LeakTest.d	🔞 E:\Suspi	cious files\All	_tests\cpil_suite	2/20/2	2019 11:	:46:44 AI	м
L											
							REFRES	Н		CLOSE	

- Select the item(s) you wish to send for analysis
- Click 'Submit' > 'Submit to Valkyrie'

The submission progress will start:

		?	—		×	
57%	C:\ProgramData\Comodo\Cis\Quarantine\data\{6CF97A5B	-E59A	431F-9	917-CDE	1581224	477}
File Name		Stat	te			
C:\ProgramData\Co	omodo\Cis\Quarantine\data\{C929E1C0-BF11-4190-AD9A	$\otimes$	Upload	led		
C:\ProgramData\Co	omodo\Cis\Quarantine\data\{6CF97A5B-E59A-431F-9917	Õ	Upload	ling		
STOP    PAU	ISE		SEND	TO BACI	KGROUN	ND

The results state whether the file was successfully submitted, or whether it has already been submitted by other users and is pending analysis.

COMODO Creating Trust Online\*

### Enable File Sharing Applications like BitTorrent and Emule

This topic explains how to configure Comodo Firewall to work with file sharing applications like Shareaza/Emule and BitTorrent/UTorrent.

To allow file sharing applications:

- Disable 'Do Protocol analysis' (disabled, by default)
- Create a 'Predefined Firewall Ruleset' for Shareaza/Emule
- Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent

### Disable 'Do Protocol analysis'

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Firewall' > 'Firewall Settings'

COMODO Advanced	d Settings ? — 🗆	×
<ul> <li>General Settings</li> <li>Antivirus</li> </ul>	Firewall Settings	^
— Firewall	Enable Firewall (Recommended)     Safe Mode	
Firewall Settings	This option enables firewall which filters inbound and outbound traffic. Alert Settings	
Application Rules Global Rules	✓ Do not show popup alerts Allow Requests ▼	
Rulesets	<ul> <li>Turn traffic animation effects on</li> <li>Create rules for safe applications</li> </ul>	
Network Zones Portsets	Set alert frequency level Low *	
✓ HIPS	Set new on-screen alert timeout to 120 secs Advanced	
<ul> <li>Containment</li> <li>File Rating</li> </ul>	✓ Filter IPv6 traffic	
<ul> <li>Advanced Protection</li> </ul>	<ul> <li>Filter loopback traffic (e.g. 127.x.x.x. ::1)</li> <li>Block fragmented IP traffic</li> </ul>	
	Do protocol analysis	
	Enable anti-ARP spoofing     OK CANCEL	~

- 3. Disable 'Do not Show popup alerts' so CCS will generate alerts when you open Shareaza or Emule.
- 4. Disable 'Do Protocol Analysis'
- 5. Click 'OK' to save your settings.

### Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

- 1. Click 'Settings' > 'Firewall' > 'Rulesets'
- 2. Click 'Add' from the options at the top.

COMODO Creating Trust Online\*

COMODO Advanced	Settings ?	
<ul><li>✓ General Settings</li><li>✓ Antivirus</li></ul>	Rulesets	
- Firewall	The following rulesets are defined on this computer:	
Firewall Settings	+     ★       Add     Edit	
Application Rules Global Rules	Ruleset Name	
Rulesets	Web Browser	
Network Zones	Email Client	
сомодо	· · · · · · · · · · · · · · · · · · ·	
Name: For allowing     Ose a Custom Ru	g Shereaza/Emule	
+ 🖌 Add Edir		
Rules	٩	
	OK CANCEL	

- 3. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing Shareaza/Emule'.
- 4. Now you need to create six rules for the newly created ruleset.
  - Click 'Add' to open the 'Firewall Rule' interface
  - Choose options for each setting as described in 'Rule 1' below
  - After the rule is created, click 'OK' to add the rule
  - Repeat until all 6 rules have been added

COMODO Creating Trust Online\*

сомодо	Firewall Rule ?	×
Action:	Allow   Log as firewall event if this rule is fired	
Protocol:	TCP	
Direction:	In 🔻	
Description	Rule for Incoming TCP Connections	]
SOURCE ADDRESS	DESTINATION ADDRESS SOURCE PORT DESTINATION PORT	
	IOT the choice below) pe: Any Address	
	OK CANC	EL

### Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your TCP port of Shareaza/Emule)

### Rule 2

- Action : Allow
- Protocol : UDP
- Direction : In
- Description : Rule for incoming UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your UDP port of Shareaza/Emule)

### Rule 3

- Action : Allow
- Protocol : TCP or UDP
- Direction : Out

COMODO Creating Trust Online\*

- Description : Rule for outgoing TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : A port range : (start port = 1024 / end port = 65535)

### Rule 4

- Action : Allow
- Protocol : ICMP
- Direction : Out
- Description : Ping the server (edk network)
- Source Address : Any Address
- Destination Address : Any Address
- ICMP Details : Message : ICMP Echo Request

### Rule 5

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : Type : Single Port; (Port : 80)

### Rule 6

- · Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any
- 6. Click 'OK' in the 'Firewall Ruleset' interface.
- 7. Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start Shareaza or Emule. When CCS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'For allowing Shareaza/Emule')
- Select 'Remember my answer'.

### Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

- 1. Click 'Settings' > 'Firewall' > 'Rulesets'
- 2. Click 'Add' from the options at the top.
- 3. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing For allowing BitTorrent/Utorrent'.
- 4. Now you need to create six rules for the newly created ruleset.

COMODO Creating Trust Online\*

### To do so,

- Click 'Add' to open the 'Firewall Rule' interface
- Choose options for each setting as described in 'Rule 1' below
- After the rule is created, click 'OK' to add the rule
- Repeat until all 6 rules have been added

### Rule 1

- Action : Allow
- Protocol : TCP or UDP
- Direction : In
- Description : Rule for incoming TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Single Port (Port: The port of BitTorrent/Utorrent)

### Rule 2

- Action : Allow
- Protocol : TCP
- Direction : Out
- Description : Rule for outgoing TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

### Rule 3

- Action : Allow
- Protocol : UDP
- Direction : Out
- Description : Rule for outgoing UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Single Port: Port: the port of utorrent
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

### Rule 4

- · Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port ; A Single Port (Port = 80)

### Rule 5

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP

COMODO Creating Trust Online\*

- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any
- Click 'OK' in the 'Firewall Ruleset' interface.
- · Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start BitTorrent or Utorrent. When CCS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'BitTorrent/Utorrent')
- Select 'Remember my answer'.

### Block any Downloads of a Specific File Type

This page explains how to configure CCS to prohibit downloads of specific types of file.

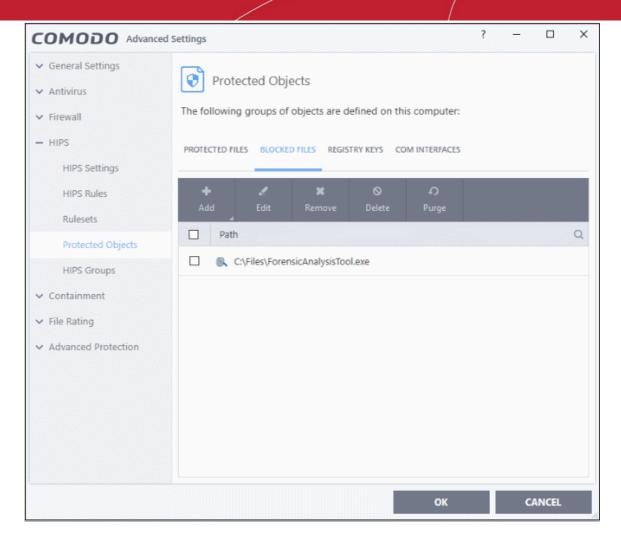
Example scenarios:

- Some malicious websites try to push malware in .exe file format. These files, known as executables, can run commands on your computer. If the .exe is malicious then these commands could install a virus, initiate a buffer overflow attack or could contain code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You may also want to block the download of audio files (.wma, .mp3, .wav, .midi), video files (.wmv, .avi, .mpeg, .swf) or image files (.bmp. .jpg, .png) for various reasons.

