COMODO
Creating Trust Online®

Comodo
Antivirus for Linux

Software Version 1.0

User Guide

Guide Version 1.0.111114

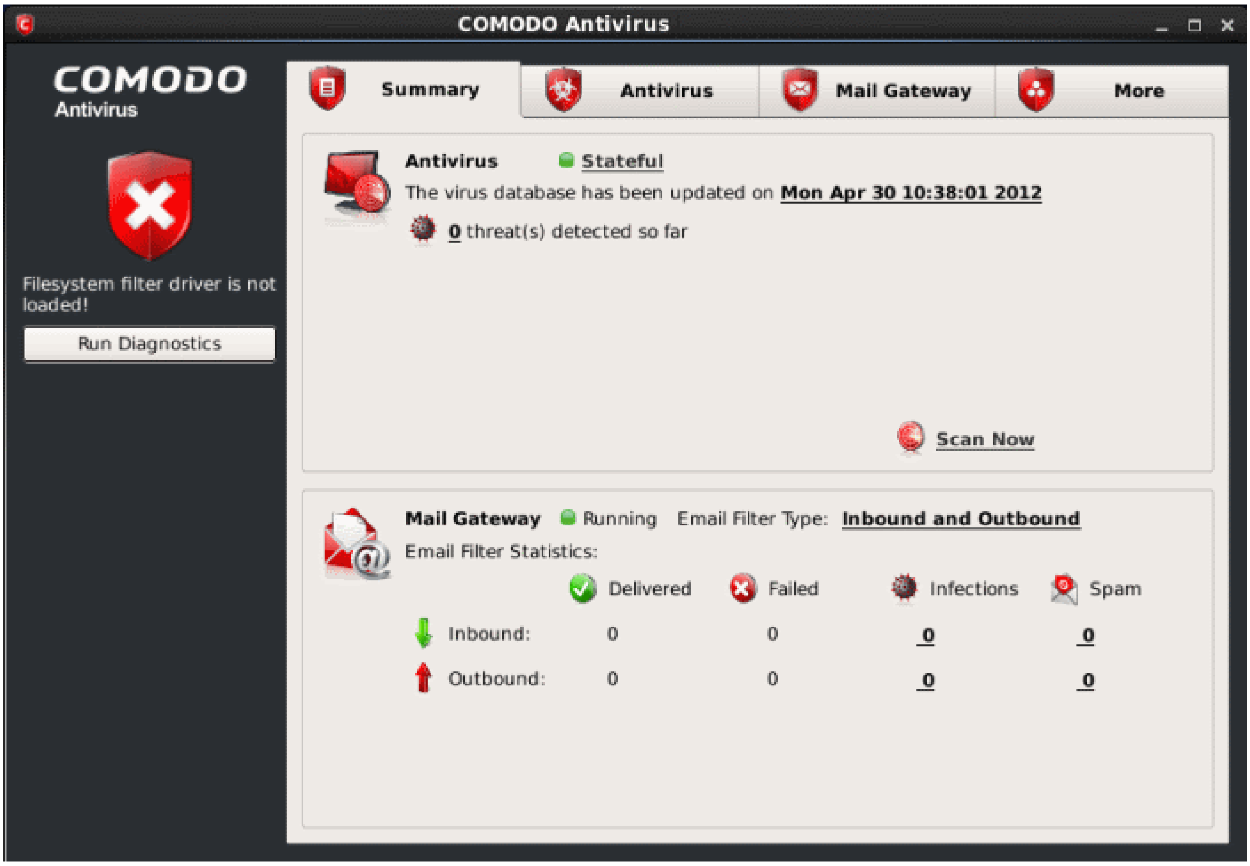
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Antivirus for Linux

Comodo Antivirus for Linux (CAVL) offers complete protection against viruses, worms and Trojan horses for Linux based computers. The software is easy to configure and use and features real-time, on-access and on-demand virus scanning, full event logging, schedules scans and more. The application has an email filtering system that blocks spam, email-borne viruses and other unwanted mail from reaching user's in-boxes. Users can start virus scans immediately by clicking the 'Scan Now' link on the summary screen.

- Detects, blocks and eliminates viruses from desktops and networks
- Constantly protects with Real-Time and On-Access scanning
- Built in scheduler allows you to run scans at a time that suits you
- Isolates suspicious files in quarantine preventing infection
- Daily, automatic updates of virus definitions
- Blocks spam mails
- Detects and blocks emails that contains viruses



Filesystem filter driver is not loaded!

Antivirus Stateful
The virus database has been updated on Mon Apr 30 10:38:01 2012
0 threat(s) detected so far

Mail Gateway Running Email Filter Type: Inbound and Outbound
Email Filter Statistics:

	Delivered	Failed	Infections	Spam
Inbound:	0	0	0	0
Outbound:	0	0	0	0

Guide Structure

This introduction is intended to provide an overview of Comodo Antivirus for Linux. Please use the links below to jump to the section that you need help with.

1.1. Special Features

Comprehensive Antivirus Protection

- Detects and eliminates viruses from desktops, laptops and network workstations;
- Performs Cloud based Antivirus Scanning;
- Employs heuristic techniques to identify previously unknown viruses and Trojans;
- Scans even Configuration files and Filesystem for possible spyware infection and cleans them;
- Rootkit scanner detects and identifies hidden malicious files stored by rootkits;
- Constantly protects with real-time, On-Access scanning;
- Highly configurable On-Demand scanner allows you to run instant checks on any file, folder or drive;
- Daily, automatic updates of virus definitions;
- 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.

Efficient Mail Gateway

- Detects and blocks incoming and outgoing email messages containing viruses
- Scans and removes all types of viruses, and other malicious programs in all incoming and outgoing email messages including attachments
- Blocks all spam emails
- Configurable mail scanner settings

1.2. System Requirements

To ensure optimal performance of Comodo Antivirus for Linux, please ensure that your PC complies with the minimum system requirements as stated below:

Supported Operating Systems (both x86 and x86_64):

- Red Hat Enterprise Linux Server 5.8, 6.2
- Fedora 16
- SUSE Linux Enterprise Server 11
- OpenSUSE Linux 12.1
- Debian 6.0.4
- Ubuntu 12.04
- CentOS 5.8, 6.2

Supported mail systems:

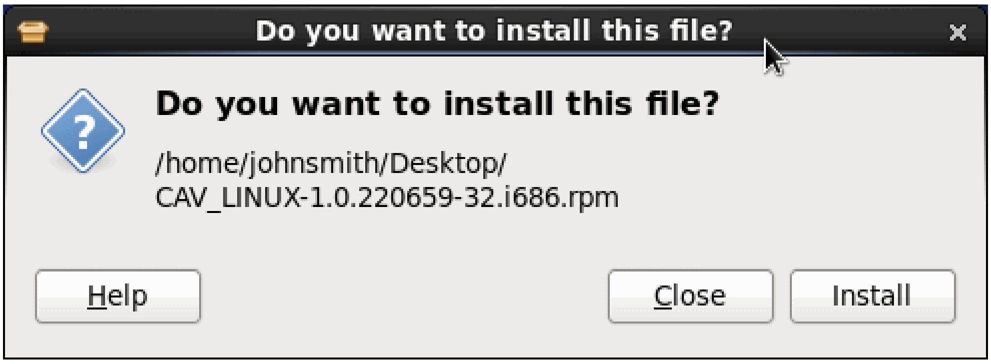
- Sendmail 8.14.3
- qmail 1.03,
- Postfix 2.5.x or higher,
- Exim 4.x.

1.3. Installation

To install, download the Comodo Antivirus setup files to your local hard drive. (setup.exe can be downloaded from
---)

After downloading the CAVL setup files to your local hard drive, double-click on CAV_LINUX-1.0.I686.rpm file to start the installation wizard.

The installation wizard starts automatically and the confirmation dialog will be displayed.



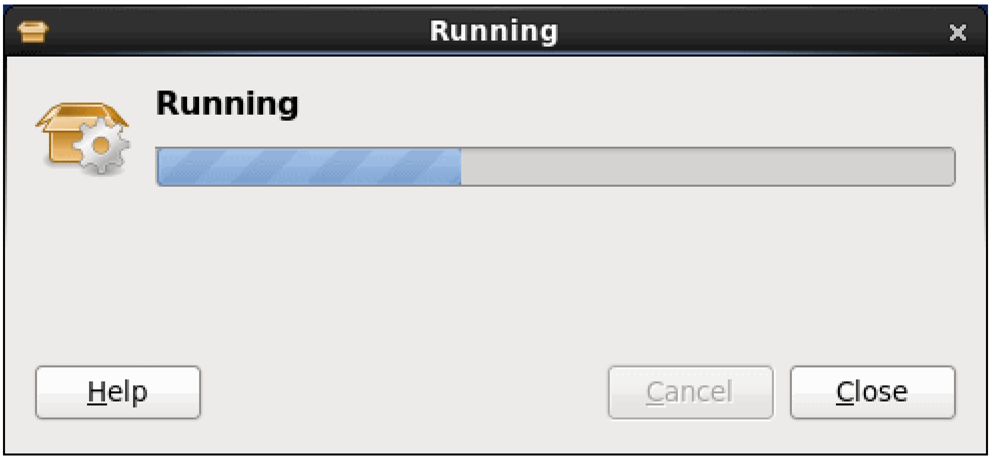
Do you want to install this file?

Do you want to install this file?

/home/johnsmith/Desktop/
CAV_LINUX-1.0.220659-32.i686.rpm

- Click 'Install' to start the installation process.

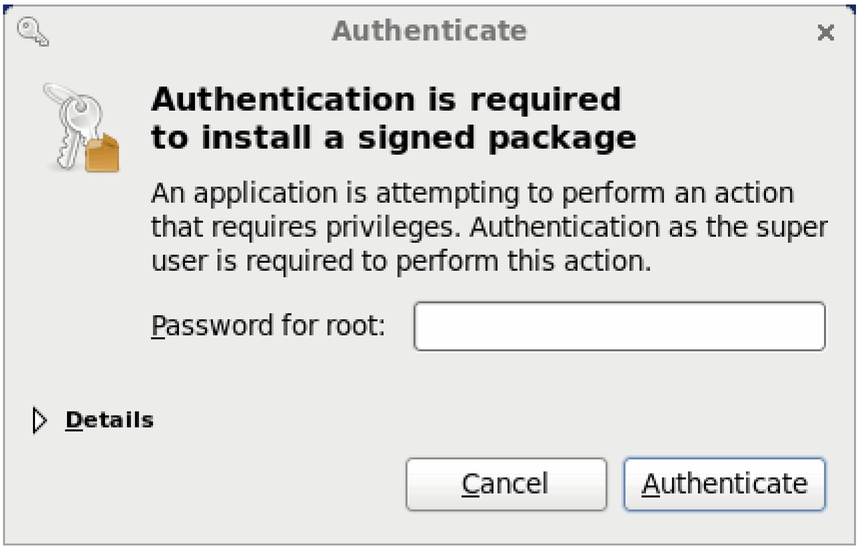
The installation process will be displayed.



Running

Running

You will be asked to authenticate the installation.



Authenticate

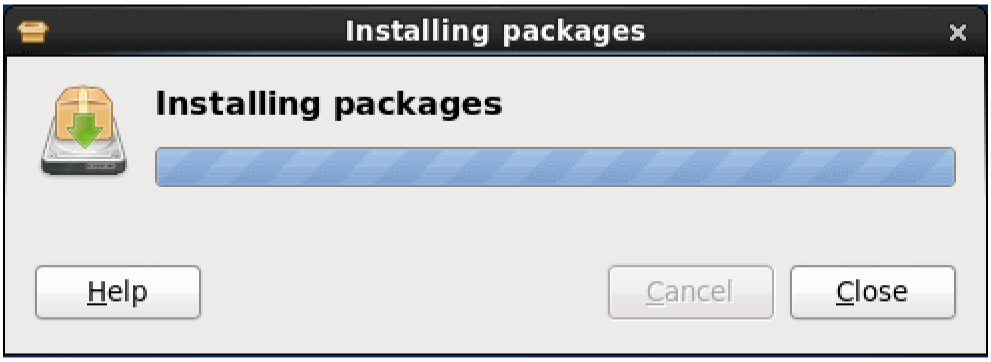
Authentication is required to install a signed package

An application is attempting to perform an action that requires privileges. Authentication as the super user is required to perform this action.

Password for root:

- Enter the administrator password and click 'Authenticate'.

After verifying the credentials, the packages will be installed.



Installing packages

Installing packages

On successful completion, shortcut icons of the application will be placed in the desktop and the Notifications area. To open the application, refer the section **Starting Comodo Antivirus**.

1.4. Starting Comodo Antivirus

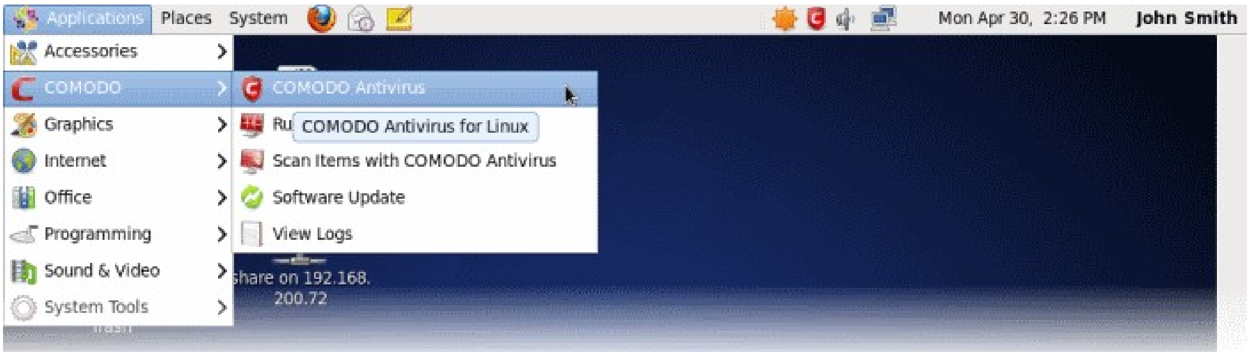
After installation, CAVL will be automatically loaded whenever you start your computer. Real-time protection and on-access scanning is automatically enabled so you are protected immediately after the restart. To configure the application and view settings, you need to access the management interface.

Management interface can be accessed by three ways:

- **Applications Menu**
- **Desktop Menu**
- **Notifications Icon**

Applications Menu

- In the Panel, click **Comodo** > **Comodo Antivirus** to start the application.



The Applications menu also provides shortcuts to:

- **Run Diagnostics**
- **Instantly Scan Objects**
- **Software Update**
- **View Logs**

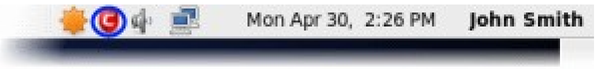
Click on the above links for more detailed explanation.

Desktop Menu

- Just double click the shield icon in the desktop to start Comodo Antivirus.

Notifications Icon

- Just double click the shield icon in the Notifications area to start Comodo Antivirus.



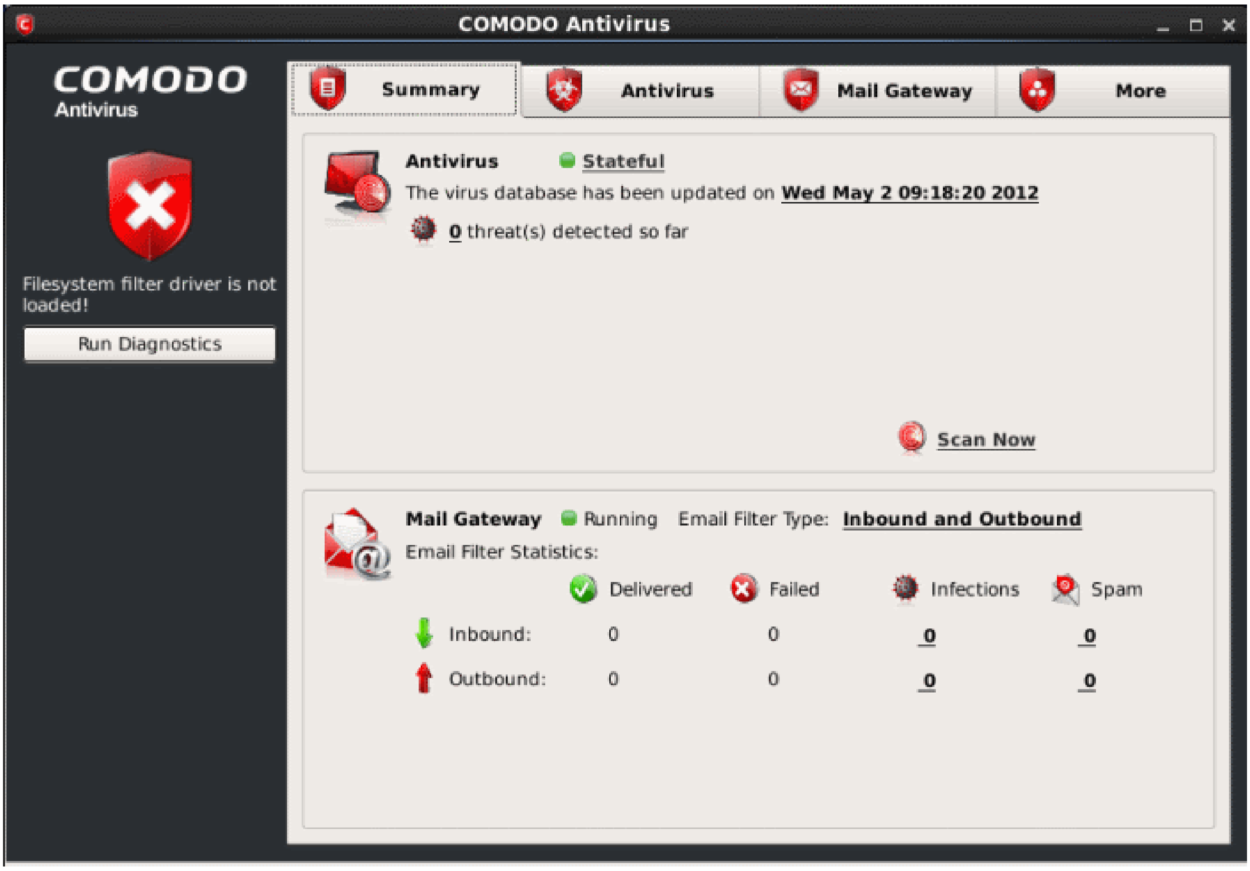
By right-clicking on the Notification area icon, you can access short cuts to selected settings such as Antivirus Security Level, Configuration, open and close the application.

Antivirus Security Level - **Click here** for more details on Antivirus Security Level setting.

Configuration - **Click here** for more details on Configuration settings.

1.5. Comodo Antivirus - The Summary Screen

The 'Summary' screen is shown by default when you open the application. It provides an at-a-glance summary of protection and update status as well as allowing you to quickly run a virus scan with a single click. You can access this area at any time by selecting the 'Summary' tab as shown in **General Navigation**.



Filesystem filter driver is not loaded!

Antivirus ● Stateful

The virus database has been updated on Wed May 2 09:18:20 2012

0 threat(s) detected so far

Mail Gateway ● Running Email Filter Type: Inbound and Outbound

Email Filter Statistics:

	Delivered	Failed	Infections	Spam
Inbound:	0	0	0	0
Outbound:	0	0	0	0

Summary screen shows the following:

1. **System Status**

   On the left-hand side of the main interface the status of the system will be displayed and recommendations on actions you need to perform.

2. **Antivirus**

   The Antivirus summary box contains:

   i. **The Status of Realtime Virus Scanning**

      The status of the virus scanning setting is displayed as a link (Stateful in this example). On clicking this link, the Virus Scanner Settings panel is opened allowing you to quickly set the level of Real Time Scanning, by moving the status slider. For more details on Virus Scanner Settings, refer **Scanner Settings**.

   ii. **When the Virus Database was Last Updated**

      The day and time at which the virus database was last updated is displayed as a link. On clicking the link, the update of the virus database is started and the current date and time are displayed on completion of the process.

   iii. **Number of Detected Threats**

      The number of threats detected so far from the start of the current session of Comodo Antivirus is displayed here as a link. On clicking the link, Antivirus Events panel is opened. For more details on viewing Antivirus events, refer **Antivirus Events**.

   iv. **Scan Now**

      The 'Scan Now' link in this box allows you to **Run a Scan**, when clicked.