You can block downloads of a specific file type by configuring 'Blocked Files' in the HIPS module:

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'HIPS' > 'Protected Objects'
- 3. Click the 'Blocked Files' tab:

COMODO Creating Trust Online\*



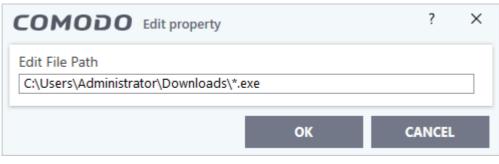
- 4. Click 'Add' > 'Applications'.
- 5. Browse to the default download folder for your browser from the 'Open' dialog:

The default download location for most browsers is C:\Users\[username]\Download.

6. Select any file from the folder and click 'Open'.

The file will be added to the 'Blocked Files' list.

- 7. Select the entry from the Blocked Files interface, and click 'Edit' at the top
- 8. Replace the name of the file with simply '\*.file\_extension', where 'file\_extension' is the file type you wish to block. For example:
  - Change 'C:\Users\[username]\Downloads\file-name.pdf' to C:\Users\[username]\Downloads\\*.exe to block all files with \*.exe extension.
  - Change 'C:\Users\[username]\Downloads\file-name.xls' to C:\Users\[username]\Downloads\\*.jpg to block all files with \*.jpg extension.



COMODO Creating Trust Online\*

- 9. Click 'OK' in the 'Edit Property' dialog.
- 10. Click 'OK' to save your settings.

This will block browser downloads of the specific file type to your 'Downloads' folder. Repeat the process if other browsers on your system have a different download folder.

**Note**: Blocking files in this way will only block downloads of specific file types to specific folders. If you change the folder for browser downloads then the download will be allowed.

### Tip:

- To unblock future downloads, go to 'HIPS' > 'Protected Objects' > 'Blocked Files', select the file path, and choose 'Remove'.
- To unblock individual files, go to 'General Tasks' > 'Unblock Applications' and choose 'Unblock'.

### Disable Auto-Containment on a Per-application Basis

- The default auto-containment rules will run all unknown executables in the container and queue them for submission to Comodo for behavior analysis.
- · Comodo recommends most users leave this setting intact to ensure the highest protection levels.
- Should you wish, you can create an 'Ignore' rule to exclude certain files or file types from containment.
- This is could be useful for developers testing new applications which, by their nature, are unknown to the Comodo safe list.

### To create an auto-containment exception

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Containment' > 'Auto-Containment' on the left
- 3. Ensure that 'Enable Auto-Containment' is selected
- 4. Click 'Add' to create a new rule:

COMODO Creating Trust Online\*

COMODO Client - Security 11			-	×
品 tasks 《② settings				
Scan		View Oua	2 rantine	
COMODO Advanced Settings		? -	- 0	×
<ul> <li>✓ General Settings</li> <li>✓ Antivirus</li> <li>✓ Auto-Containment</li> </ul>				
<ul> <li>Firewall</li> <li>HIPS</li> <li>Enable Auto-Containment</li> <li>This option enables automatic containment of policy defined below.</li> </ul>	executable files	and scripts a	eccording to	the
Containment Settings     Auto-Containment     Auto-Containment     Auto-Containment     Auto-Containment     Auto-Containment     Auto-Containment		Cr Reset to Default	Taskla Rula	•
Auto-Containment     □     Action     Q     Target       ✓ File Rating     □     Run Virtually     □     C:\Program	Q Reputati	ion Q I	Enable Rule	
COMODO Manage Contained Program	ŝ	? 🗆	×	
Action Run Virtually			-	
The selected containment action will be applied if file properties ma	itch the follow	wing criter	ia:	
		Edit		
No criteria selected				
0	к	CANCE	L	

5. Select 'Ignore' from the 'Action' drop-down:

COMODO Creating Trust Online\*

сом	ODO Manage Contained Program	?		×
	Ignore Run Restricted Run Virtually Block			•
No crite	eria selected		Edit	

- 6. Click the 'Edit' button under the 'Criteria' tab
- 7. Click 'Browse' to specify the type of item you wish to exclude:

	?	
Please select the criteria to be applied.		
File location:		
D:\My safe program\cuckoo-setup.exe		Brows
		Files
File created by applications:	Any	Running Processe
File started by processes:	Any	File Groups
		Folder File Hash
		Process Hash
	E	
File created by users:	Any	Add 🗸
File created by users: File origin:	Any Any	Add 🗸
File origin:	Any	
-	Any	Add 🔻 🗸
File origin: File rating:	Any Any Any Any	Add 🔻 🗸 Select 👻 🏹