3. **Mail Gateway**

   The Mail Gateway summary box contains:

   i. **Email Filter Type**

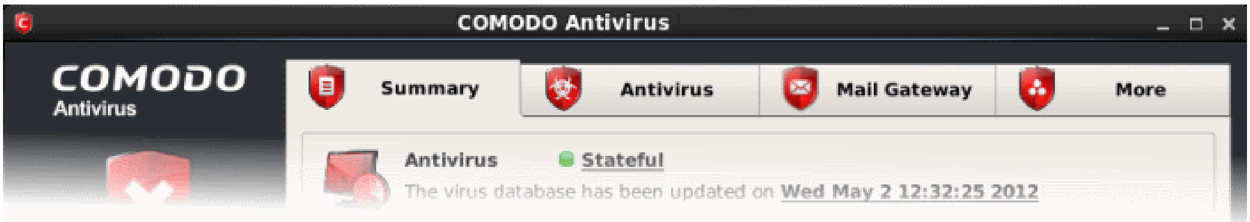
      The status of the mail filter type is displayed here as a link. On clicking on the link, the SMTP Configuration settings panel is opened allowing you to change the mail filtering type. The mail filter statistics displayed below this depends on the filter type chosen. For more details on mail filtering types, refer **SMTP Configuration**.

ii. **Email Filter Statistics**

A summary of email filter statistics is displayed here. The summary screen depends on the mail filter type chosen in SMTP Configuration settings. The number of inbound or/and outbound mails, and their statuses whether delivered, failed, infected or the mail is spam are displayed here. Clicking on any of the number links under Infections or Spam columns will open the Mail Events screen. Refer to section **View Mail Events** for more details.

1.6. Comodo Antivirus - Navigation

The Comodo Antivirus interface is divided into four main functional areas - 'Summary', 'Antivirus', 'Mail Gateway' and 'More'. You can access any of these areas by clicking the tabs along the top of the interface.

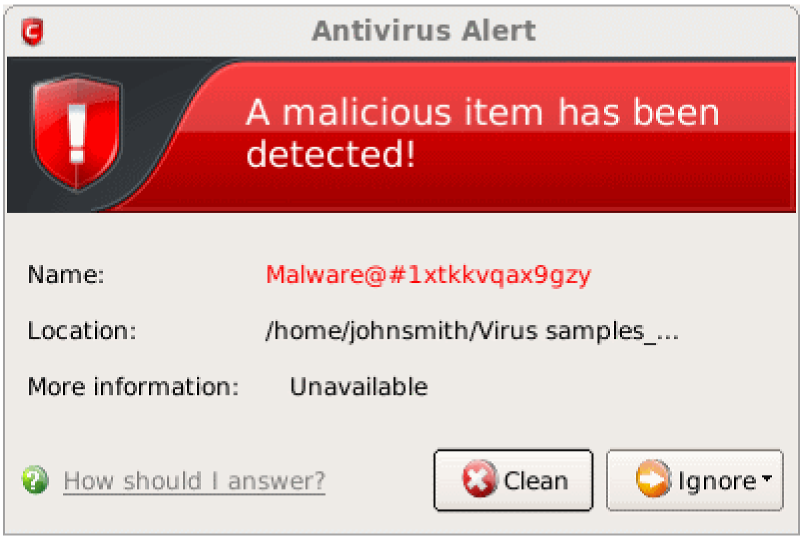


Antivirus ● Stateful
The virus database has been updated on Wed May 2 12:32:25 2012

- **Summary** - Contains at-a-glance details of important settings, activity and other information.
- **Antivirus** - Opens the **Antivirus Tasks** configuration section. This area allows you to run scans, configure settings, schedules, updates, scan profiles and more.
- **Mail Gateway** - Opens the **Mail Gateway** configuration section. From this area, you can configure mail gateway settings, antispam settings, scanner settings and more.
- **More** - Opens the **More** options screen which contains options relating to the overall configuration of Comodo Antivirus and Mail Gateway.

1.7. Understanding Alerts

Antivirus alerts immediately warn you if a virus has been detected and provide options and information so you can make an informed decision on how to proceed. Alerts can also be used to instruct Comodo Antivirus on how it should behave in future when it encounters activities of the same type.



Name: Malware@#1xtkkvqax9gzy
Location: /home/johnsmith/Virus samples_...
More information: Unavailable

Answering an Antivirus Alert

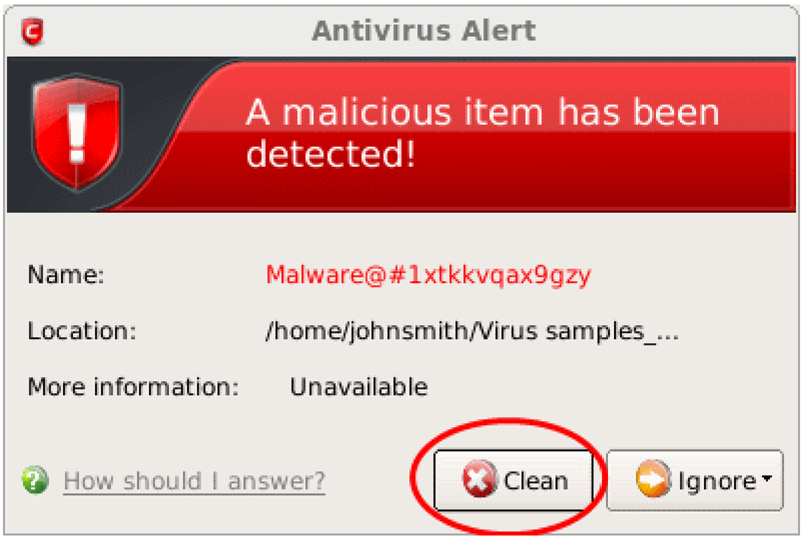
Alerts are generated whenever a virus or malware tries to be copied to or run on your system. The alert contains the name of the virus detected and the location of the virus on your disk and, if available, more information about the virus.

You can take one of the following steps to answer the Antivirus alert.

- Disinfect the file if there exists a disinfection routine for the detected file or move the file or application to **Quarantined Items** for later analysis.
- Ignore the alert only if you trust the application or the source of application by clicking 'Ignore'.

To disinfect the file or application

- Click the 'Clean' button.



Antivirus Alert

A malicious item has been detected!

Name: Malware@#1xtkkvqax9gzy

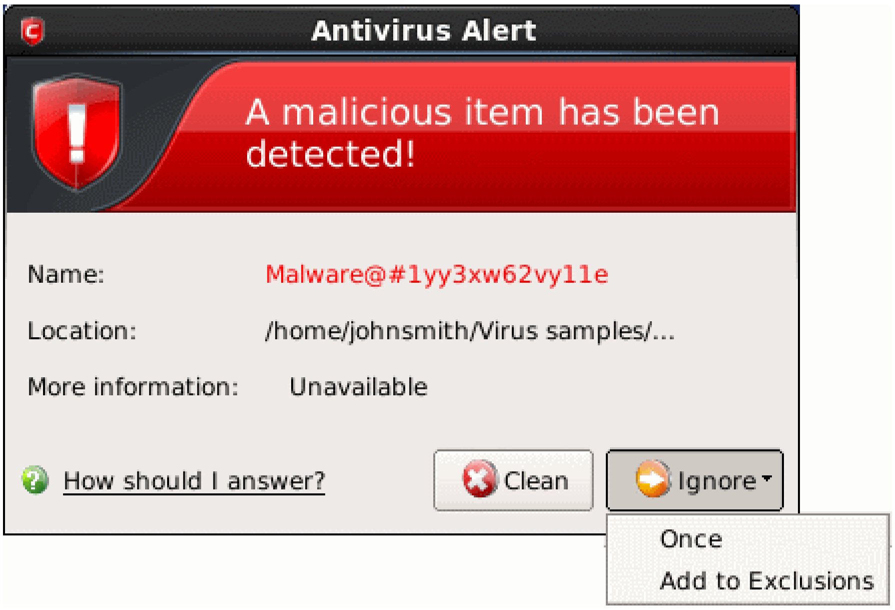
Location: /home/johnsmith/Virus samples_...

More information: Unavailable

Comodo Antivirus will disinfect and clean the file or application. If the threat detected is new one and the disinfection routine does not exist, then CAVL will move the file/application to **Quarantined Items** for later analysis. You can submit the file/application to Comodo for analysis from the Quarantine. Refer to **Quarantined Items** for more details.

To ignore the alert if you trust the file/application

- Click 'Ignore'. Selecting Ignore provides you with two options.



Antivirus Alert

A malicious item has been detected!

Name: Malware@#1yy3xw62vy11e

Location: /home/johnsmith/Virus samples/...

More information: Unavailable

- **Once** - If you click 'Once', the file is ignored this time only. If the same file is detected at a later date then another alert will be displayed.

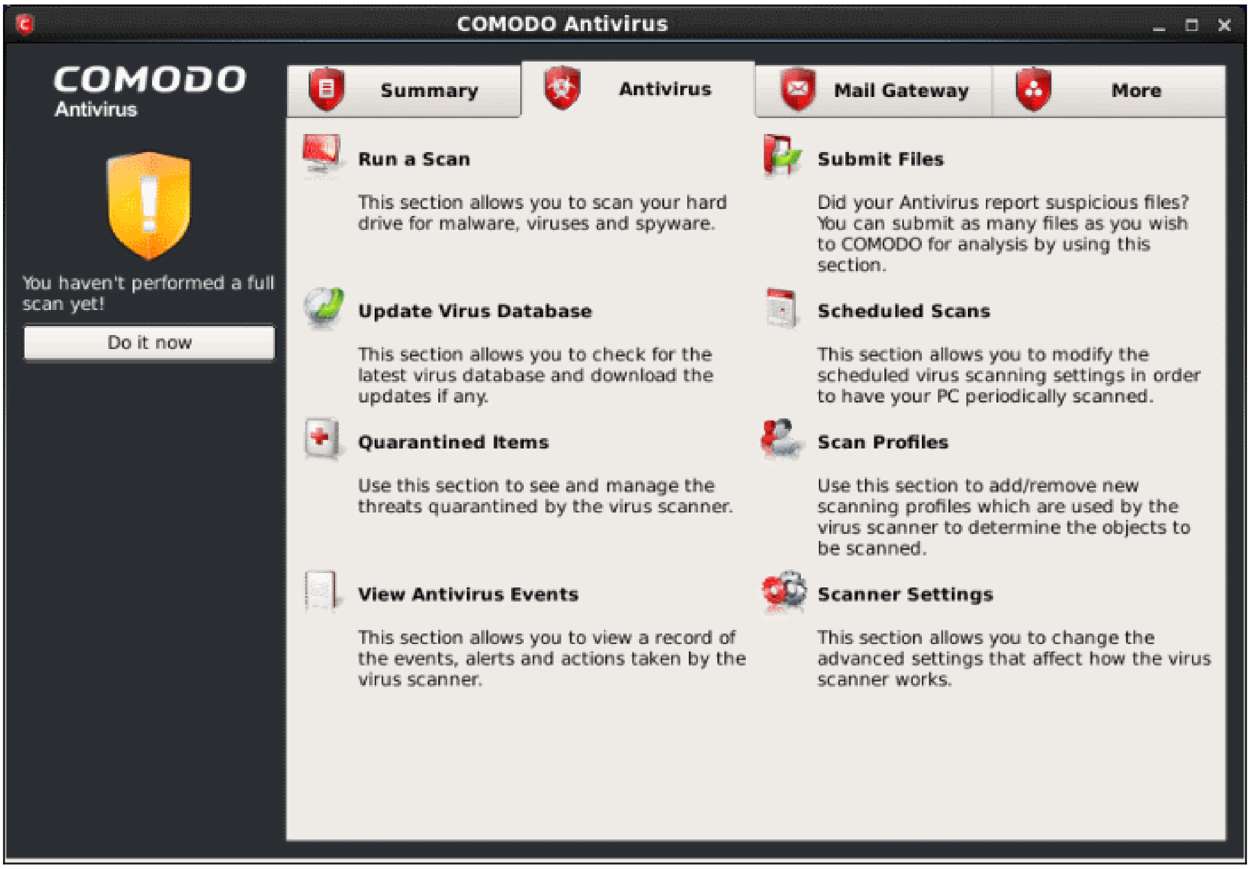
- **Add to Exclusions** - If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. This means CAVL will no longer report this file as malicious or raise an alert the next time the file is detected.

2.Antivirus Tasks - Introduction

The Antivirus Task Center allows you to run custom, on-demand virus scans and to configure how you want the antivirus scanner to behave.

This area also allows you to alter scan settings for each scan type and to use the fully featured scheduler to run scans according to a time table of your choice. Other features include the ability to create custom scan profiles, view/export event logs, specify update settings, submit files for analysis and to view any quarantined files.

The Antivirus tasks center can be accessed at all times by clicking on the Antivirus tab from the main interface.



You haven't performed a full scan yet!

Run a Scan

This section allows you to scan your hard drive for malware, viruses and spyware.

Submit Files

Did your Antivirus report suspicious files? You can submit as many files as you wish to COMODO for analysis by using this section.

Update Virus Database

This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans

This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items

Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles

Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

View Antivirus Events

This section allows you to view a record of the events, alerts and actions taken by the virus scanner.

Scanner Settings

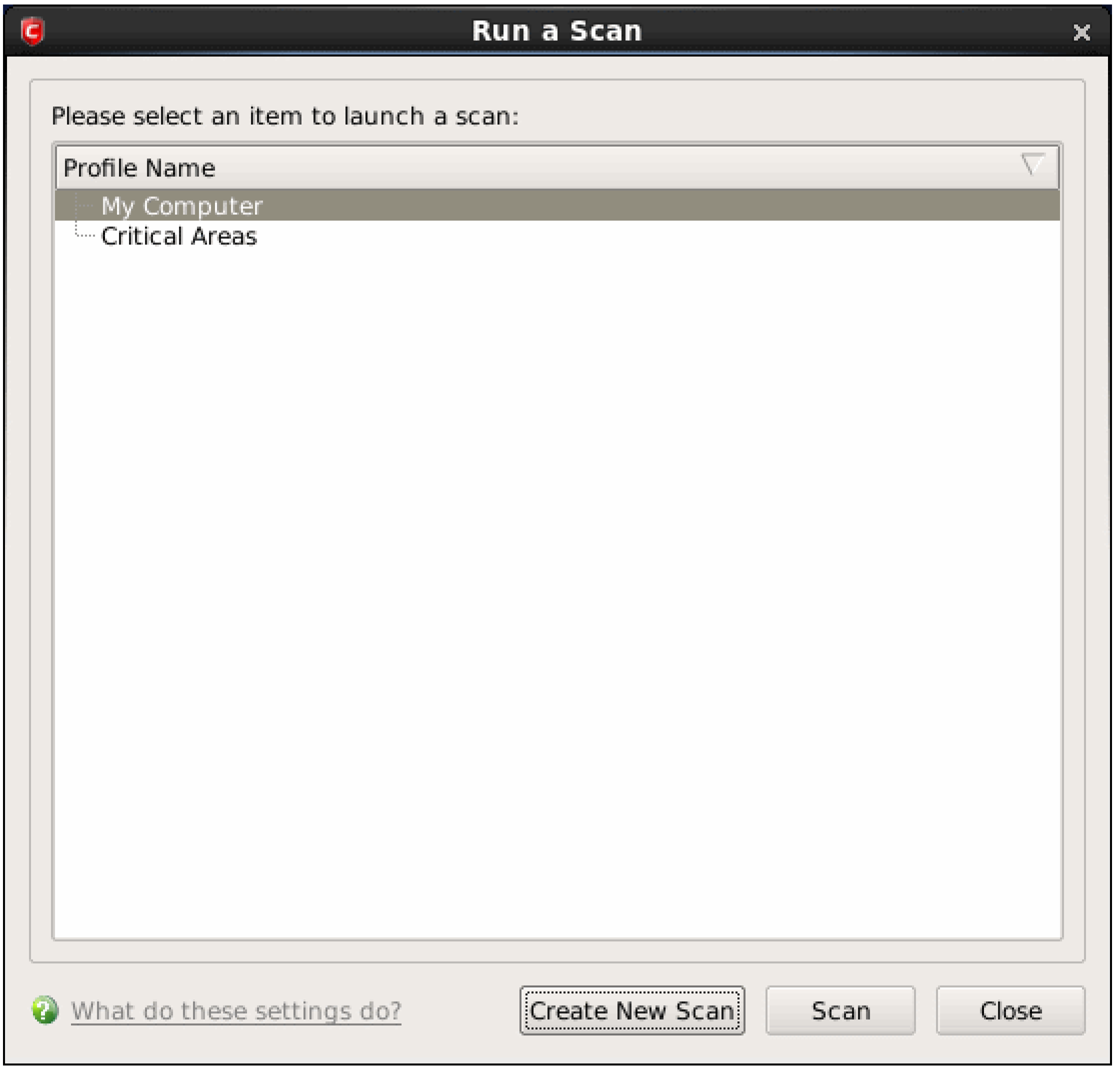
This section allows you to change the advanced settings that affect how the virus scanner works.

The Antivirus main configuration area provides easy access to all the features. Click the links below to see detailed explanations of each area in this section.

- Run a Scan
- Update Virus Database
- Quarantined Items
- View Antivirus Events
- Submit Files
- Scheduled Scans
- Scan Profiles
- Scanner Settings

2.1. Run a Scan

The 'Run a Scan' area allows you to launch an On-Demand Scan on an item of your choice. The item can be anything you choose - your entire computer, a specific drive or partition or even a single file. You can also choose to scan a wide range of removable storage devices such as CD's, DVD's, external hard-drives, USB connected drives, digital cameras and more.



You have two main options available when from the 'Run a Scan' interface:

1. Scan a **preselected area**
2. Define a **custom scan** of the areas you choose

Scanning Preselected Areas

Comodo Antivirus has two pre-defined scan profiles - 'My Computer' and 'Critical Areas'. These cannot be edited or removed. They are:

- **My Computer** *(Default)* - When this Profile is selected, Comodo Antivirus scans every local drive, folder and file on your system.
- **Critical Areas** - When this profile is selected, Comodo Antivirus runs a targeted scan of important operating system files and folders.

To run one of these profiles, simply highlight it from the list and click the 'Scan' button.

Custom Scan

To run a scan on a particular item of your choosing, you first need to create a scan profile. To do this:

- Click the 'Create New Scan' button.
- Type a name for your new profile in the 'Scan Profile' dialog (for example, 'My External Drives').
- Click the 'Add' button to choose the files, folders or drives you wish to include in the scan profile. You can select multiple items.
- Click 'Apply' to return to the 'Scan Profile' dialog then 'Apply' again. Your new profile will be listed in the 'Run a Scan' dialog (see '**Create a scan profile**' if you need more help with this).
- Select your new profile in the list and click 'Scan'.

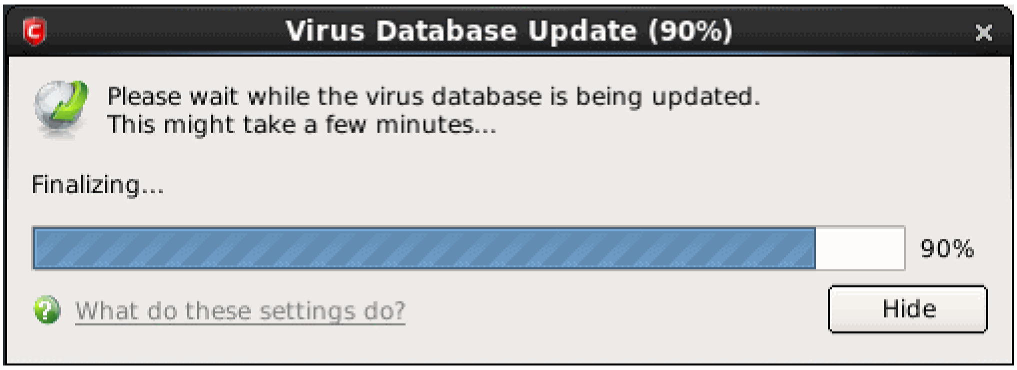
The scan will begin. Next, see:

- **Scan progress and results**
- **The results window**
- **Saving results as a text file**
- **Disinfecting or moving threats to quarantine**
- **Ignore a result once / Ignore and create an exception**

Tip: For more details on scan profiles, refer to section **Antivirus Tasks > Scan Profiles**.

Scan Progress and Results

Before running the scan, Comodo Antivirus will first check for AV database updates. If updates are available they will be downloaded and installed.



Virus Database Update (90%)

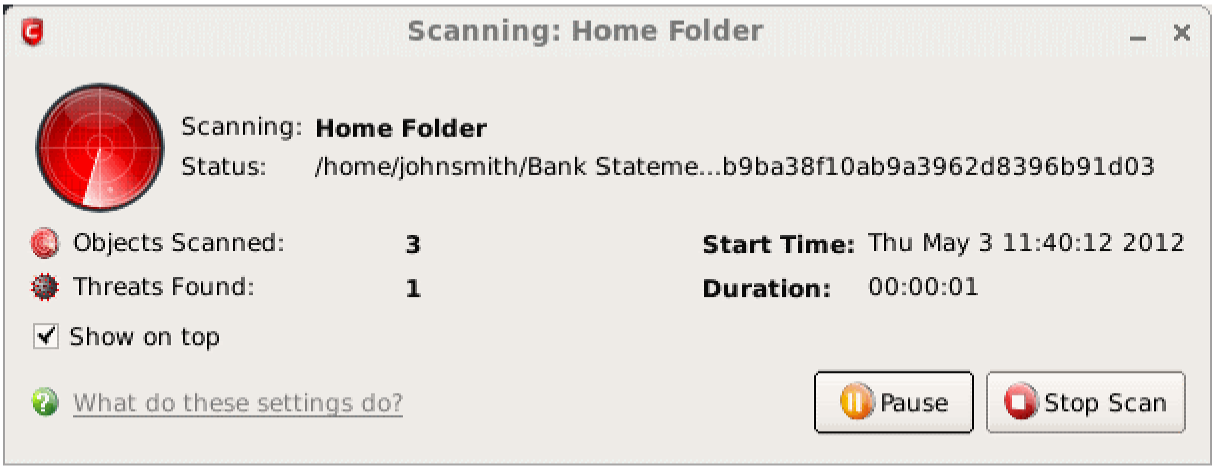
Please wait while the virus database is being updated.
This might take a few minutes...

Finalizing...

90%

The scan, based on the profile you selected, will begin immediately after updates have been installed. The progress dialog displays the profile name, the location that is currently being scanned, the start time and duration of the scan, the total number of objects scanned so far and the number of threats found.

Clicking the 'Pause' button will suspend the scan until such time that you click 'Resume'. Click 'Stop Scan' to abort the scan process altogether.



Scanning: Home Folder

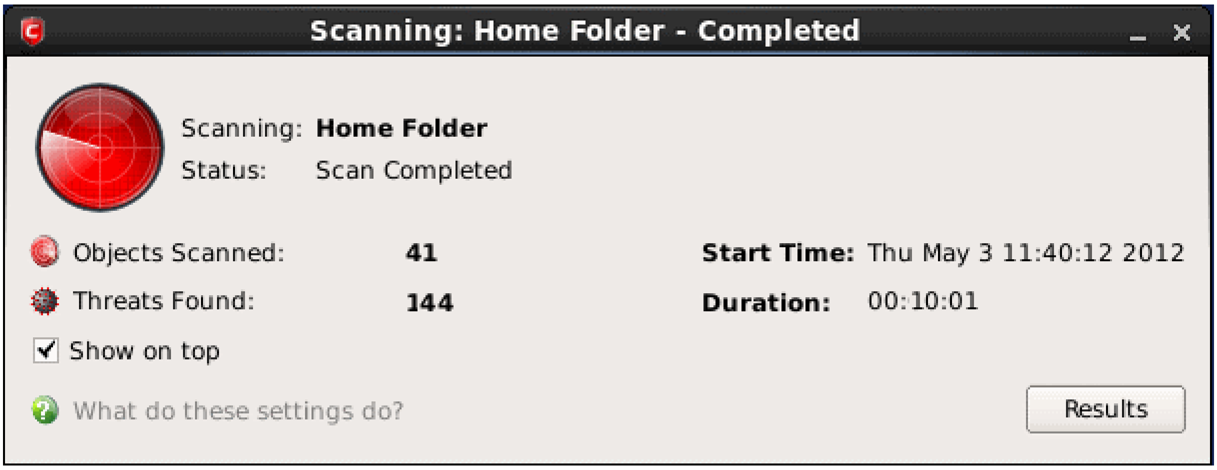
Scanning: **Home Folder**
Status: /home/johnsmith/Bank Stateme...b9ba38f10ab9a3962d8396b91d03

Objects Scanned: **3**
Threats Found: **1**
Start Time: Thu May 3 11:40:12 2012
Duration: 00:00:01

☑ Show on top

On completion of scanning, the 'scanning completed' window will be displayed.

- Click the 'Results' to view the results of the scan.



Scanning: Home Folder - Completed

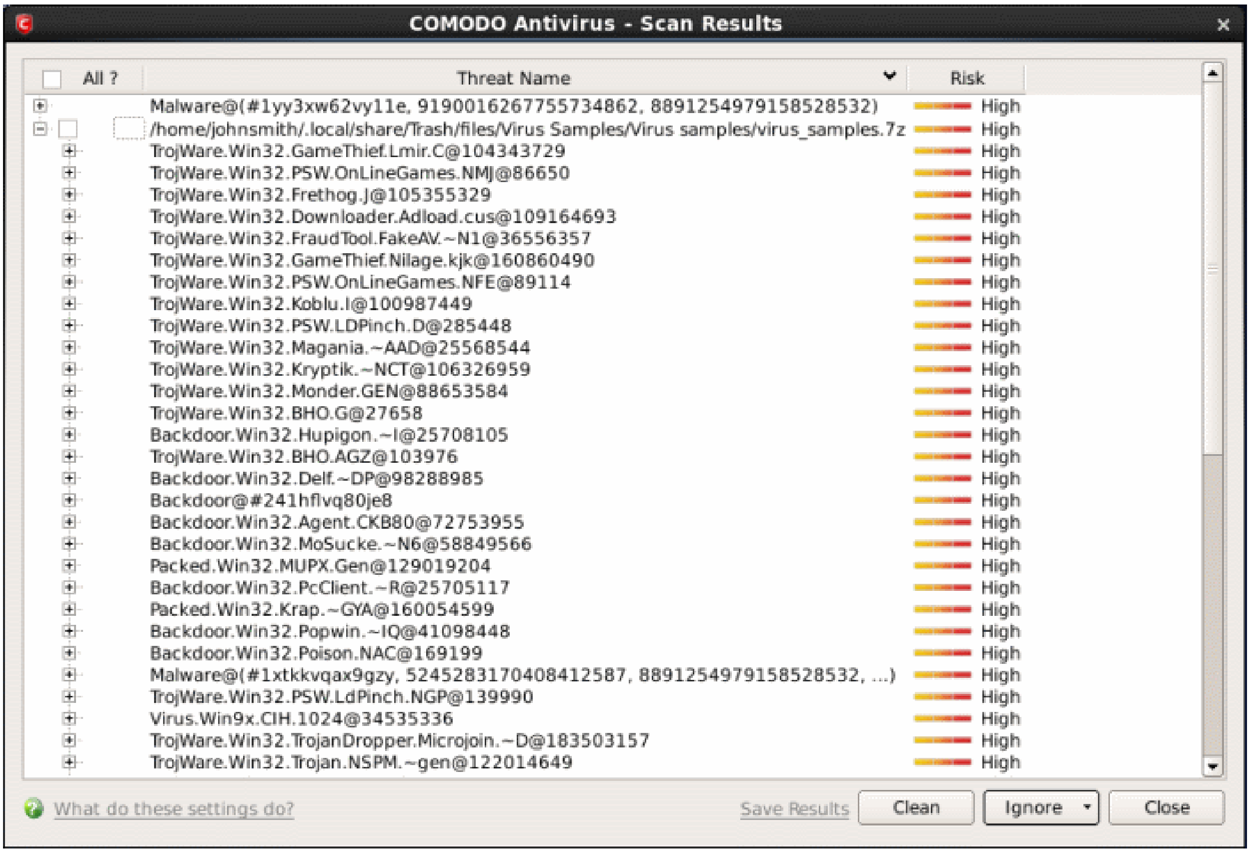
Scanning: **Home Folder**
Status: Scan Completed

Objects Scanned: **41**
Threats Found: **144**
Start Time: Thu May 3 11:40:12 2012
Duration: 00:10:01

☑ Show on top

The Results Window

The scan results window will display the number of objects scanned and the number of threats (viruses, malware and so on).



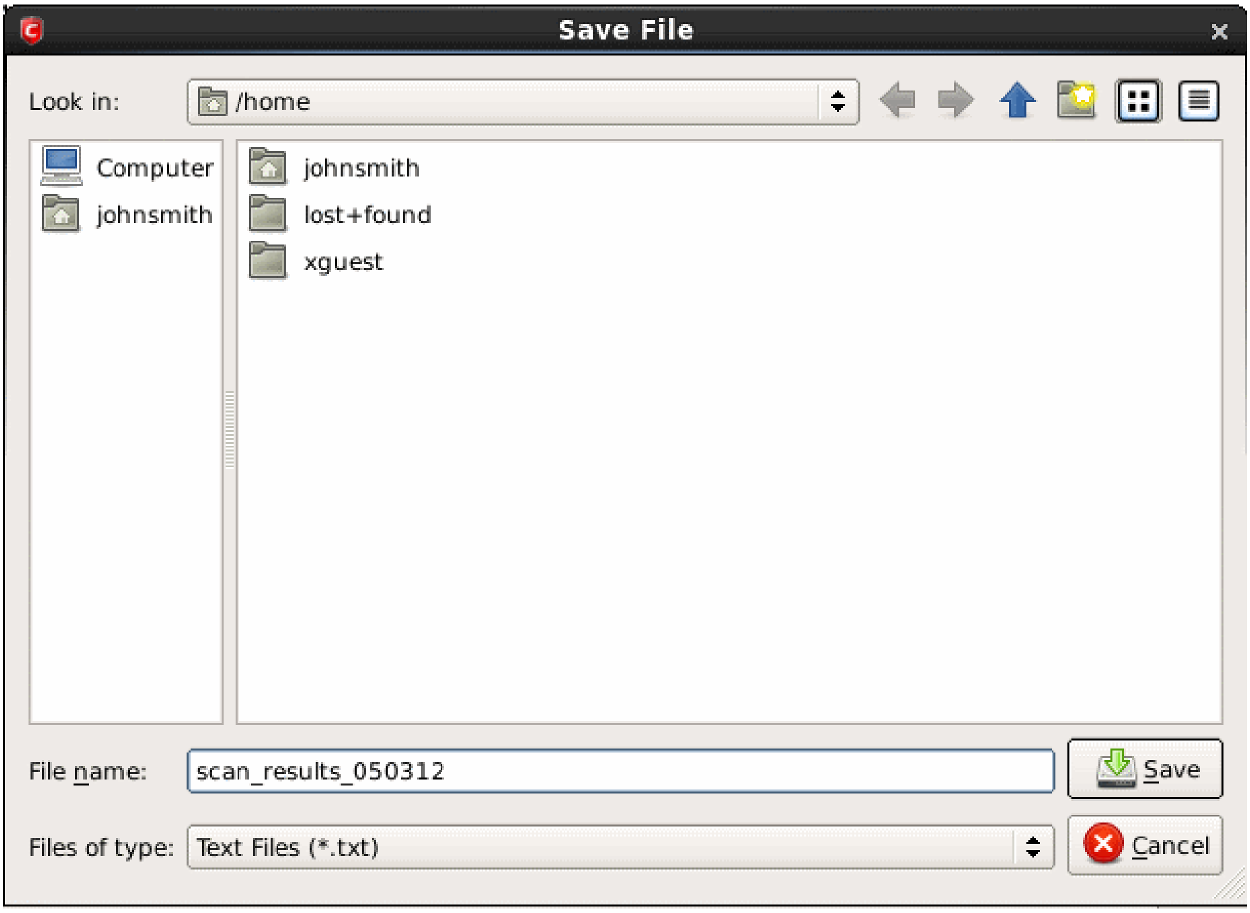
COMODO Antivirus - Scan Results

□ All ?	Threat Name	Risk
⊞	Malware@(#1yy3xw62vy11e, 9190016267755734862, 8891254979158528532)	High
⊟ □	/home/johnsmith/.local/share/Trash/files/Virus Samples/Virus samples/virus_samples.7z	High
⊞	TrojWare.Win32.GameThief.Lmir.C@104343729	High
⊞	TrojWare.Win32.PSW.OnLineGames.NMJ@86650	High
⊞	TrojWare.Win32.Frethog.J@105355329	High
⊞	TrojWare.Win32.Downloader.Adload.cus@109164693	High
⊞	TrojWare.Win32.FraudTool.FakeAV.~N1@36556357	High
⊞	TrojWare.Win32.GameThief.Nilage.kjk@160860490	High
⊞	TrojWare.Win32.PSW.OnLineGames.NFE@89114	High
⊞	TrojWare.Win32.Koblu.I@100987449	High
⊞	TrojWare.Win32.PSW.LDPinch.D@285448	High
⊞	TrojWare.Win32.Magania.~AAD@25568544	High
⊞	TrojWare.Win32.Kryptik.~NCT@106326959	High
⊞	TrojWare.Win32.Monder.GEN@88653584	High
⊞	TrojWare.Win32.BHO.G@27658	High
⊞	Backdoor.Win32.Hupigon.~I@25708105	High
⊞	TrojWare.Win32.BHO.AGZ@103976	High
⊞	Backdoor.Win32.Delf.~DP@98288985	High
⊞	Backdoor@#241hflvq80je8	High
⊞	Backdoor.Win32.Agent.CKB80@72753955	High
⊞	Backdoor.Win32.MoSucke.~N6@58849566	High
⊞	Packed.Win32.MUPX.Gen@129019204	High
⊞	Backdoor.Win32.PcClient.~R@25705117	High
⊞	Packed.Win32.Krap.~GYA@160054599	High
⊞	Backdoor.Win32.Popwin.~IQ@41098448	High
⊞	Backdoor.Win32.Poison.NAC@169199	High
⊞	Malware@(#1xtkkvqax9gzy, 5245283170408412587, 8891254979158528532, ...)	High
⊞	TrojWare.Win32.PSW.LdPinch.NGP@139990	High
⊞	Virus.Win9x.CIH.1024@34535336	High
⊞	TrojWare.Win32.TrojanDropper.Microjoin.~D@183503157	High
⊞	TrojWare.Win32.Trojan.NSPM.~gen@122014649	High

You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header. To select all the entries for actions such as moving them to quarantine or disinfect, select the check box beside 'All?'.

To save the Scan Results as a Text File

- Click 'Save Results' and enter the location in the 'Save' dialog box.

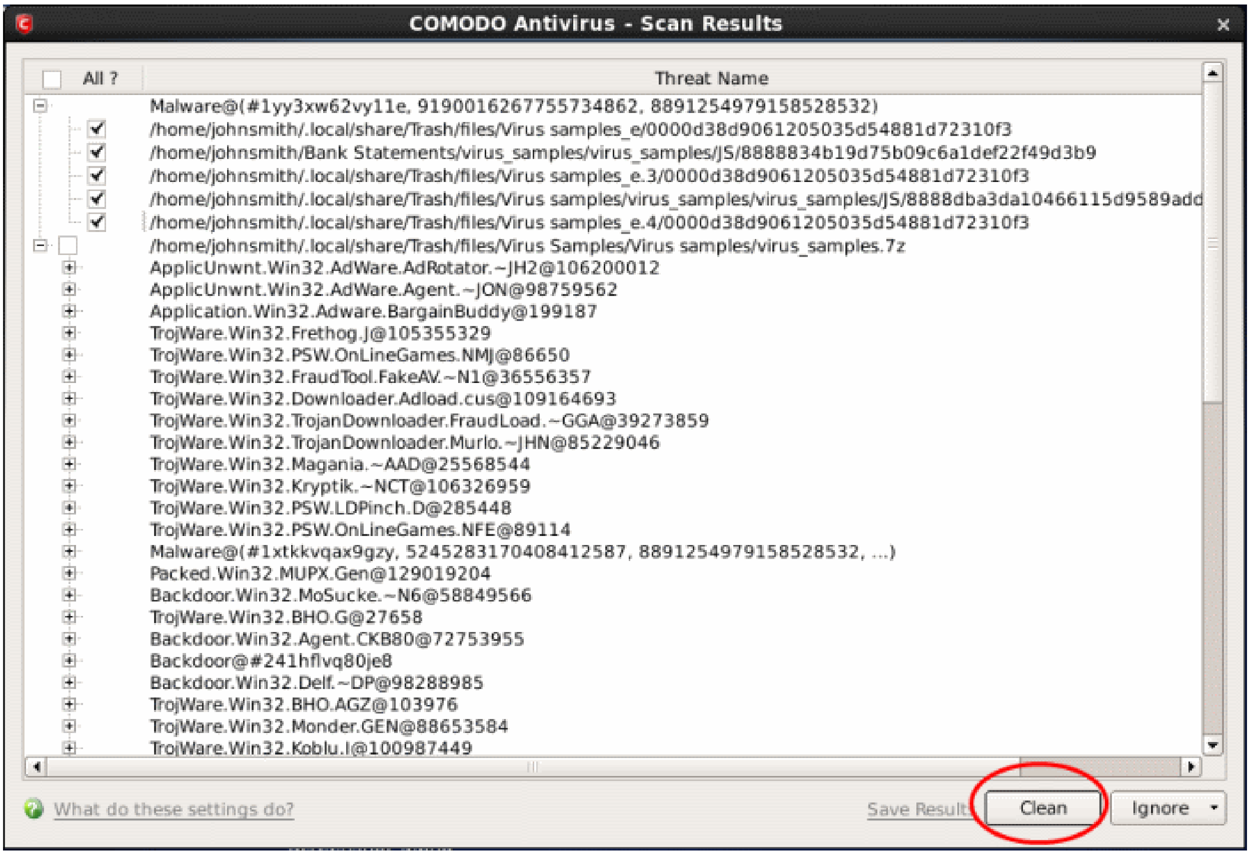


File name: scan_results_050312

Files of type: Text Files (*.txt)

To disinfect a file or application

- Select the application from the results and click the 'Clean' button.

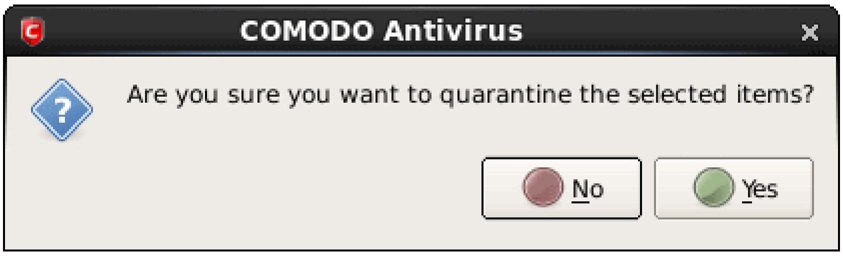


COMODO Antivirus - Scan Results

```
□ All ?   Threat Name
Malware@(#1yy3xw62vy11e, 9190016267755734862, 8891254979158528532)
  ☑ /home/johnsmith/.local/share/Trash/files/Virus samples_e/0000d38d9061205035d54881d72310f3
  ☑ /home/johnsmith/Bank Statements/virus_samples/virus_samples/JS/8888834b19d75b09c6a1def22f49d3b9
  ☑ /home/johnsmith/.local/share/Trash/files/Virus samples_e.3/0000d38d9061205035d54881d72310f3
  ☑ /home/johnsmith/.local/share/Trash/files/Virus samples/virus_samples/virus_samples/JS/8888dba3da10466115d9589add
  ☑ /home/johnsmith/.local/share/Trash/files/Virus samples_e.4/0000d38d9061205035d54881d72310f3
□ /home/johnsmith/.local/share/Trash/files/Virus Samples/Virus samples/virus_samples.7z
ApplicUnwnt.Win32.AdWare.AdRotator.~JH2@106200012
ApplicUnwnt.Win32.AdWare.Agent.~JON@98759562
Application.Win32.Adware.BargainBuddy@199187
TrojWare.Win32.Frethog.J@105355329
TrojWare.Win32.PSW.OnLineGames.NMJ@86650
TrojWare.Win32.FraudTool.FakeAV.~N1@36556357
TrojWare.Win32.Downloader.Adload.cus@109164693
TrojWare.Win32.TrojanDownloader.FraudLoad.~GGA@39273859
TrojWare.Win32.TrojanDownloader.Murlo.~JHN@85229046
TrojWare.Win32.Magania.~AAD@25568544
TrojWare.Win32.Kryptik.~NCT@106326959
TrojWare.Win32.PSW.LDPinch.D@285448
TrojWare.Win32.PSW.OnLineGames.NFE@89114
Malware@(#1xtkkvqax9gzy, 5245283170408412587, 8891254979158528532, ...)
Packed.Win32.MUPX.Gen@129019204
Backdoor.Win32.MoSucke.~N6@58849566
TrojWare.Win32.BHO.G@27658
Backdoor.Win32.Agent.CKB80@72753955
Backdoor@#241hflvq80je8
Backdoor.Win32.Delf.~DP@98288985
TrojWare.Win32.BHO.AGZ@103976
TrojWare.Win32.Monder.GEN@88653584
TrojWare.Win32.Koblu.I@100987449
```

If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to **Quarantined Items**.

A confirmation dialog will be displayed for moving the threat(s) to quarantine.