COMODO Creating Trust Online\*

- 8. You can select individual files, folders, processes, file groups or hashes. Click 'Open' when you have made your selection.
- 9. Click 'Select' at the end of the 'File Rating' row and select 'Unrecognized' from the drop-down:

File Created by User(s):	Any Add 🗸
File Origin(s):	Any Add 🗸 🗸
File Rating:	Unrecognized Select
	Trusted
Unrecognized	Unrecognized
	Malicious

10. Next, click the 'Options' tab.

COMODO Manage Contained Program	?		×
Action Ignore			•
The selected containment action will be applied if file properties match the	following	g criteria	:
CRITERIA OPTIONS			
Log when this action is performed			
Don't apply the selected action to child processes			
		CANCEL	
ОК		CANCEL	

- Log when this action is performed Optional. Whenever this rule is applied for a file, it will be added to CCS containment logs.
- **Don't apply the selected action to child processes** Child processes are processes spawned by a parent application. By default, CCS treats all child processes individually.
  - Disabled The ignore rule will apply to the target application and all child processes that it spawns. All

COMODO Creating Trust Online\*

will be allowed to run outside the container.

- Enabled The ignore rule will apply only to the target application. All child processes will be inspected and possibly contained as per their file rating.
- 11. Select options as required and click 'OK'.

nced S	ettings						?	-		×
	Enable	to-Containn Auto-Contain ption enables a defined below.	ment utomatic cor	tainment of e	xecut	able files and	d script	s accor	ding to t	the
	+ Add	ي Edit	XX Remove	<b>↑</b> Move Up	Mo	Uve Down	<b>(၂)</b> Reset to Default	) :		
		ction	<b>Q</b> Ta	rget	Q	Reputation	Q	Enab	le Rule	
	☑ →	Ignore	6	D:\My safe p	ro	Unrecogniz	ed		2	
		Block		All Applicatio	ons	Malicious			0	
		Block		Suspicious L	DC	Any			2	
		Block		Containment	F	Any			2	
	•	Ignore		COMODO CI	ie	Trusted			<b>)</b>	
		Ignore		Metro Apps		Any			<b>)</b>	11
										Ŧ
						ок	U	C	ANCEL	

The new rule will be listed in the 'Auto-Containment' screen. Make sure to keep this rule above all other rules for unrecognized files.

#### Alternatively...

- 1. Assign a 'Trusted' rating to the file in the File List interface
- Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the Vendors List as trusted.
- 3. Disable auto-containment by de-selecting the 'Enable Auto-Containment' check box in the 'Autocontainment' settings panel. *Not recommended*

See Unknown Files: The Scanning Processes, for more details on auto-containment process.

COMODO Creating Trust Online\*

## Switch Off Automatic Antivirus Updates

- By default, Comodo Client Security automatically downloads software and antivirus database updates.
- However, some users like to control when updates are downloaded. For example, network admins may not want automatic updates because they take up too much bandwidth during the day.

CCS provides full control over virus and software updates. Click the appropriate link below to find out more:

- Switch off automatic updates entirely
- Switch off automatic virus updates selectively
- Switch off automatic virus signature database updates prior to Antivirus Scans

### Switch off automatic updates entirely

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'General Settings' > 'Updates'
- 3. Disable 'Check for database updates every'

COMODO Advanced	I Settings ? - $\Box$ X
- General Settings	
User Interface	Updates
Updates	Check for database updates every
Logging	Options
Configuration	Do not check for updates if I am using <u>these connections</u>
✓ Antivirus	Do not check for updates if running on battery
✓ Firewall	Check for updates during Windows Automatic Maintenance
✓ HIPS	Send requests to COMODO online services only if internet connection is present
✓ Containment	Proxy and Host Settings
✓ File Rating	
<ul> <li>Advanced Protection</li> </ul>	
	OK CANCEL

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

### Switch off automatic updates selectively

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'General Settings' > 'Updates'

COMODO Creating Trust Online\*

сомодо	Advanced Settings ? —	×
<ul> <li>General Settings</li> <li>User Interface</li> </ul>	O Updates	
Updates	Check for database updates every	
Logging Configuration	Options Do not check for updates if I am using these connections	
<ul> <li>Antivirus</li> <li>Firewall</li> </ul>	COMODO Connections ?	
<ul><li>HIPS</li><li>Containment</li></ul>	Connection Names	
<ul> <li>File Rating</li> <li>Advanced Pro</li> </ul>		
	OK CANCEL	
	OK CANCEL	