COMODO Antivirus

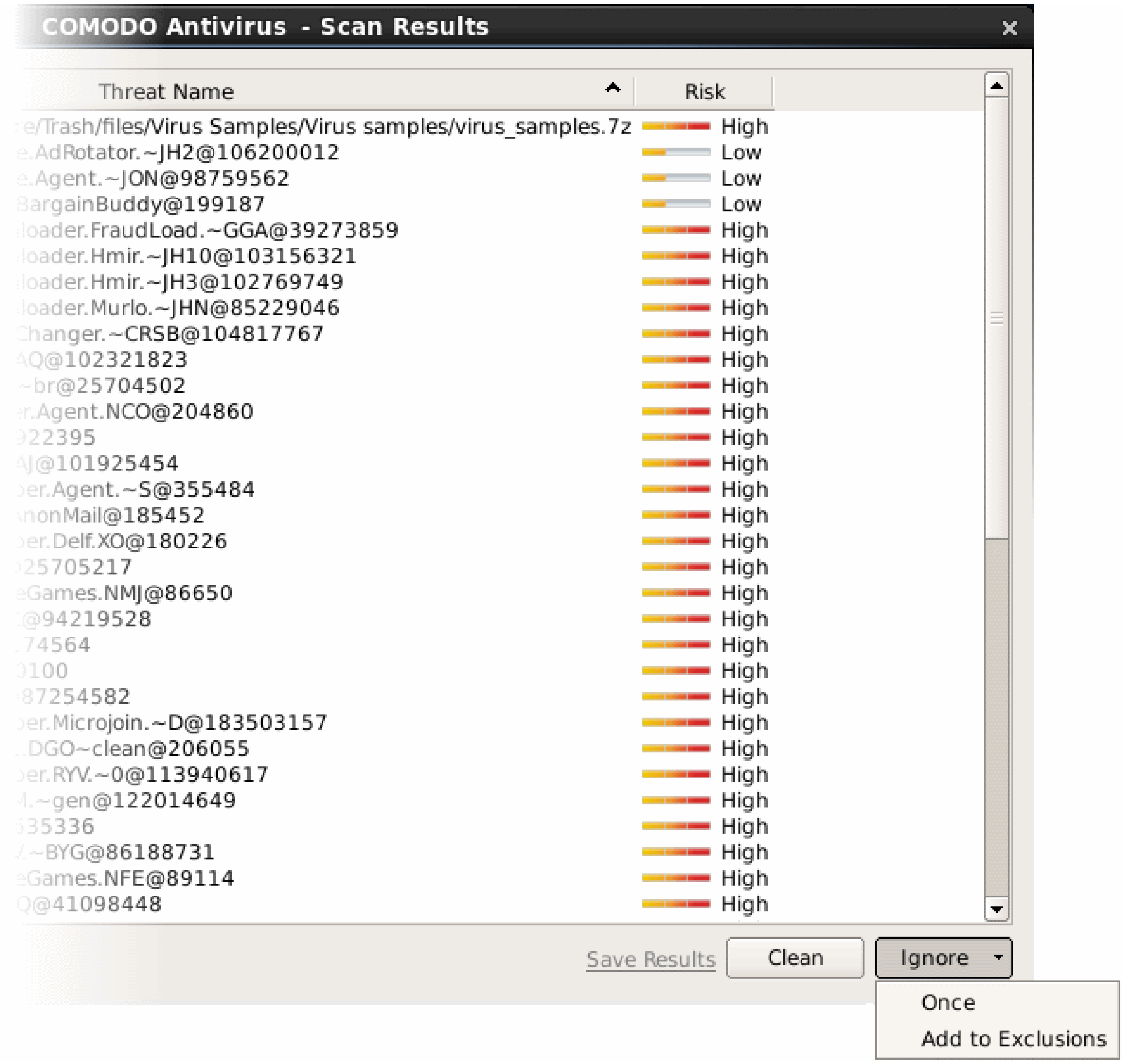
Are you sure you want to quarantine the selected items?

- Click 'Yes' to move the infected items to quarantine.

To ignore an application / file you consider as safe from the threat list

- Select the application from the results.

TIP: To select all the items at once, select the 'All?' checkbox at the top left of the interface.



Threat Name	Risk
re/Trash/files/Virus Samples/Virus samples/virus_samples.7z	High
e.AdRotator.~JH2@106200012	Low
e.Agent.~JON@98759562	Low
BargainBuddy@199187	Low
loader.FraudLoad.~GGA@39273859	High
loader.Hmir.~JH10@103156321	High
loader.Hmir.~JH3@102769749	High
loader.Murlo.~JHN@85229046	High
Changer.~CRSB@104817767	High
AQ@102321823	High
~br@25704502	High
r.Agent.NCO@204860	High
922395	High
AJ@101925454	High
per.Agent.~S@355484	High
nonMail@185452	High
per.Delf.XO@180226	High
25705217	High
eGames.NMJ@86650	High
@94219528	High
74564	High
0100	High
87254582	High
per.Microjoin.~D@183503157	High
DGO~clean@206055	High
per.RYV.~0@113940617	High
M.~gen@122014649	High
535336	High
V.~BYG@86188731	High
eGames.NFE@89114	High
Q@41098448	High

- Click the 'Ignore' button.

Selecting Ignore provides you with two options.

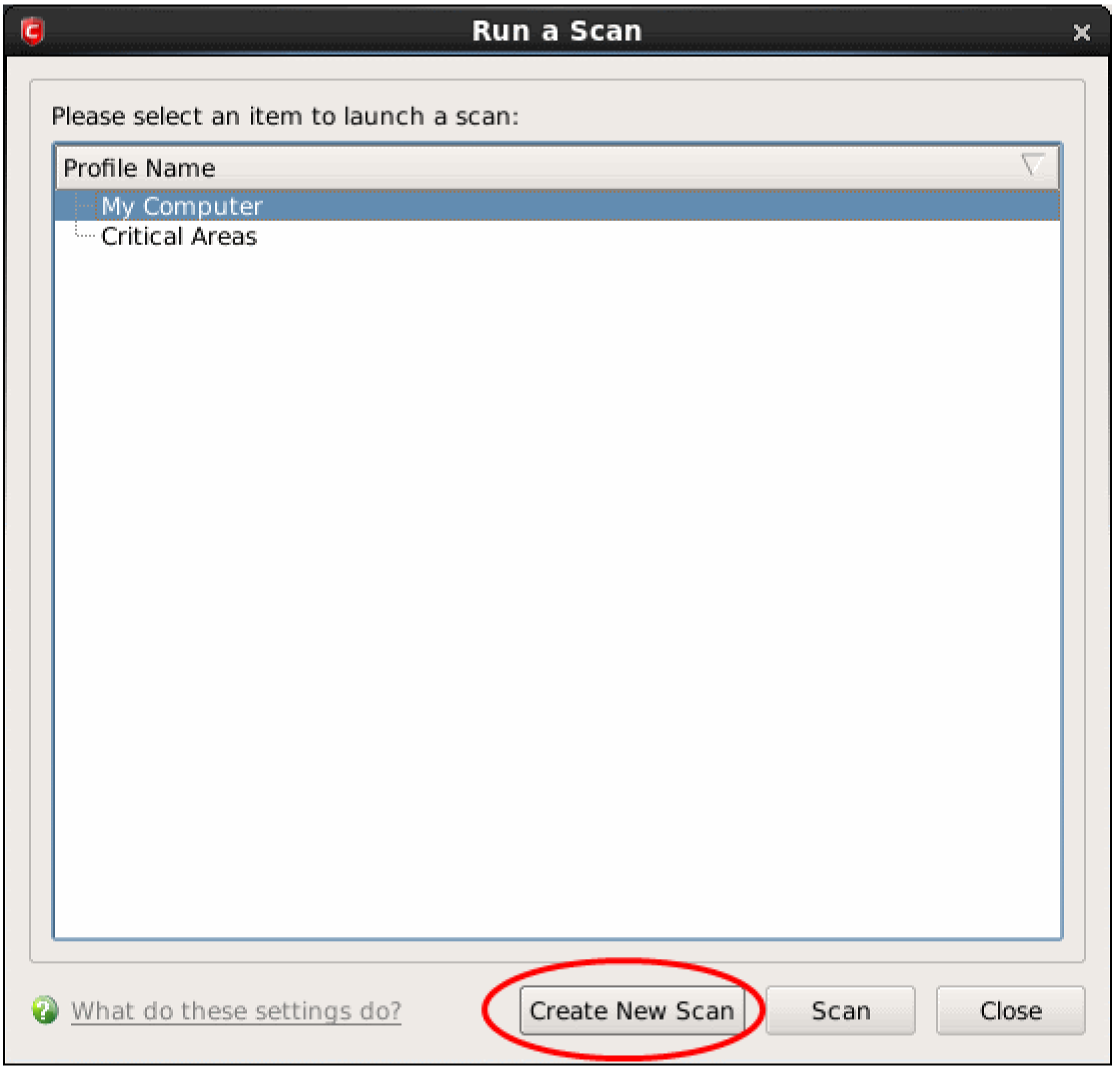
- **Once** - If you click 'Once', the virus is ignored only at that time only. If the same application invokes again, an Antivirus alert is displayed.
- **Add to Exclusions** - If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. The alert is not generated if the same application invokes again.

Creating a Scan Profile

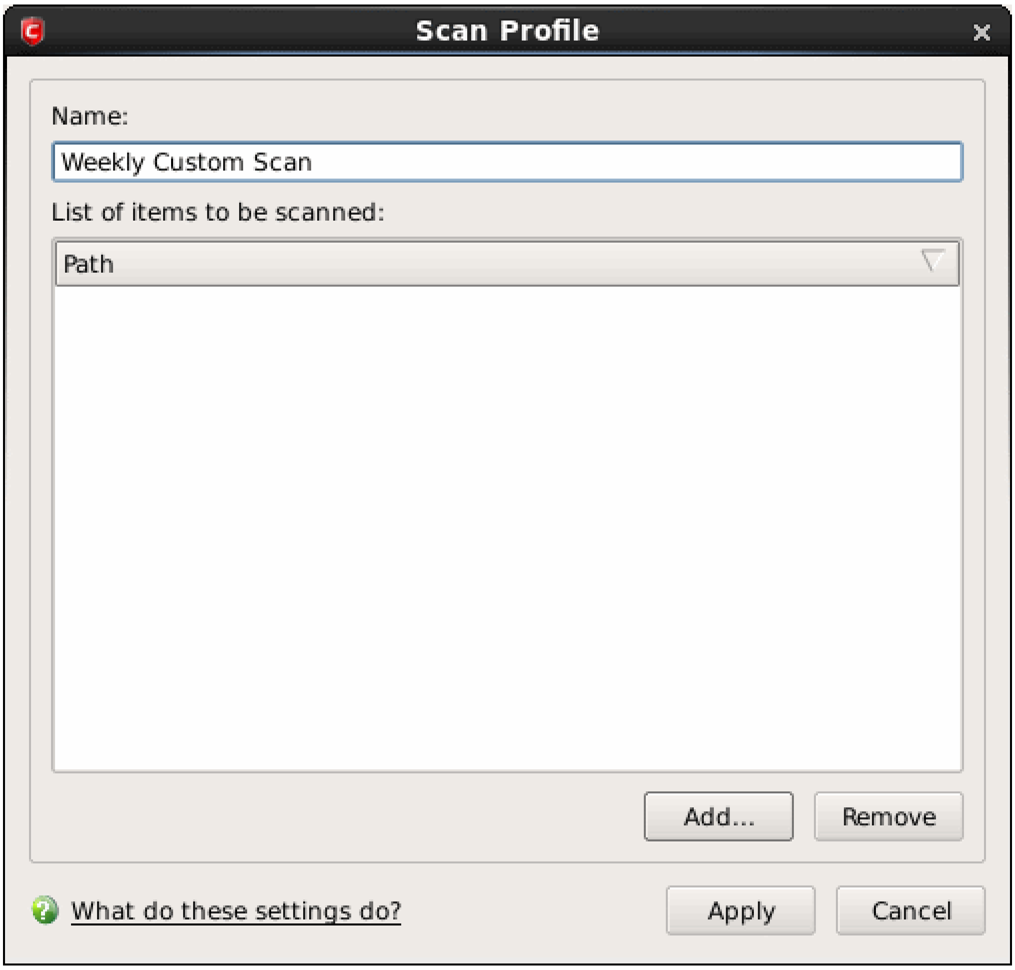
Scan Profiles are the user-defined profiles containing specific areas on your system that you wish to scan and can be re-used for all future scans.

To create a new scan profile

- Click 'Create New Scan' in the 'Run a Scan' interface.



A 'Scan Profile' configuration screen appears.

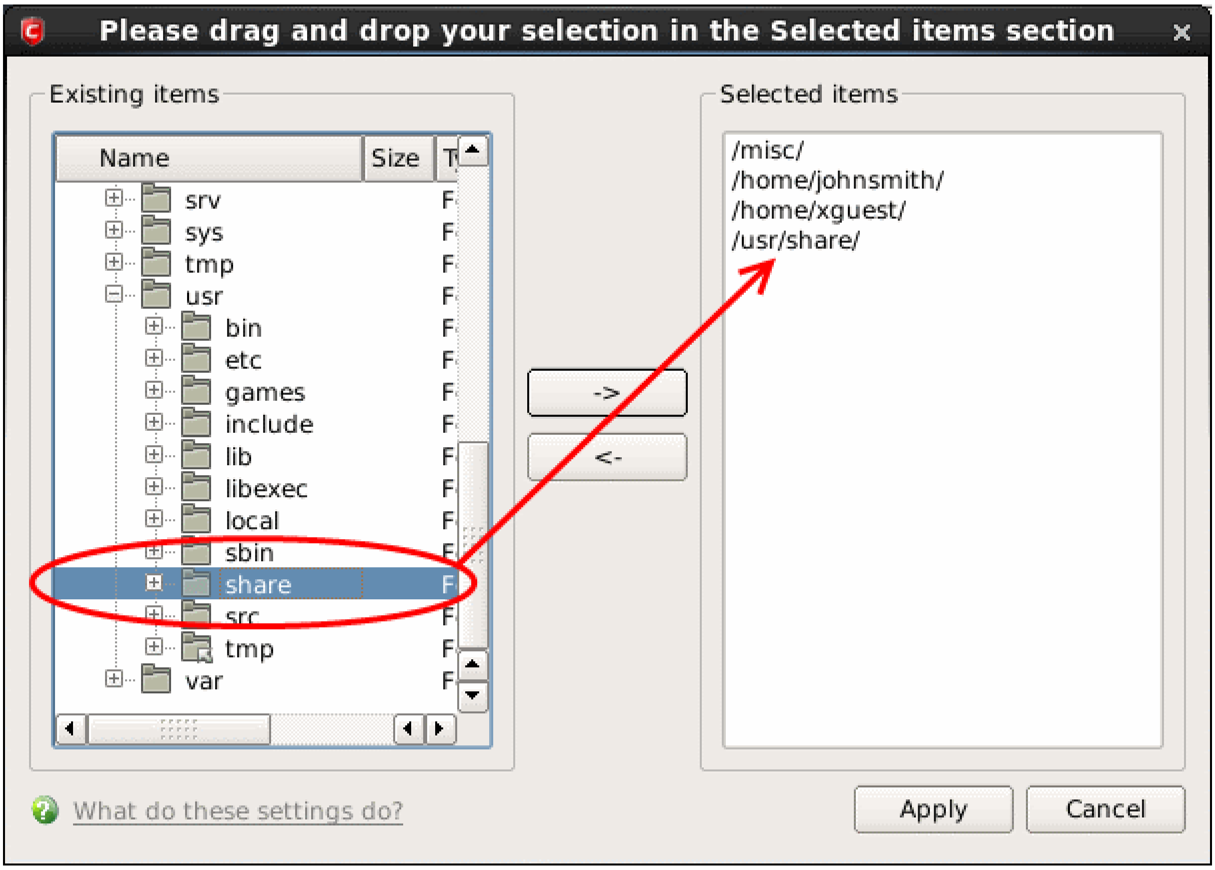


Name: Weekly Custom Scan

List of items to be scanned:

- Type a name for the scan profile to be created in the 'Name' box and click the 'Add' button.

A configuration screen appears, prompting you to select the locations to be scanned when the newly created scan profile is selected.



Please drag and drop your selection in the Selected items section

Existing items

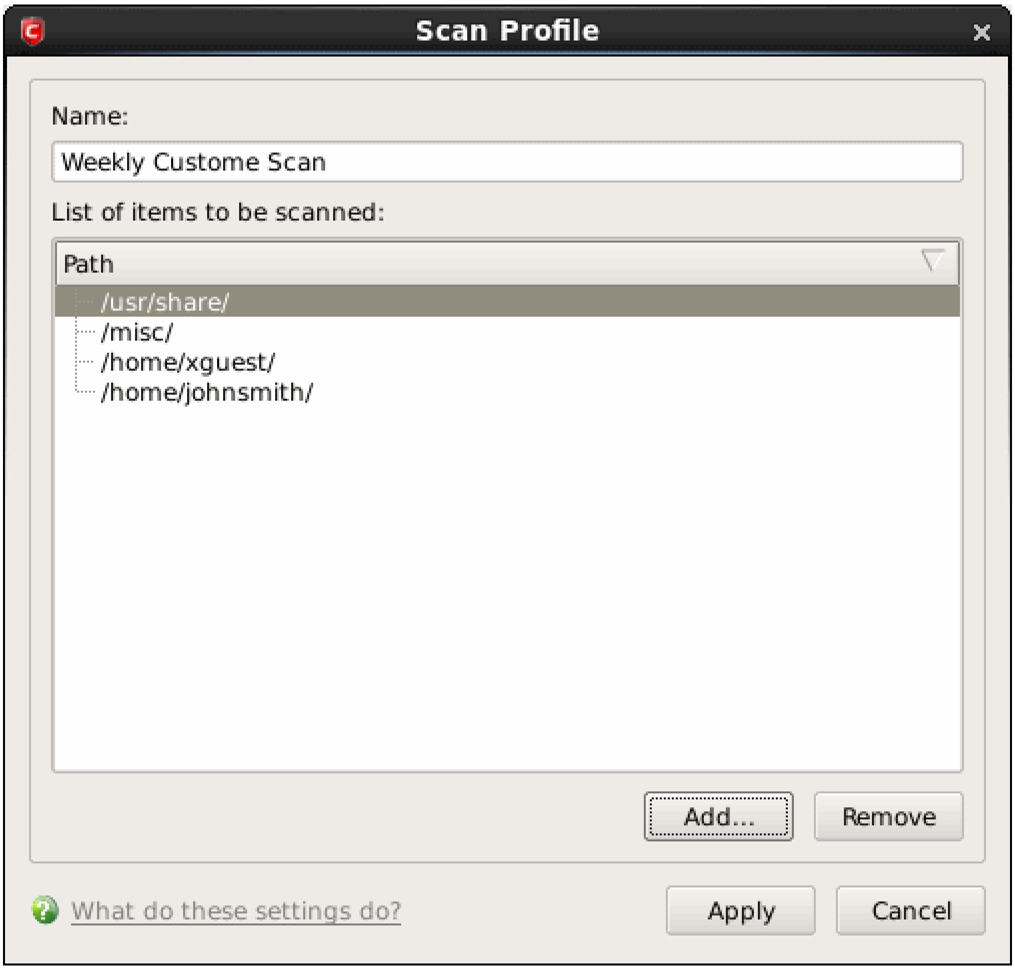
Name	Size	T
srv		F
sys		F
tmp		F
usr		F
bin		F
etc		F
games		F
include		F
lib		F
libexec		F
local		F
sbin		F
share		F
src		F
tmp		F
var		F

Selected items

/misc/
/home/johnsmith/
/home/xguest/
/usr/share/

- Select the locations from the left column, drag and drop to the right column or select the locations and click right arrow to move selected folders to right column.
- Click 'Apply' in the configuration screen.

The Scan Profile screen will be displayed with the added items for the new scan profile.



Name: Weekly Custome Scan

List of items to be scanned:

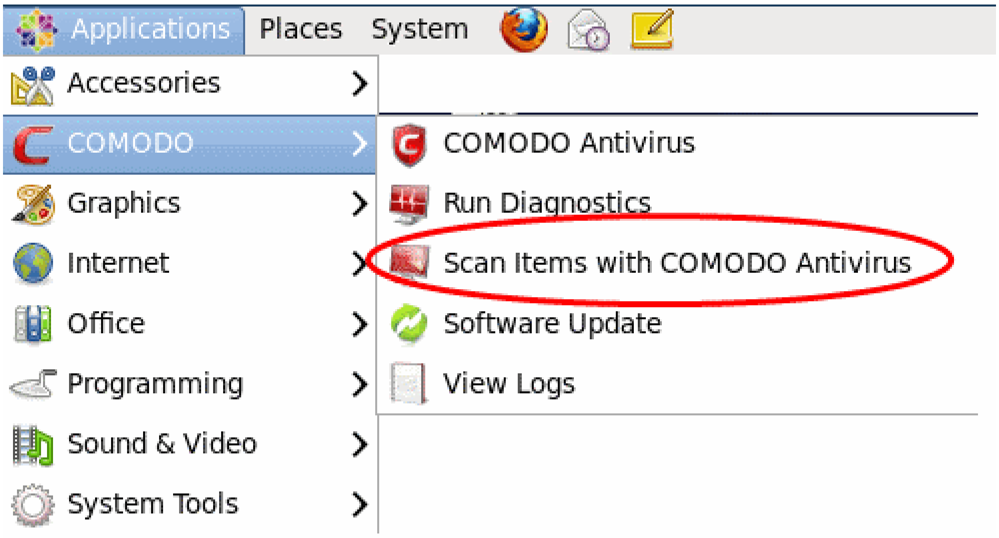
```
Path
/usr/share/
/misc/
/home/xguest/
/home/johnsmith/
```

- Review the items added. If you want to add more items, then click the 'Add' button again and repeat the process.
- Once done, click the 'Apply' button for the new scan profile to be created.
- Repeat the process to create more Scan Profiles.

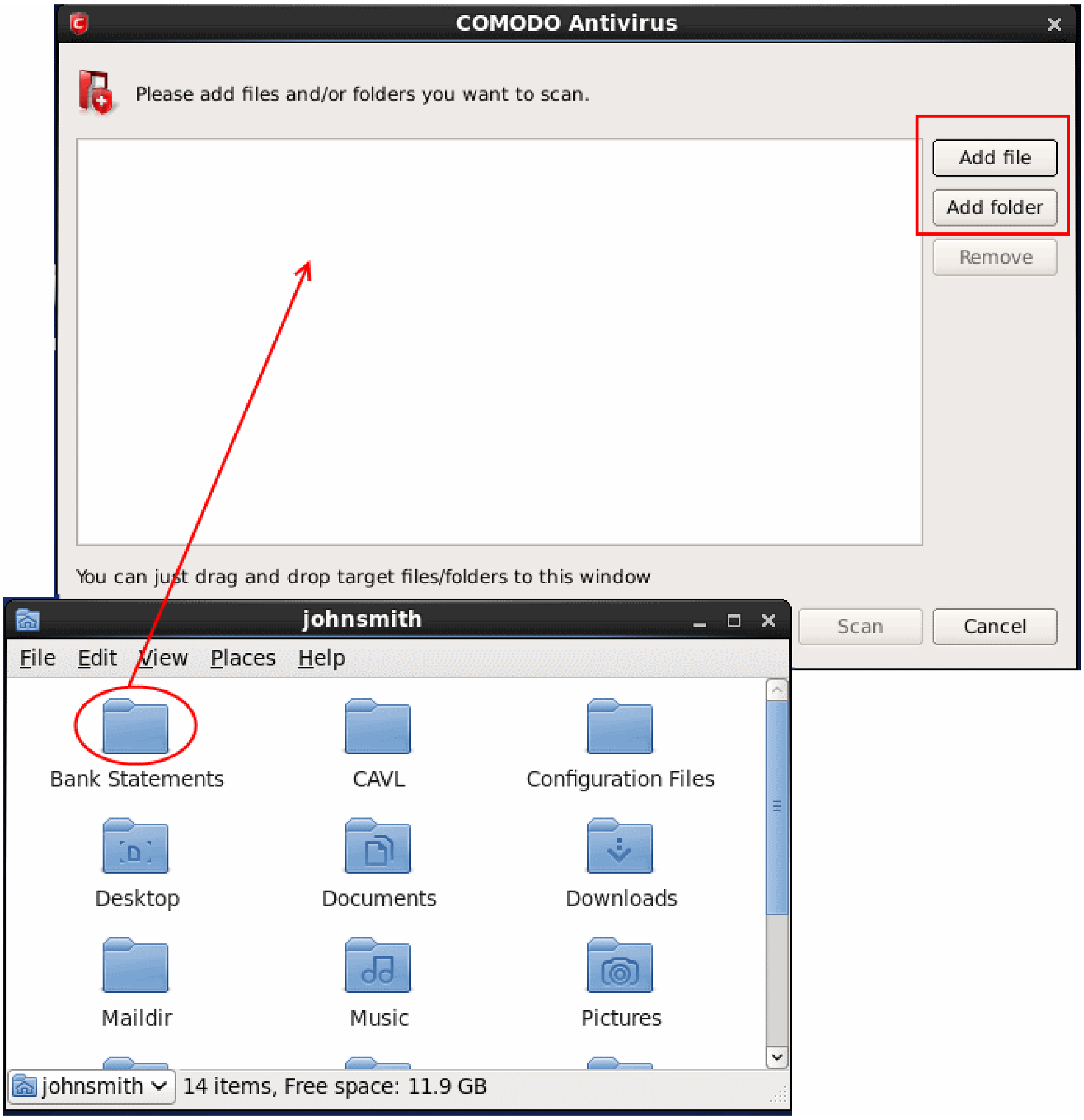
Note: You can also create new Scan Profiles by accessing **Scan Profiles** in the Antivirus Screen..

Instantly Scan Objects

You can instantly virus scan virtually any file, folder, photo, application or hard-drive by clicking 'Scan Items with COMODO Antivirus' in the Applications menu.



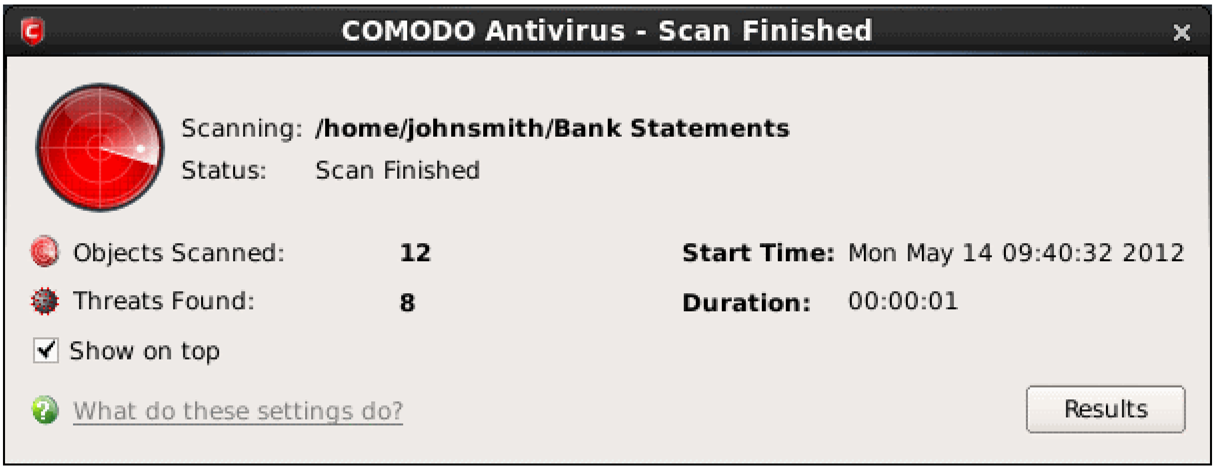
You can simply drag and drop files or add files and folders using the 'Add File' and 'Add Folder' buttons located on the right side of the interface and click the 'Scan' button.


COMODO Antivirus

Please add files and/or folders you want to scan.

You can just drag and drop target files/folders to this window

After the scanning process is completed, the 'Scan Finished' dialog will be displayed.



COMODO Antivirus - Scan Finished

Scanning: /home/johnsmith/Bank Statements
Status: Scan Finished

Objects Scanned: 12
Threats Found: 8
Start Time: Mon May 14 09:40:32 2012
Duration: 00:00:01

☑ Show on top

- Click the 'Results' button to view the scan results.
- See the section '**The Results Window**' to know how to deal with the infected files/folders.

2.2. Update Virus Database

In order to guarantee the relevance of your antivirus software, it is imperative that your virus databases are updated as regularly as possible.

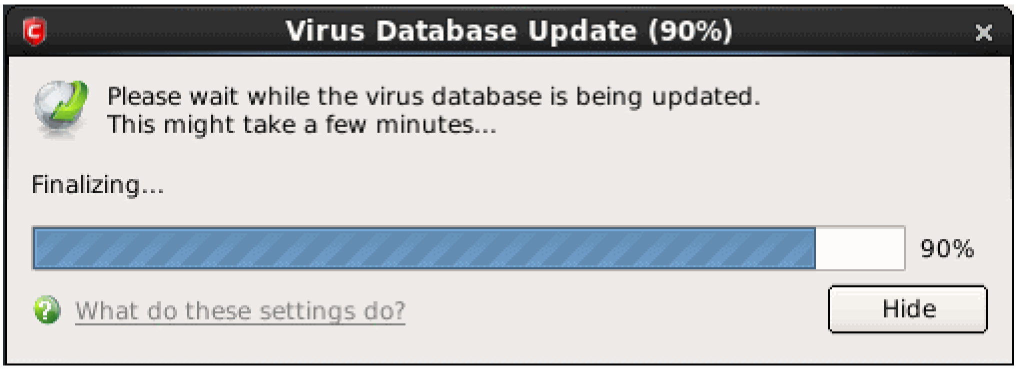
Our antivirus database is maintained and updated around the clock by a team of dedicated technicians, providing you with the solutions to the latest virus outbreaks. Updates can be downloaded to your system **manually** or **automatically** from Comodo's update servers.

To manually check for the latest virus Database and then download the updates

- Click on the 'Update Virus Database' from the main Antivirus Task Manager Screen.

Note: You must be connected to Internet to download the updates.

A dialog box appears, showing you the progress of update process.



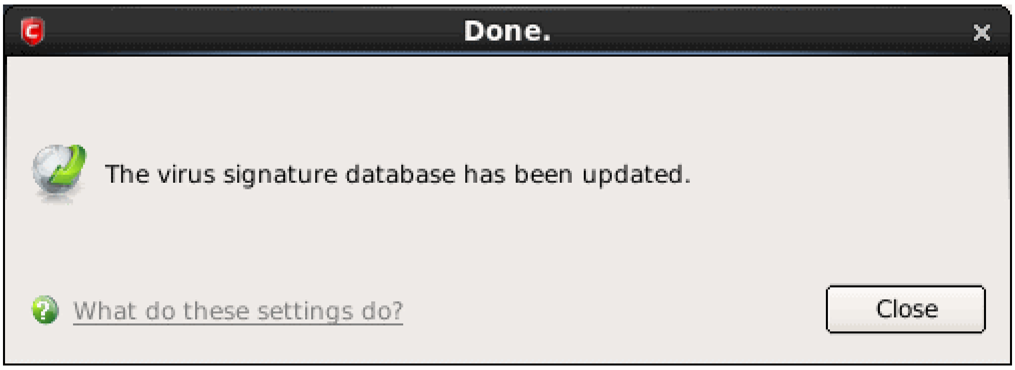
Virus Database Update (90%)

Please wait while the virus database is being updated.
This might take a few minutes...

Finalizing...

90%

You will see the following notification when the update process is complete:



The virus signature database has been updated.

When infected or possibly infected files are found, if the antivirus database has been not updated for a critically long time, or your computer has not been scanned for a long time, the main window of Comodo Antivirus recommends a course of action and gives a supporting explanation. We have customized our application to achieve optimal performance based on the extensive expertise of Comodo in the antivirus protection business.

Automatic Updates

Comodo AntiVirus checks for latest virus database updates from Comodo website and downloads the updates automatically. You can configure Comodo Antivirus to download updates automatically in the Scanner Settings for Real Time Scanning (On-Access Scanning), Manual Scanning (on-demand scanning) and Scheduled Scanning. Refer to **Real Time Scanning Settings**, **Manual Scanning Settings** and **Scheduled Scanning Settings**.

2.3. Quarantined Items

The quarantine facility removes and isolates suspicious files into a safe location before analyzing them for possible infection. Any files transferred in this fashion are encrypted- meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC. If a file cannot be disinfected, then it provides a reliable safe-house until the virus database is updated- neutralizing the impact of any new virus.

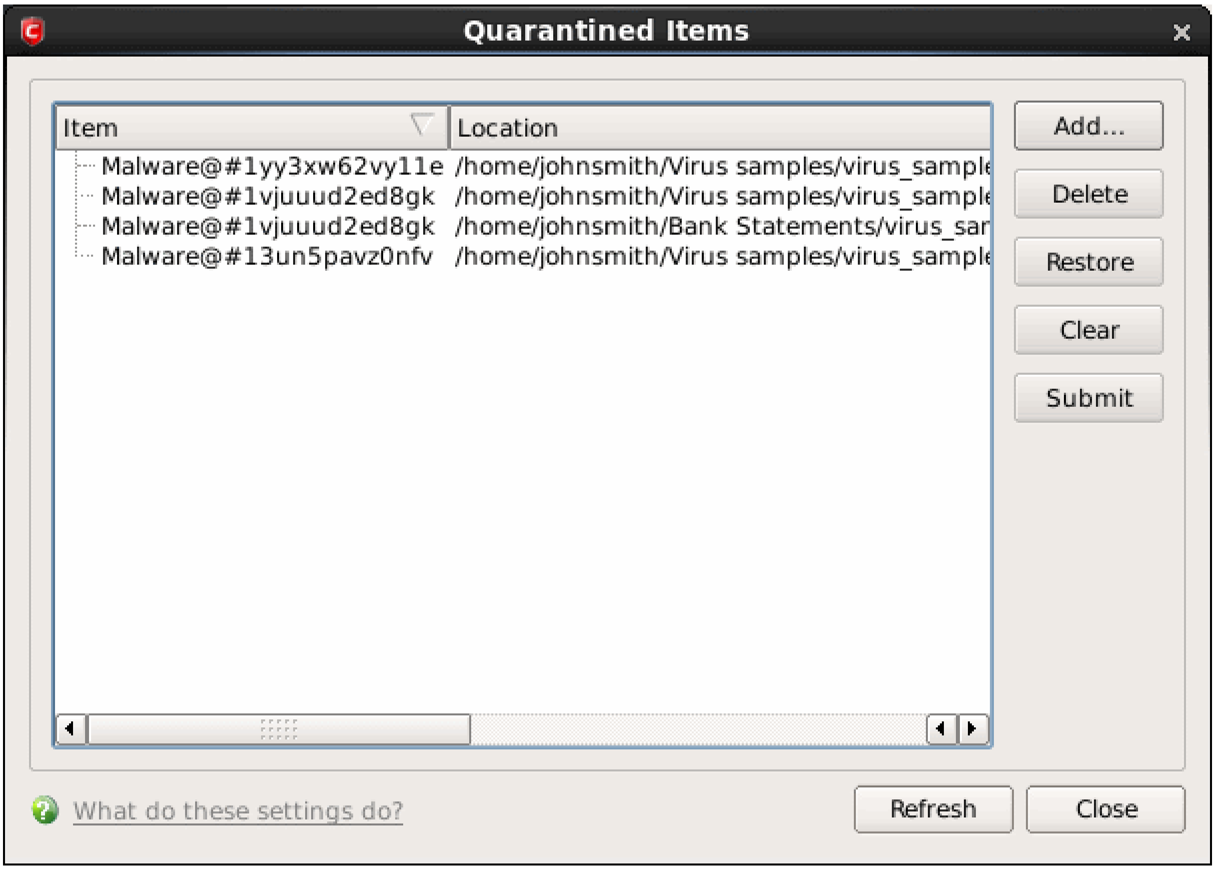
For adding executables to Quarantined items, refer to **Antivirus Tasks > Run a Scan**. You can also:

- **Manually add applications, executables or other files, that you do not trust, as a Quarantined item**
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item**
- **Delete all quarantined items**
- **Submit selected quarantined items to Comodo for analysis**

To view the list of Quarantined Items

- Click 'Quarantined Items' from the main Antivirus Task Manager Screen.

The Quarantined Items will be displayed.



Item	Location
Malware@#1yy3xw62vy11e	/home/johnsmith/Virus samples/virus_sample
Malware@#1vjuuud2ed8gk	/home/johnsmith/Virus samples/virus_sample
Malware@#1vjuuud2ed8gk	/home/johnsmith/Bank Statements/virus_sar
Malware@#13un5pavz0nfv	/home/johnsmith/Virus samples/virus_sample

Column Description

- **Item** - Indicates which application or process propagated the event;
- **Location** - Indicates the location where the application or the file is stored;
- **Date/Time** - Indicates date and time, when the item is moved to quarantine.

Manually adding files as Quarantined Items

If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

- Click **Add** and select the file from **Open** dialog box.

To delete a quarantined item from the system

- Select the item and click **Delete**.

This deletes the file from the system permanently.

To restore a quarantined item to its original location

- Select the item and click **Restore**.

If the restored item does not contain a malware, it operates as usual. But if it contains a malware, it is detected as a threat immediately, if the Real Time Scanning is enabled or during the next scan.

To remove all the quarantined items permanently

- Click **Clear**.

This deletes all the quarantined items from the system permanently.

To submit selected quarantined items to Comodo for analysis

- Select the item from the list and click **Submit**.

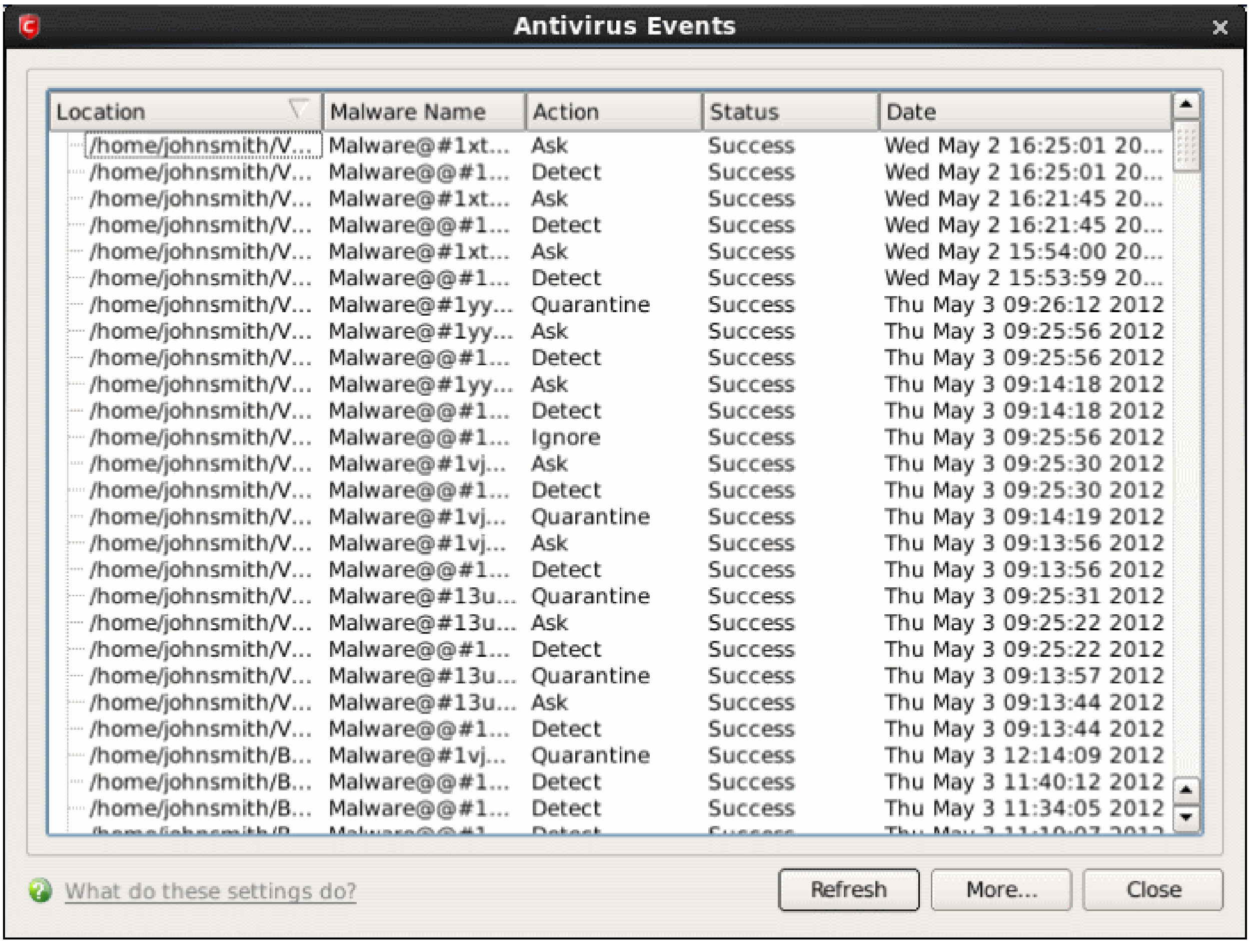
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.4. View Antivirus Events

Comodo Antivirus documents the results of all actions performed by it in extensive but easy to understand reports. A detailed scan report contains statistics of all scanned objects, settings used for each task and the history of actions performed on each individual file. Reports are also generated during real-time protection, and after updating the anti-virus database and application modules.

To view a log of Antivirus Events

- Click 'View Antivirus Events' from the main Antivirus Task Manager Screen.