- Suppress automatic updates when using certain networks:
  - Select the 'Do not check updates if am using these connections' check-box
  - Then click 'these connections' to view a list of connections you use.
  - Select the connection over which you do not want CCS to check for updates and click 'OK.'
- Do not check for updates if running on battery Will only download updates when the computer is plugged in to the mains.
- 5. Click 'OK' for your settings to take effect

### Switch off automatic virus signature database updates prior to AV Scans

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Antivirus' > 'Scans'
- 3. Select a target scan profile
- 4. Click 'Edit' from the options at the top
- 5. Click 'Options', scroll down, and clear the 'Update virus database before running' checkbox.

COMODO Creating Trust Online\*

COMODO Advanced	Settings		?	- 0	×
✓ General Settings	Scans				
- Antivirus	Scalls				
Waltime Scan	This page allows you to add, re	move and edit scar	n profiles and sched	uled scans.	
Scans V Firewall	+ Add Edit Rem				
✓ HIPS	Name	Action	Last Scan	Status	
✓ Containment	🗌 Full Scan	<u>Scan</u>	Never		
✓ File Rating	Quick Scan	<u>Scan</u>	Never		
<ul> <li>Advanced Protection</li> </ul>	Downloaded Files	Scan	Never		
	¥				
COMODO Scan				?	×
Scan Name: Downloade	ed Files				
	size is larger than specified, it i	s not scanned			^
Ryn this scan with	Background	uter resources are	used among other	r tasks	
Jpdate virus databas					
This option makes sure	the database is updated before	e running the scar	I		
Detect potentially un Potentially unwanted a consented to download	pplications are programs that a	re unwanted desp	ite the possibility t	hat users	
Apply this action to s	uspicious autorun processes	Terminate	and Disable 🔹 🔻		
The selected action wil scheduled tasks are de	I be automatically applied if unr tected.	ecognized Windo	ws services, autost	art entries or	
Limit scan time of a sing	gle file to 9 🚔 min(s)				
When the set time limi	t is reached, the file will be skip	ped and antivirus	will proceed scann	ing other files.	~
			ОК	CANCEL	

- 6. Click 'OK' on the 'Scan' interface.
- 7. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

COMODO Creating Trust Online\*

## Suppress CCS Alerts Temporarily

- CCS shows you an alert if it finds a security threat, and also shows alerts for general system messages.
- 'Silent mode' lets you temporarily disable these alerts so they don't interrupt games or a presentation etc.
- During this time, operations that can interfere with user experience are either suppressed or postponed. This includes alerts and scheduled scans.
- All protection components are still 100% active in silent mode.

### Temporarily stop pop-up alerts

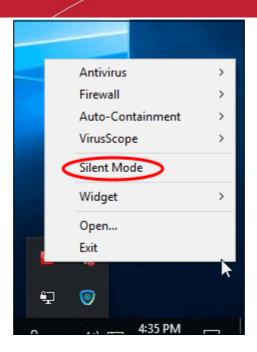
• Click 'Silent Mode' button on the CCS home screen:

COMODO Client - Security 11		-	×
吕 TASKS 《ⓒ SETTINGS			
Secure	Scan	View Quarantine	- >
All systems are active and running	Update	Open Task Manager	/
MANAGE PROTECTION		•	?

OR

· Right-click on the CCS tray icon and select 'Silent Mode'

COMODO Creating Trust Online\*



The alerts are now suppressed.

• To resume alerts and scheduled scans, just deactivate 'Silent Mode' from the home screen or tray icon.