Location	Malware Name	Action	Status	Date
/home/johnsmith/V...	Malware@#1xt...	Ask	Success	Wed May 2 16:25:01 20...
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Wed May 2 16:25:01 20...
/home/johnsmith/V...	Malware@#1xt...	Ask	Success	Wed May 2 16:21:45 20...
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Wed May 2 16:21:45 20...
/home/johnsmith/V...	Malware@#1xt...	Ask	Success	Wed May 2 15:54:00 20...
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Wed May 2 15:53:59 20...
/home/johnsmith/V...	Malware@#1yy...	Quarantine	Success	Thu May 3 09:26:12 2012
/home/johnsmith/V...	Malware@#1yy...	Ask	Success	Thu May 3 09:25:56 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:25:56 2012
/home/johnsmith/V...	Malware@#1yy...	Ask	Success	Thu May 3 09:14:18 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:14:18 2012
/home/johnsmith/V...	Malware@@#1...	Ignore	Success	Thu May 3 09:25:56 2012
/home/johnsmith/V...	Malware@#1vj...	Ask	Success	Thu May 3 09:25:30 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:25:30 2012
/home/johnsmith/V...	Malware@#1vj...	Quarantine	Success	Thu May 3 09:14:19 2012
/home/johnsmith/V...	Malware@#1vj...	Ask	Success	Thu May 3 09:13:56 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:13:56 2012
/home/johnsmith/V...	Malware@#13u...	Quarantine	Success	Thu May 3 09:25:31 2012
/home/johnsmith/V...	Malware@#13u...	Ask	Success	Thu May 3 09:25:22 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:25:22 2012
/home/johnsmith/V...	Malware@#13u...	Quarantine	Success	Thu May 3 09:13:57 2012
/home/johnsmith/V...	Malware@#13u...	Ask	Success	Thu May 3 09:13:44 2012
/home/johnsmith/V...	Malware@@#1...	Detect	Success	Thu May 3 09:13:44 2012
/home/johnsmith/B...	Malware@#1vj...	Quarantine	Success	Thu May 3 12:14:09 2012
/home/johnsmith/B...	Malware@@#1...	Detect	Success	Thu May 3 11:40:12 2012
/home/johnsmith/B...	Malware@@#1...	Detect	Success	Thu May 3 11:34:05 2012
/home/johnsmith/B...	Malware@@#1...	Detect	Success	Thu May 3 11:10:07 2012

Column Description

- **Location** - Indicates the location where the application detected with a threat is stored.
- **Malware Name** - Name of the malware event that has been detected.
- **Action** - Indicates action taken against the malware through Antivirus.
- **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.
- **Date** - Indicates the date of the event.

Sorting the Entries

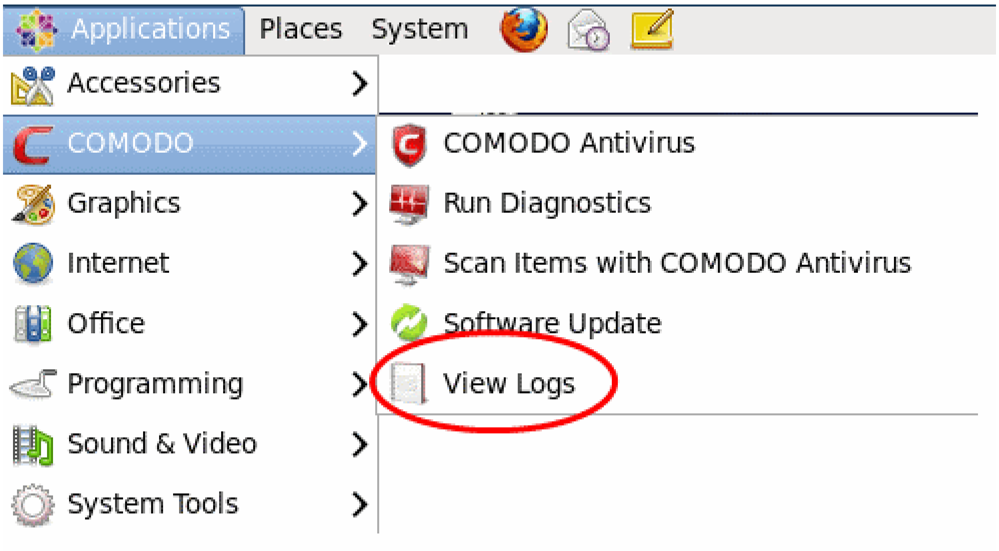
- Click on any column header to sort the entries alphabetically, ascending or descending order as the case may be.

Comodo Antivirus Log Viewer Module

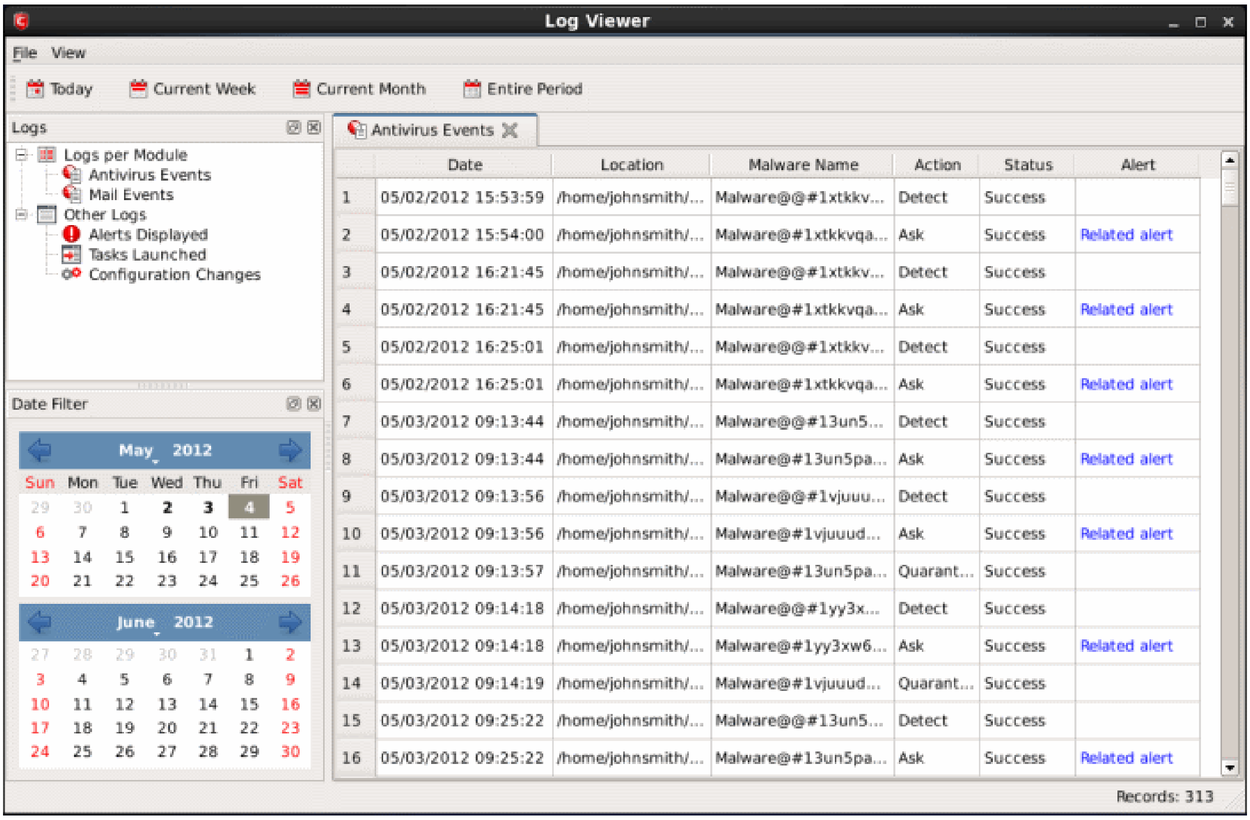
- Click 'More ...' to load the full Comodo Antivirus Log Viewer module.

OR

- Click 'View Logs' in the Applications menu in the panel to load the full Log Viewer module.



This window contains a full history of logged events in two categories: Logs per Module and Other Logs.
It also allows you to build custom log files based on **specific filters** and to **export log files** for archiving or troubleshooting purposes.



	Date	Location	Malware Name	Action	Status	Alert
1	05/02/2012 15:53:59	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
2	05/02/2012 15:54:00	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
3	05/02/2012 16:21:45	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
4	05/02/2012 16:21:45	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
5	05/02/2012 16:25:01	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
6	05/02/2012 16:25:01	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
7	05/03/2012 09:13:44	/home/johnsmith/...	Malware@@#13un5...	Detect	Success	
8	05/03/2012 09:13:44	/home/johnsmith/...	Malware@#13un5pa...	Ask	Success	Related alert
9	05/03/2012 09:13:56	/home/johnsmith/...	Malware@@#1vjuuu...	Detect	Success	
10	05/03/2012 09:13:56	/home/johnsmith/...	Malware@#1vjuuud...	Ask	Success	Related alert
11	05/03/2012 09:13:57	/home/johnsmith/...	Malware@#13un5pa...	Quarant...	Success	
12	05/03/2012 09:14:18	/home/johnsmith/...	Malware@@#1yy3x...	Detect	Success	
13	05/03/2012 09:14:18	/home/johnsmith/...	Malware@#1yy3xw6...	Ask	Success	Related alert
14	05/03/2012 09:14:19	/home/johnsmith/...	Malware@#1vjuuud...	Quarant...	Success	
15	05/03/2012 09:25:22	/home/johnsmith/...	Malware@@#13un5...	Detect	Success	
16	05/03/2012 09:25:22	/home/johnsmith/...	Malware@#13un5pa...	Ask	Success	Related alert

Records: 313

The Log Viewer Module is divided into three sections. The top panel displays a set of handy, predefined time **Filters**. The left panel the types of Logs. The right hand side panel displays the actual events that were logged for the time period you selected in the top panel and the type of log selected in the left panel (or the events that correspond to the filtering criteria you selected).

The Logs per Module option contains the logged events of Antivirus modules and Other Logs options contains logged events of the following:

- **Alerts Displayed:** Displays the list of various alerts that were displayed to the user, the response given by the user to those alerts and other related details of the alert.
- **Tasks Launched:** Displays the various Antivirus tasks such as updates and scans that have taken place. This area will contain a log of all on-demand and scheduled AV scans and the result of that scan.
- **Configuration Changes:** Displays a log of all configuration changes made by the user in the CAVL application.

Filtering Log Files

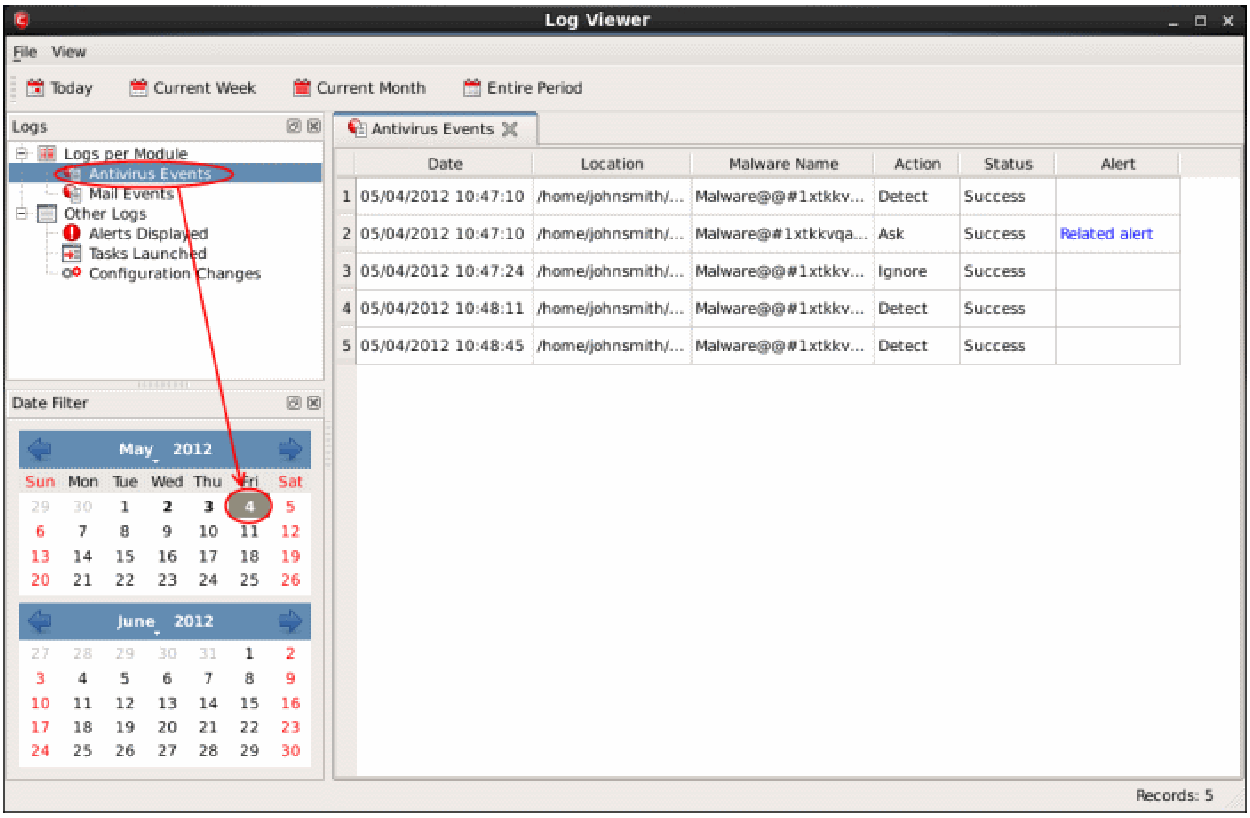
Comodo Antivirus allows you to create custom views of all logged events according to user defined criteria.

Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. (The current week is calculated from Monday to Sunday that holds the current date.)
- **Current Month -** Displays all logged events during the month that holds the current date.
- **Entire Period -** Displays every event logged since CAVL was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).

The example below shows an example display when the Antivirus Events for 'Today' are displayed.



	Date	Location	Malware Name	Action	Status	Alert
1	05/04/2012 10:47:10	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
2	05/04/2012 10:47:10	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
3	05/04/2012 10:47:24	/home/johnsmith/...	Malware@@#1xtkkv...	Ignore	Success	
4	05/04/2012 10:48:11	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
5	05/04/2012 10:48:45	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	

May 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
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

June 2012

27	28	29	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

Note: The type of events logged by the Antivirus modules of CAVL differ from each other. This means that the information and the columns displayed in the right hand side panel change depending on which type of log you have selected in the top and left hand side panel. For more details on the data shown in the columns, see **View Mail Events**.

User Defined Filters:

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. The type of filters available for Antivirus logs differ to those available for Mail logs. The table below provides a summary of available filters and their meanings:

Available Filters - Logs per Module	
Antivirus Filter	**Mail Filters**
Action - Displays events according to the response (or action taken) by the Antivirus	**Sender** - Displays events according to the name of the sender
Location - Displays only the events logged from a specific location	**Subject -** Displays only the events according to the subject in the mail
Malware Name - Displays only the events logged corresponding to a specific malware	**From IP** - Displays only the events with a specific From IP address
Status - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'	**Location** - Displays only the events logged from a specific location
	Type - Displays only the events logged corresponding to specific type of mailware in the mail
	Malware Name - Displays only the events logged corresponding to a specific malware
	Spam - Displays only the events logged corresponding to a specific spam mail
	Action - Displays events according to the response (or action taken) by CAVL
	Status - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

Creating Custom Filters

Custom Filters can be created through the Advanced Filter Interface. You can open the Advanced Filter interface either by using the View option in the menu bar or using the context sensitive menu.

- Click View > Advanced Filter to open the 'Advanced Filter' configuration area.

  Or

- Right click on any event and select 'Advanced Filter' option to open the corresponding configuration area.

The 'Advanced Filter' configuration area is displayed in the top half of the interface whilst the lower half displays the Events, Alerts, Tasks or Configuration Changes that the user has selected from the upper left pane. If you wish to view and filter event logs for other modules then simply click log name in the tree on the upper left hand pane.

The Advanced Log filter displays different fields and options depending on the log type chosen from the left hand pane (Antivirus, Mail).

This section will deal with Advanced Event Filters related to 'Antivirus Events' and will also cover the custom filtering that can be applied to the 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes'). The Mail Advanced Event Filters is dealt in the respective section.

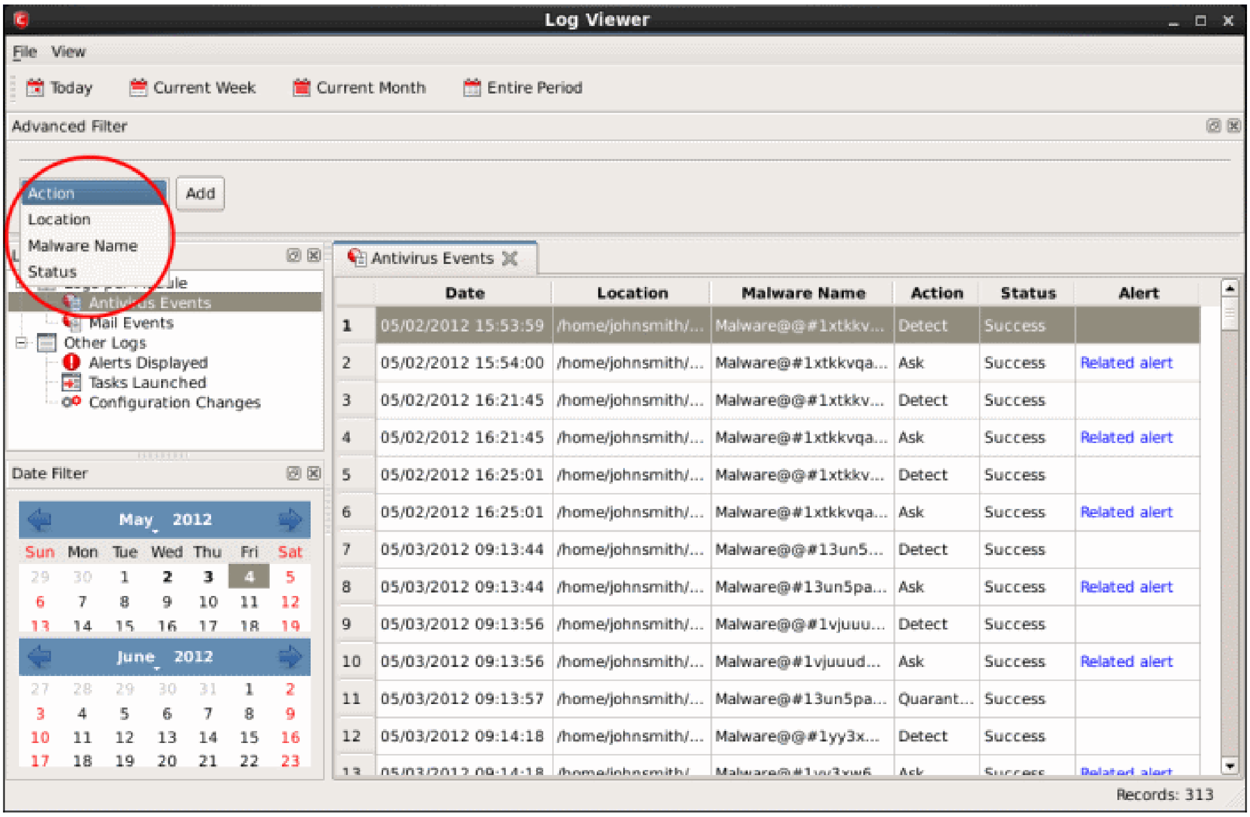
Antivirus Events - Advanced Filters

To configure Advanced Filters for Antivirus events

1. Select 'View > Advanced Filter'
2. Select 'Antivirus Events' under 'Logs Per Module'

You have 4 categories of filter that 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.

3. Click the 'Add' button when you have chosen the category upon which you wish to filter.

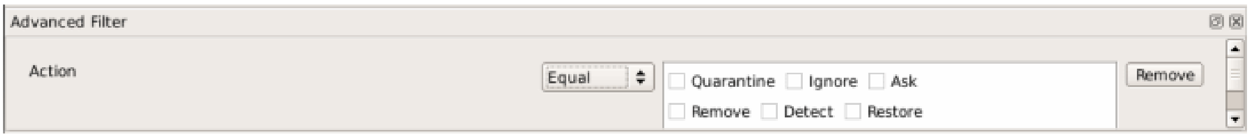


	Date	Location	Malware Name	Action	Status	Alert
1	05/02/2012 15:53:59	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
2	05/02/2012 15:54:00	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
3	05/02/2012 16:21:45	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
4	05/02/2012 16:21:45	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
5	05/02/2012 16:25:01	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
6	05/02/2012 16:25:01	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
7	05/03/2012 09:13:44	/home/johnsmith/...	Malware@@#13un5...	Detect	Success	
8	05/03/2012 09:13:44	/home/johnsmith/...	Malware@#13un5pa...	Ask	Success	Related alert
9	05/03/2012 09:13:56	/home/johnsmith/...	Malware@@#1vjuuu...	Detect	Success	
10	05/03/2012 09:13:56	/home/johnsmith/...	Malware@#1vjuuud...	Ask	Success	Related alert
11	05/03/2012 09:13:57	/home/johnsmith/...	Malware@#13un5pa...	Quarant...	Success	
12	05/03/2012 09:14:18	/home/johnsmith/...	Malware@@#1yy3x...	Detect	Success	
13	05/03/2012 09:14:18	/home/johnsmith/	Malware@#1yy3xw6	Ask	Success	Related alert

Records: 313

Following are the options available in the 'Add' drop-down:

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



□ Quarantine □ Ignore □ Ask
□ Remove □ Detect □ Restore

a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

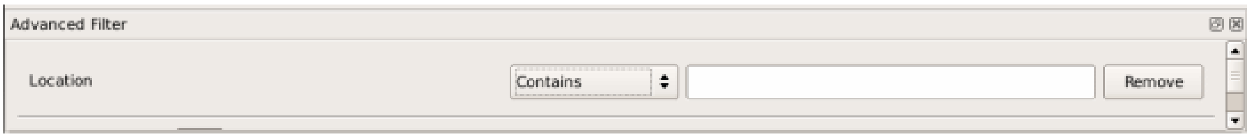
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- **Quarantine:** Displays events where the user chose to quarantine a file
- **Remove:** Displays events where the user chose to delete an item
- **Ignore:** Displays events where the user chose to ignore an item
- **Detect:** Displays events for detection of a malware
- **Ask**: Displays events when user was asked by alert concerning some Antivirus event
- **Restore:** Displays events of the applications that were quarantined and restored.