### **Control External Device Accessibility**

- Click 'Settings' > 'Advanced Protection' > 'Device Control'
- CCS helps you block access to selected external devices attempting to connect to your computer.
- The 'Device Control' panel lets you specify types of external devices that are to be blocked and define
  exclusions to it

### Block an external device

- 1. Click 'Settings' on the CCS home screen
- 2. Click 'Advanced Protection' > 'Device Control'

COMODO Creating Trust Online\*

COMODO Client	- Security 11	- >
🔠 tasks 🔅 settin	IGS	
COMODO Advand	ed Settings ?	- 0 ×
<ul> <li>General Settings</li> <li>Antivirus</li> <li>Firewall</li> <li>HIPS</li> <li>Containment</li> <li>File Rating</li> <li>Advanced Protection</li> <li>VirusScope</li> <li>Scan Exclusions</li> <li>Device Control</li> </ul>	<ul> <li>Device Control</li> <li>Enable Device Control</li> <li>This option blocks devices of a client computer from accessing, such Bluetooth devices, printers, serial and parallel ports.</li> <li>Log detected devices</li> <li>Show notifications when devices are being disabled or enabled</li> <li>BLOCKED DEVICES EXCLUSIONS</li> <li>Use this table to manage the list of devices to which you want to block.</li> </ul>	
Script Analysis	Device Q Identification	
Miscellaneous	USB storage devices Class: {8A63AD2	7-0CD7-4F43-B8E1-07
	ок	CANCEL

- Enable Device Control Activate the device control functionality to selectively prohibit access to external devices. You should specify devices to be banned in the 'Blocked Devices' pane. (Default = Enabled)
- Blocked Devices List of external device classes which are not allowed to connect to the endpoint. Example classes include 'USB Storage Devices', 'CD/DVD Drives', 'BlueTooth Devices' and 'Firewire Devices'.
- **Exclusions** Add exceptions to a blocked class. For example, if you wish block the class 'USB Devices' but wish to allow access for your company's authentication tokens, then you should add those USB tokens as exceptions.

### Click here for more details on controlling device access

COMODO Creating Trust Online\*

# Appendix 2 - Comodo Secure DNS Service

### Introduction

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary directory services platform. Most of the networks use recursive DNS services that are provided by their ISP or that reside on their own set of small DNS servers but it becomes essential to have a secure and broadly distributed DNS service to have a faster and safe DNS resolution.

**Background Note**: Every device on the internet is uniquely identified by a 32-bit number (IPv4 address) or a 128bit number (IPv6 address). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The 'Domain Name System' (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with the internet. It requires no hardware or software and provides reliable, faster, smarter and safer internet experience.

- Reliable Comodo Secure DNS Directory Services Platform currently spans across five continents around the world. This allows us to offer you the most reliable fully redundant DNS service anywhere. Each node has multiple servers, and is connected by several Tier 1 carriers to the internet.
- Faster Our strategically placed nodes are located at the most optimal intersections of the internet. Unlike
  most DNS providers, Comodo Secure DNS directory services platform uses Anycast routing technology which means that no matter where you are located in the world, your DNS requests are answered by the
  closest available Comodo Secure DNS set of servers. Combine this with our huge cache and we can get
  the answers you seek faster and more reliably than anyone else. Furthermore, our "name cache
  invalidation" solution signals the Comodo Secure DNS recursive servers anytime one of our authoritative
  customers or partners updates a DNS record, fundamentally eliminating the concept of a TTL.
- Smarter Comodo's highly structured search and guide pages get you where you want to be, when you inadvertently attempt to go to a site that doesn't exist.
- Safer As a leading provider of computer security solutions, Comodo is keenly aware of the dangers that
  plague the internet today. Secure DNS helps users keep safe online with its malware domain filtering
  feature. Secure DNS references a real-time block list (RBL) of harmful websites (i.e. phishing sites,
  malware sites, spyware sites, excessive advertising sites, etc.) and will warn you whenever you attempt to
  access a site containing potentially threatening content. Directing your requests through highly secure
  servers can also reduce your exposure to the DNS Cache Poisoning attacks that may affect everybody else
  using your ISP.

To start Comodo Secure DNS service the DNS settings of your computer has to be modified to point to our server's IP addresses. Comodo Client Security automatically modifies the DNS settings of your system during its installation to get the services. You can also modify the DNS settings of your system manually, if you haven't selected the option during installation. You can also revert to the previous settings if you want, at anytime.

Click the following links to get the instructions for manually modifying the DNS settings on your router or on your computer.

- Router
- Windows

COMODO Creating Trust Online\*

### Router - Enable or Disable Comodo Secure DNS

You can manually enable or disable Comodo Secure DNS service in your Router by modifying the DNS settings accessible through DNS Server settings of your router. Comodo recommends making the change on your router so that with one change, all the computers on your network can benefit from Comodo Secure DNS.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Primary DNS : 8.26.56.26

Secondary DNS : 8.20.247.20

### Modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

http://192.168.0.1 http://192.168.1.1 http://192.168.10.1

If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).

DNS AND ADVANCED SETTINGS				
Use these DNS Servers : Primary DNS Server : Secondary DNS Server : Advanced >>				

 Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

When you are done, the above example would look like this.

DNS AND ADVANCED SETTINGS				
Use these DNS Servers :	$\checkmark$			
Primary DNS Server :	8.26.56.26			
Secondary DNS Server :	8.20.247.20			
Advanced >>				

### **Disable Comodo DNS**

You can disable Comodo Secure DNS by:

 Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

COMODO

### OR

• Entering different preferred and alternate DNS server IP addresses.

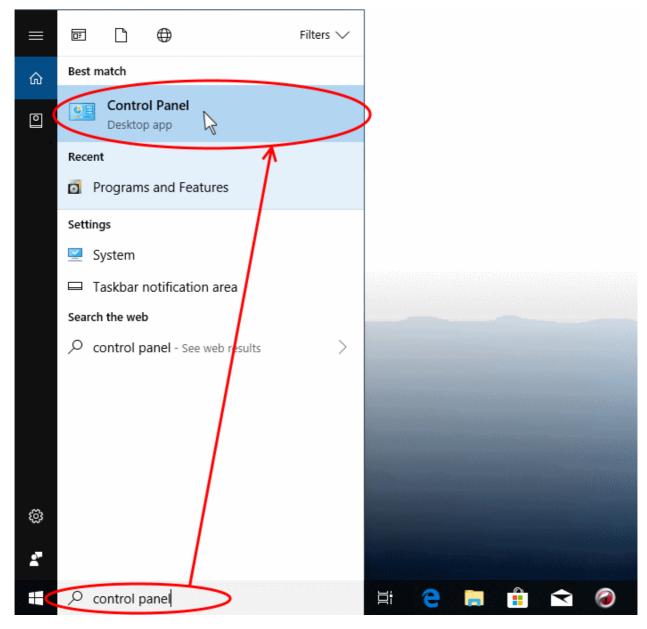
### Windows - Enable Comodo Secure DNS

You can manually enable Comodo Secure DNS by changing your DNS server addresses to:

- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

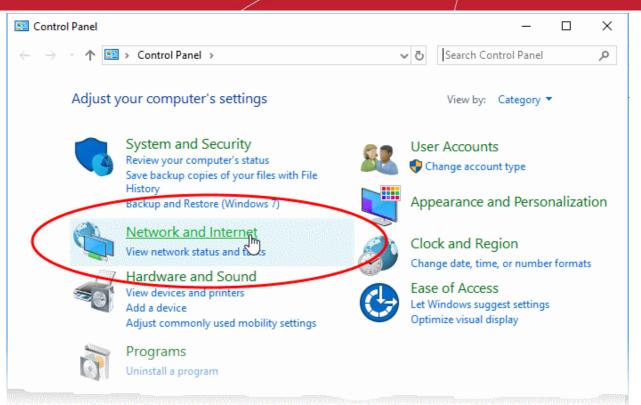
Enable Comodo Secure DNS

- 1. Click the Windows 'Start' menu
- 2. Type 'control panel' into the search box then click the program name:

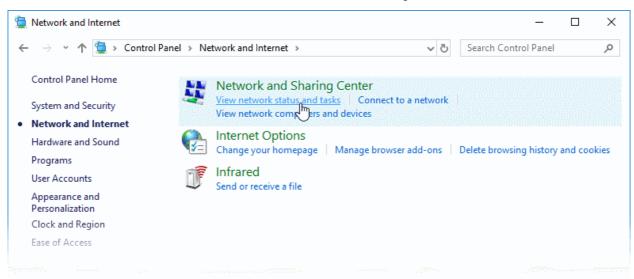


3. Select 'Network and Internet' from the control panel menu:

COMODO



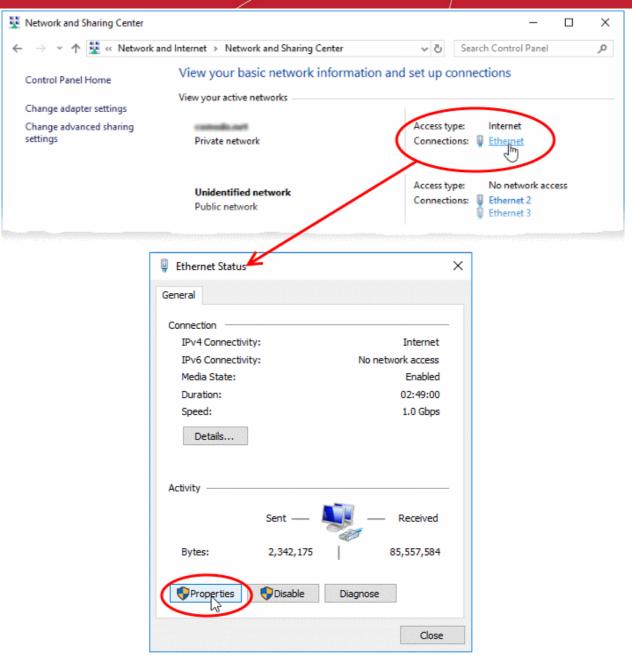
4. Select 'View network status and tasks' under Network and Sharing Center' as shown below:



The list of networks to which you are currently connected is shown.

5. Click the network type link in the network through which you are connected to internet:

COMODO Creating Trust Online\*



This opens the 'Status' dialog for the selected connection.

- 6. Click 'Properties' in the status dialog
  - At this point, Windows might ask for your permission to continue or request that you enter an administrator password.
  - Once you have granted permission/entered an admin password, the 'Connection Properties' dialog appears:

COMODO Creating Trust Online\*

¥ Ethe Network		roperties haring						>
Conne	ct using	<b>j</b> :						
7	Intel(R)	PRO/10	00 MT [	)esktop /	Adapter			
This co	onnecti	on uses t	he follow	ving items	8:	Confi	gure	
	File a COM QoS Inten Micro	t for Micr and Printe IODO Inte Packet S net Proto psoft Net psoft LLD	er Sharin ernet Se Schedule col Vers work Ad	g for Mic curity Fire on 4 (TC apter Mu	ewall Driv P/IPv4) Itiplexor I	ver	>	<b>*</b>
Desc Trar wide	e area r	on Contro	l Protocol t	hat provi	des com	Prope ol. The de municatio	∂ efault	
					ОК		Can	cel

- 7. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button as shown above.
- 8. Enable 'Use the following DNS server addresses'.
- 9. Enter the addresses listed below:

Preferred DNS : 8.26.56.26 Alternate DNS : 8.20.247.20

COMODO Creating Trust Online\*

Internet Protocol Version 4 (TCP/IPv4) Properties							×	
General	Alternate Configuration							
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.								
⊙ Ob	tain an IP address automatical	у						
US	e the following IP address:							
IP ad	dress:				e	]		
Subn	et mask:				e	]		
Defa	ult gateway:					]		
- (i) Us Prefe	otain DNS server address autom e the following DNS server add erred DNS server: nate DNS server:	resses:	. 26	. 56		]		
Vi	alidate settings upon exit				Advar	nced		
			(	ОК		Cancel		

- 10. Click 'OK' to save your settings
- 11. Click 'OK' in the connection properties dialog to activate your settings
- Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the internet.

#### **Disable Comodo DNS**

You can revert to the DNS servers provided by your ISP at anytime by instructing Windows to automatically obtain the address of a DNS servers.

- Follow steps 1 to 7 of the 'Enable Comodo DNS' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.

COMODO Creating Trust Online\*

nternet P	Protocol Version 4 (TCP/IP)	/4) Properties	>
General	Alternate Configuration		
this cap		tomatically if your network supports to ask your network administrator	ł
() Ob	otain an IP address automati	cally	
	e the following IP address: -		
IP address:		• • •	
Subnet mask:		• • •	
Defa	ult gateway:	· · ·	
		11 - H	
	otain DNS server address aut		
<u> </u>	erred DNS server:	* * *	
Alter	nate DNS server:	к і і	
V	alidate settings upon exit	Advanced	
		OK Cance	el

**Note**: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

COMODO Creating Trust Online\*

# 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