The filtered entries are shown directly underneath.

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.

ii. **Location:** Selecting the 'Location' option displays a drop-down field and text entry field.



Advanced Filter

Location: Contains

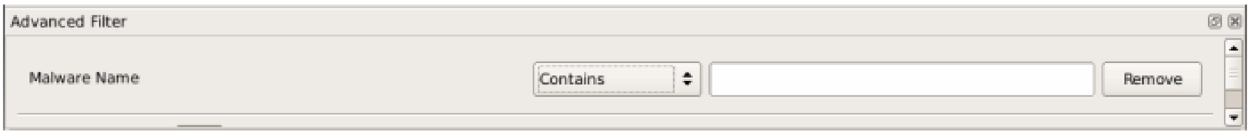
a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

For example, if you select 'Contains' option from the drop-down field and enter the word 'unclassifiedMalware' in the text field, then all events containing the word 'unclassifiedMalware' in the Location field will be displayed directly underneath. If you select 'Does Not Contain' option from the drop-down field and enter the word 'System' in the text field, then all events that do not have the word 'System' will be displayed directly underneath.

iii. **Malware Name:** Selecting the 'Malware' option displays a drop-down field and text entry field.



Advanced Filter

Malware Name: Contains

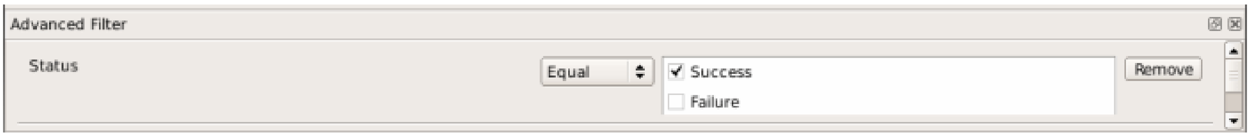
a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Location' option for better understanding.

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



Advanced Filter

Status: Equal

☑ Success

□ Failure

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 that successfully executed (for example, the database was successfully updated)
- **Failure:** Displays Events that failed to execute (for example, the database failure to update correctly)

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Action' option for better understanding.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, the option to select the next filter type automatically appears. You can also remove a filter type by clicking the 'Remove' option at the end of every filter option.

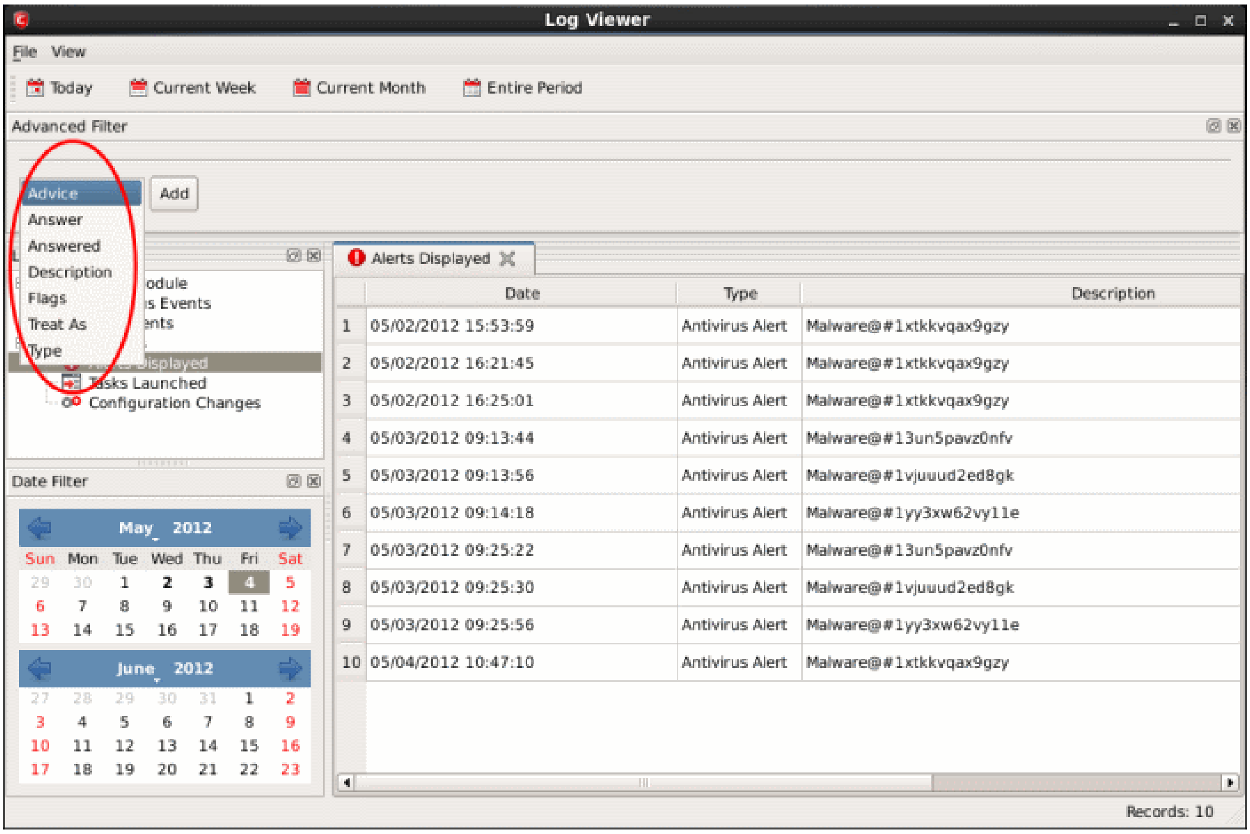
Other Logs - Advanced Filters

The Advanced Filter function for Alerts Displayed, Tasks Launched and Configuration Changes are the same in Antivirus and Mail interfaces.

To configure Advanced Filters for Alerts Displayed

1. Select 'View > Advanced Filter'.
2. Under 'Other Logs', select 'Alerts Displayed'.

   This will open the Advanced Filter pane above the other two panes . From here, you can chose the category of filter from a drop-down box. 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.
3. Click 'Add' when you have chosen the category upon which you wish to filter.



	Date	Type	Description
1	05/02/2012 15:53:59	Antivirus Alert	Malware@#1xtkkvqax9gzy
2	05/02/2012 16:21:45	Antivirus Alert	Malware@#1xtkkvqax9gzy
3	05/02/2012 16:25:01	Antivirus Alert	Malware@#1xtkkvqax9gzy
4	05/03/2012 09:13:44	Antivirus Alert	Malware@#13un5pavz0nfv
5	05/03/2012 09:13:56	Antivirus Alert	Malware@#1vjuuud2ed8gk
6	05/03/2012 09:14:18	Antivirus Alert	Malware@#1yy3xw62vy11e
7	05/03/2012 09:25:22	Antivirus Alert	Malware@#13un5pavz0nfv
8	05/03/2012 09:25:30	Antivirus Alert	Malware@#1vjuuud2ed8gk
9	05/03/2012 09:25:56	Antivirus Alert	Malware@#1yy3xw62vy11e
10	05/04/2012 10:47:10	Antivirus Alert	Malware@#1xtkkvqax9gzy

The following table lists the various filter categories and parameters for 'Alerts Displayed'.

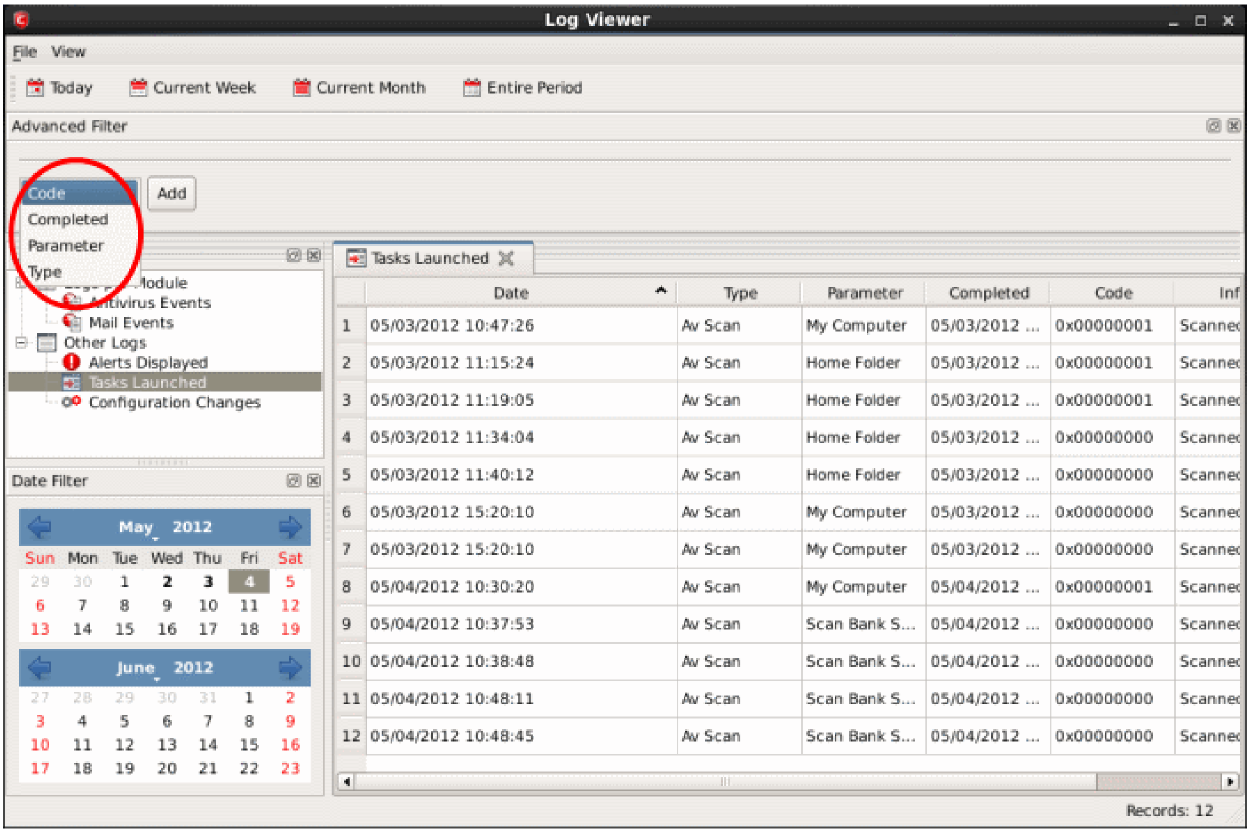
Available Filters - Other Logs - Alerts Displayed	
Filter Option	**Description**
Type	Displays the type of alert. It can be a Mail or Antivirus alert
Description	Displays the name of the event
Advice	Suggests an advice that can be executed by the user for that event
Answered	Displays the date and time on which the alert was answered
Flags	Filters the events based on the flags set for them.
Answer	Displays the answer that was given by you for the alert
Treat As	Displays the type of policy, if any, for the corresponding event type

To configure Advanced Filters for Tasks Launched

1. Select 'View > Advanced Filter'.
2. Under 'Other Logs', select 'Tasks Launched'.

   This will open the Advanced Filter pane above the other two panes. From here, you can chose the category of filter from a drop-down box. 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.

3. Click 'Add' when you have chosen the category upon which you wish to filter.



	Date	Type	Parameter	Completed	Code	Inf
1	05/03/2012 10:47:26	Av Scan	My Computer	05/03/2012 ...	0x00000001	Scannec
2	05/03/2012 11:15:24	Av Scan	Home Folder	05/03/2012 ...	0x00000001	Scannec
3	05/03/2012 11:19:05	Av Scan	Home Folder	05/03/2012 ...	0x00000001	Scannec
4	05/03/2012 11:34:04	Av Scan	Home Folder	05/03/2012 ...	0x00000000	Scannec
5	05/03/2012 11:40:12	Av Scan	Home Folder	05/03/2012 ...	0x00000000	Scannec
6	05/03/2012 15:20:10	Av Scan	My Computer	05/03/2012 ...	0x00000000	Scannec
7	05/03/2012 15:20:10	Av Scan	My Computer	05/03/2012 ...	0x00000000	Scannec
8	05/04/2012 10:30:20	Av Scan	My Computer	05/04/2012 ...	0x00000001	Scannec
9	05/04/2012 10:37:53	Av Scan	Scan Bank S...	05/04/2012 ...	0x00000000	Scannec
10	05/04/2012 10:38:48	Av Scan	Scan Bank S...	05/04/2012 ...	0x00000000	Scannec
11	05/04/2012 10:48:11	Av Scan	Scan Bank S...	05/04/2012 ...	0x00000000	Scannec
12	05/04/2012 10:48:45	Av Scan	Scan Bank S...	05/04/2012 ...	0x00000000	Scannec

Records: 12

The following table lists the various filter categories and parameters for 'Tasks Launched'.

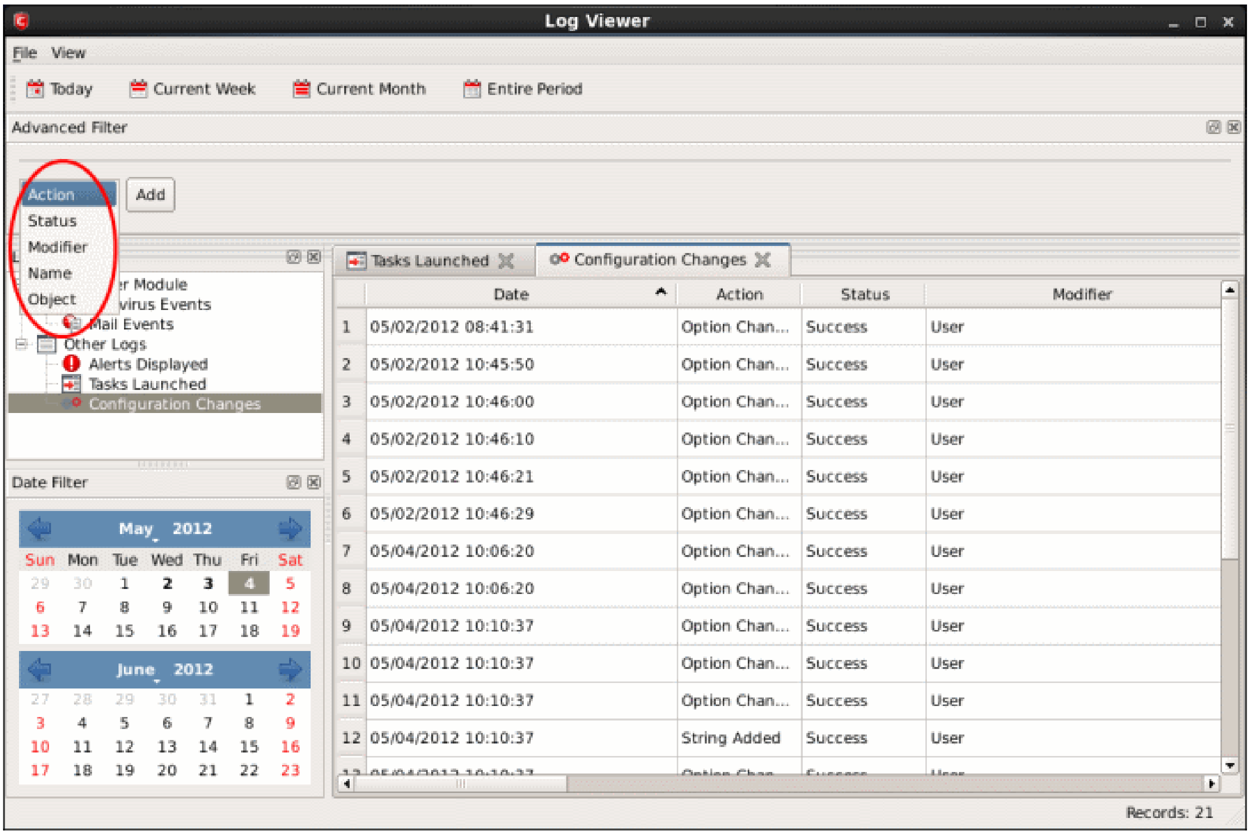
Available Filters - Other Logs - Tasks Launched	
Filter Option	**Description**
Type	Displays the type of task. It can be an antivirus update or scan type.
Parameter	Displays the name of the scan profile. This column is populated only if 'Av Scan' option is displayed in 'Type' column.
Completed	Displays the date and time at which the task was executed.
Code	Displays a code value if the task was not performed successfully and for task updates it shows a standard value: 0x00000001 if base is up to date

To configure Advanced Filters for 'Configuration Changes'

1. Select 'View' > 'Advanced Filter'
2. Under 'Other Logs', select 'Configuration Changes'

   This will open the Advanced Filter pane above the other two panes. From here, you can chose the category of filter from a drop-down box. 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.

3. Click 'Add' when you have chosen the category upon which you wish to filter.



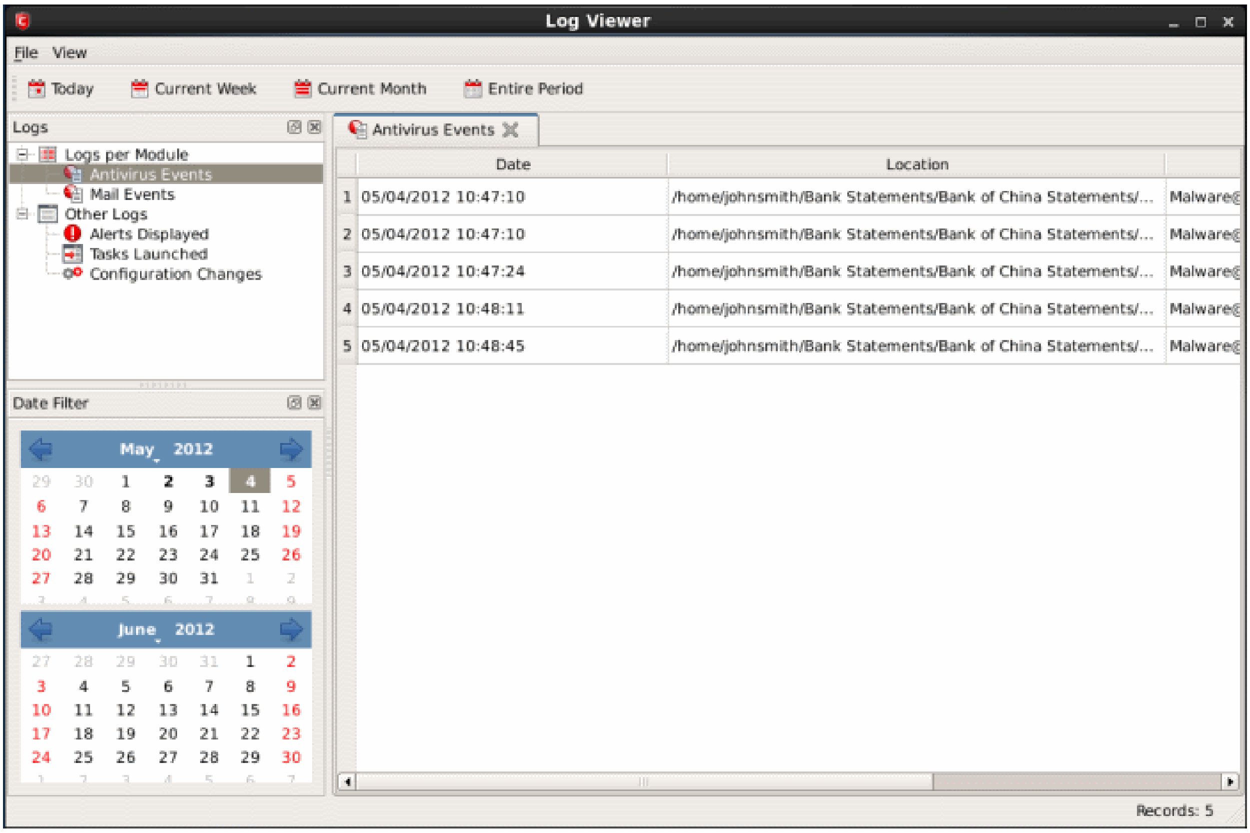
	Date	Action	Status	Modifier
1	05/02/2012 08:41:31	Option Chan...	Success	User
2	05/02/2012 10:45:50	Option Chan...	Success	User
3	05/02/2012 10:46:00	Option Chan...	Success	User
4	05/02/2012 10:46:10	Option Chan...	Success	User
5	05/02/2012 10:46:21	Option Chan...	Success	User
6	05/02/2012 10:46:29	Option Chan...	Success	User
7	05/04/2012 10:06:20	Option Chan...	Success	User
8	05/04/2012 10:06:20	Option Chan...	Success	User
9	05/04/2012 10:10:37	Option Chan...	Success	User
10	05/04/2012 10:10:37	Option Chan...	Success	User
11	05/04/2012 10:10:37	Option Chan...	Success	User
12	05/04/2012 10:10:37	String Added	Success	User

The following table lists the various filter categories and parameters for 'Configuration Changes'.

Available Filters - Other Logs - Configuration Changes	
Filter Option	**Description**
Action	Displays events according to the response (or action taken) by Antivirus.
Modifier	Displays events sorted based on whether the configuration was changed by the User or Antivirus alert.
Object	Displays the object for which the configuration change took place.
Name	Displays the name of the configuration entry, if it can be determined
Status	Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'.

Date Filter

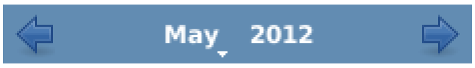
The Date Filter can be seen in the lower left hand pane. Using the Date Filter you can easily see the events on a particular date or on a date range.



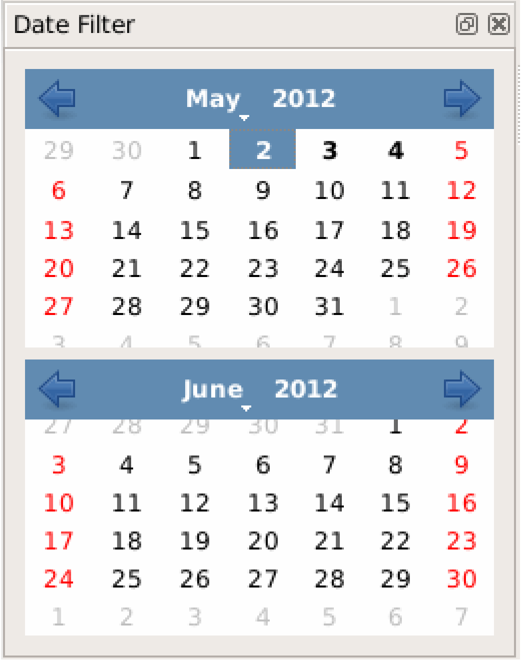
	Date	Location	
1	05/04/2012 10:47:10	/home/johnsmith/Bank Statements/Bank of China Statements/...	Malware@
2	05/04/2012 10:47:10	/home/johnsmith/Bank Statements/Bank of China Statements/...	Malware@
3	05/04/2012 10:47:24	/home/johnsmith/Bank Statements/Bank of China Statements/...	Malware@
4	05/04/2012 10:48:11	/home/johnsmith/Bank Statements/Bank of China Statements/...	Malware@
5	05/04/2012 10:48:45	/home/johnsmith/Bank Statements/Bank of China Statements/...	Malware@

To view the events on a particular date

1. Click the right arrow or the left arrow to select the required month and year. You can also select the month by clicking the down-arrow beside the month name and select from the list.



2. Now, click the required date. The events on that particular date is displayed.



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	30	31	1	2
3	4	5	6	7	8	9

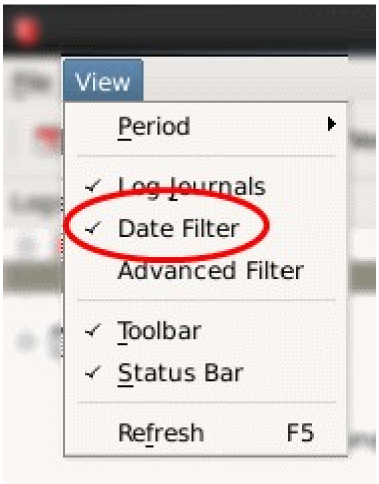
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

To close the Date Filter

- Click the 'X' symbol in Date Filter.

  Or

- Click 'View' in the menu bar and click the 'Date Filter' option. This is a toggle command and you can repeat this step to make the Date Filter appear.



Exporting Log Files to HTML

Exporting log files is useful for archiving and troubleshooting purposes. After making your choice and setting the filters. the log displayed can be directly exported as HTML file. There are two ways to export log files in the Log Viewer interface - using the context sensitive menu and via the 'File' menu option.

i. **File Menu**

1. Select the event for which the log report is to be taken.
2. Click 'Export' from the File menu.
3. Select the location where the log report has to be saved, provide a file name and click 'Save'.

ii. **Context Sensitive Menu**

1. Right click in the log display window to export the currently displayed log file to HTML.

You can export a custom view that you created using the available Filters by right clicking and selecting 'Export' from the context sensitive menu. Again, you are asked to provide a file name and save location for the file.

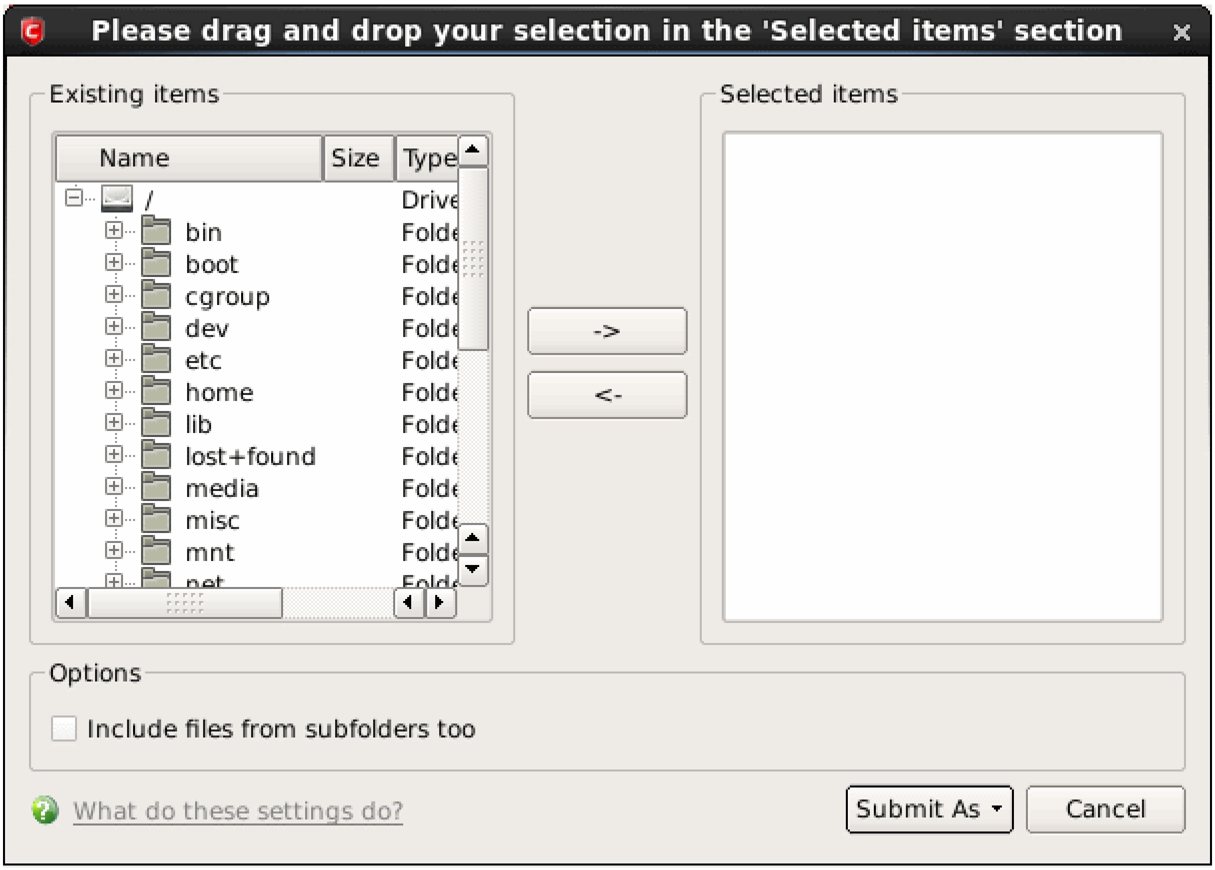
2.5. Submit Files to Comodo for Analysis

Files which are not in the Comodo safe list and are also unknown to the user can be submitted directly to Comodo for analysis and possible addition to the safe list.

You can submit the files which you suspect to be a malware or the files which you consider as safe but identified as malware by Comodo Antivirus (False Positives). The files are analyzed by experts in Comodo and added to white list or black list accordingly.

To submit files to Comodo

1. Click on the 'Submit Files' link from the main Antivirus Task Manager screen. The Browser dialog opens.


Please drag and drop your selection in the 'Selected items' section
Existing items
Name
Size
Type
/
Drive
bin
boot
cgroup
dev
etc
home
lib
lost+found
media
misc
mnt
net
Folde
Selected items
->
<-
Options
□ Include files from subfolders too
What do these settings do?
Submit As
Cancel

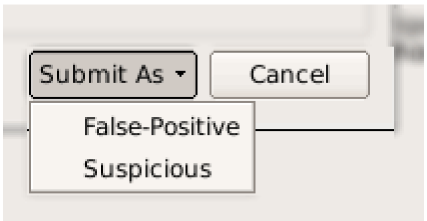
2. Select the items (files or folders) you wish to submit to Comodo for analysis from the left hand pane and move them to right hand pane by clicking the right arrow one by one. (If you want to revert a file, select the file from the right hand pane and click the left arrow).

3. Click 'Submit As' and select :

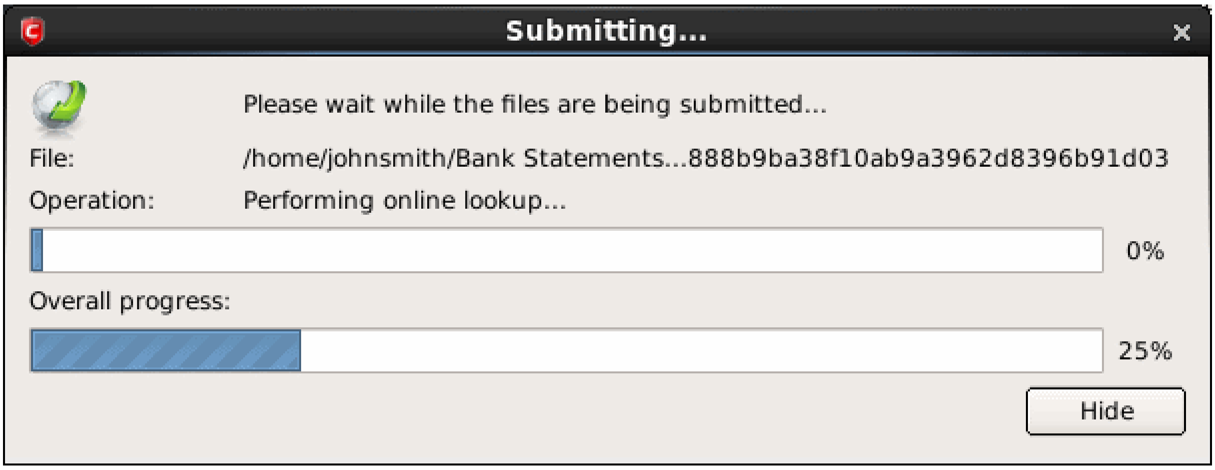
- 'False-Positive' for files you consider to be safe

  OR

- 'Suspicious' for files you suspect to be malware from the submit options.



Progress bars indicate the progress of the files submission to Comodo.

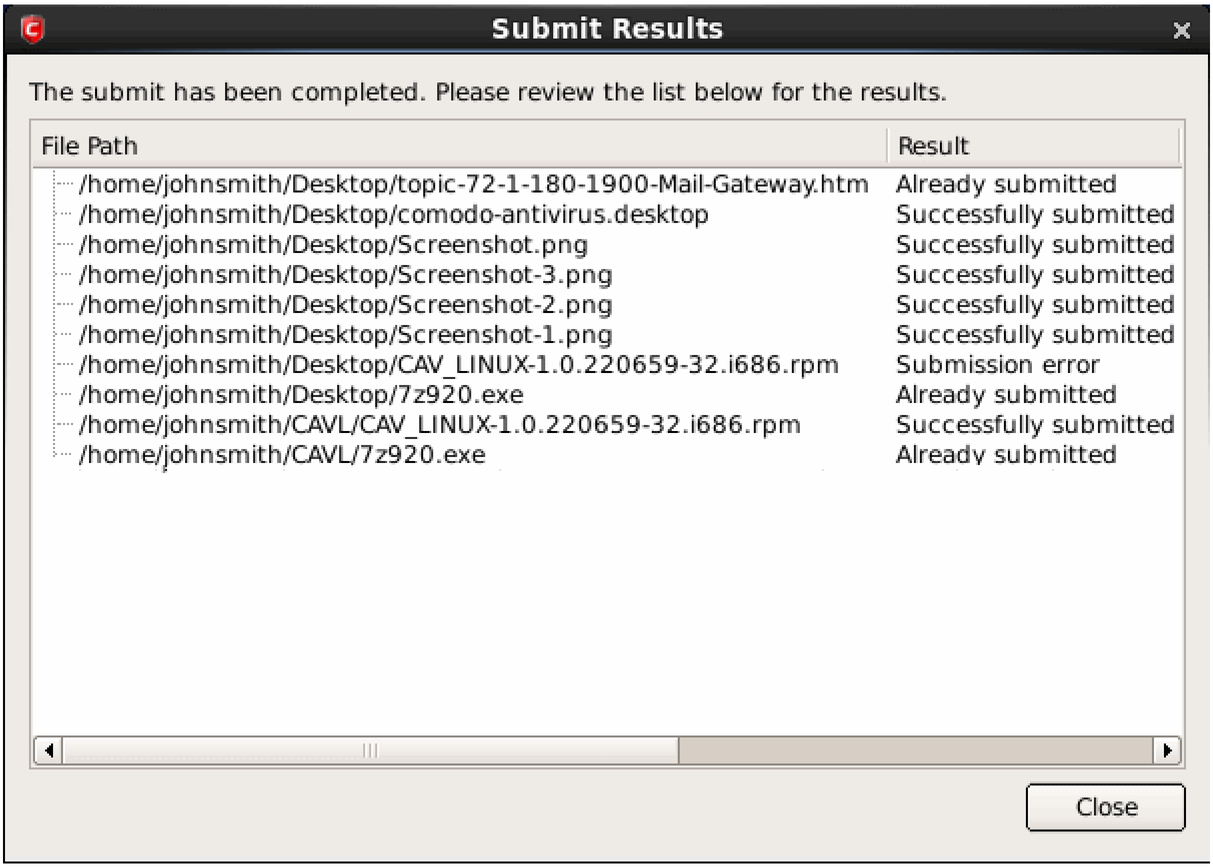


Please wait while the files are being submitted...

File: /home/johnsmith/Bank Statements...888b9ba38f10ab9a3962d8396b91d03

Operation: Performing online lookup...

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 displays these results:



The submit has been completed. Please review the list below for the results.

File Path	Result
/home/johnsmith/Desktop/topic-72-1-180-1900-Mail-Gateway.htm	Already submitted
/home/johnsmith/Desktop/comodo-antivirus.desktop	Successfully submitted
/home/johnsmith/Desktop/Screenshot.png	Successfully submitted
/home/johnsmith/Desktop/Screenshot-3.png	Successfully submitted
/home/johnsmith/Desktop/Screenshot-2.png	Successfully submitted
/home/johnsmith/Desktop/Screenshot-1.png	Successfully submitted
/home/johnsmith/Desktop/CAV_LINUX-1.0.220659-32.i686.rpm	Submission error
/home/johnsmith/Desktop/7z920.exe	Already submitted
/home/johnsmith/CAVL/CAV_LINUX-1.0.220659-32.i686.rpm	Successfully submitted
/home/johnsmith/CAVL/7z920.exe	Already submitted

- **Successfully submitted** - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- **Already submitted** - The file has already been submitted to our labs by another CAVL user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

2.6. Scheduled Scans

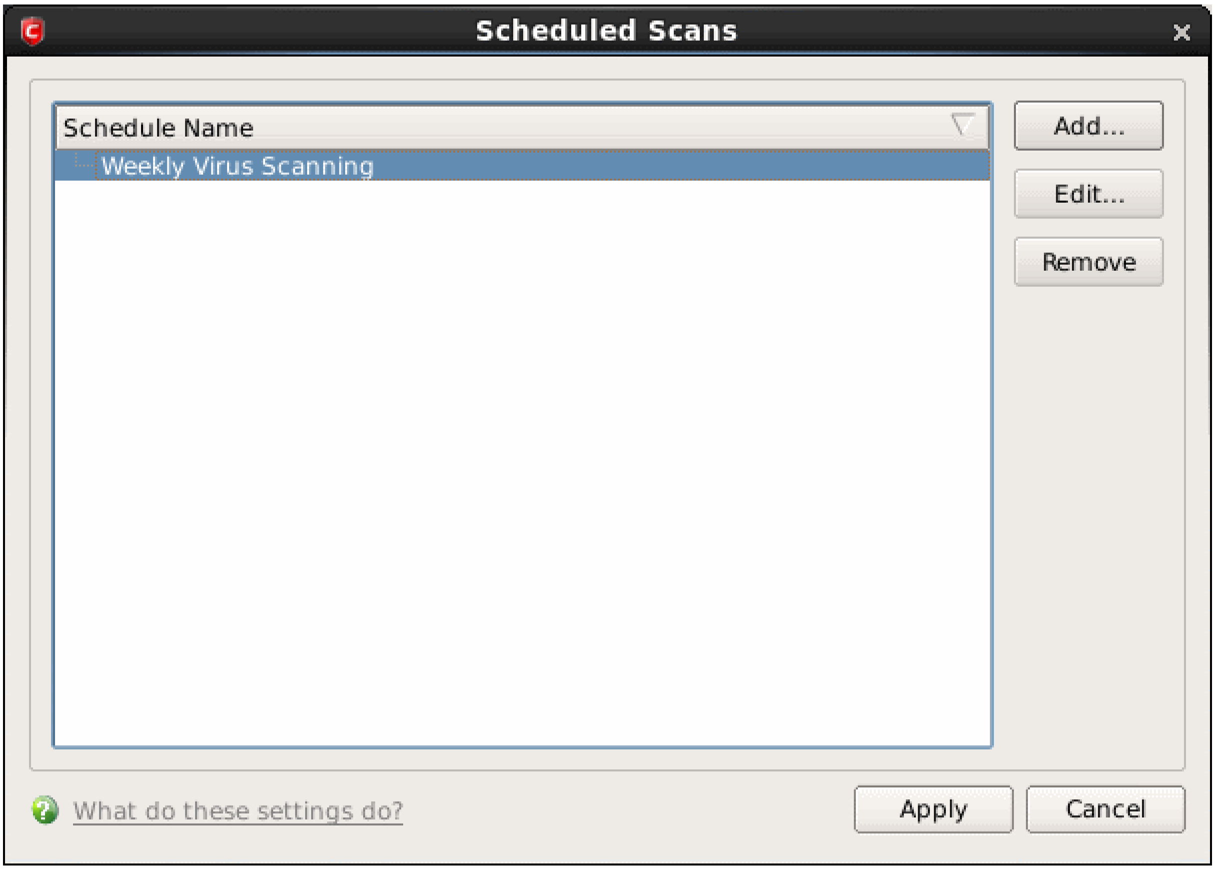
Comodo Antivirus features a highly customizable scheduler that lets you timetable scans according to your preferences. Comodo Antivirus automatically starts scanning the entire system or the disks or folders contained in the profile selected for that scan.

You can add an unlimited number of scheduled scans to run at a time that suits your preference. A scheduled scan may contain any profile of your choice.

You can choose to run scans at a certain time on a daily, weekly, monthly or custom interval basis. You can also choose which specific files, folders or drives are included in that scan.

Perhaps you wish to check your entire system first thing in the morning; maybe you prefer the middle of the night!! Comodo Antivirus gives you the power to choose, allowing you to get on with more important matters with complete peace of mind.

- To view the Scheduled Scans interface, click on the 'Scheduled Scans' link in the Antivirus Tasks interface.



Comodo Antivirus is shipped with a default schedule 'Weekly Virus Scanning to scan your computer on every Thursday at 3:20 pm . You can edit these schedule by selecting it and clicking the 'Edit' button.

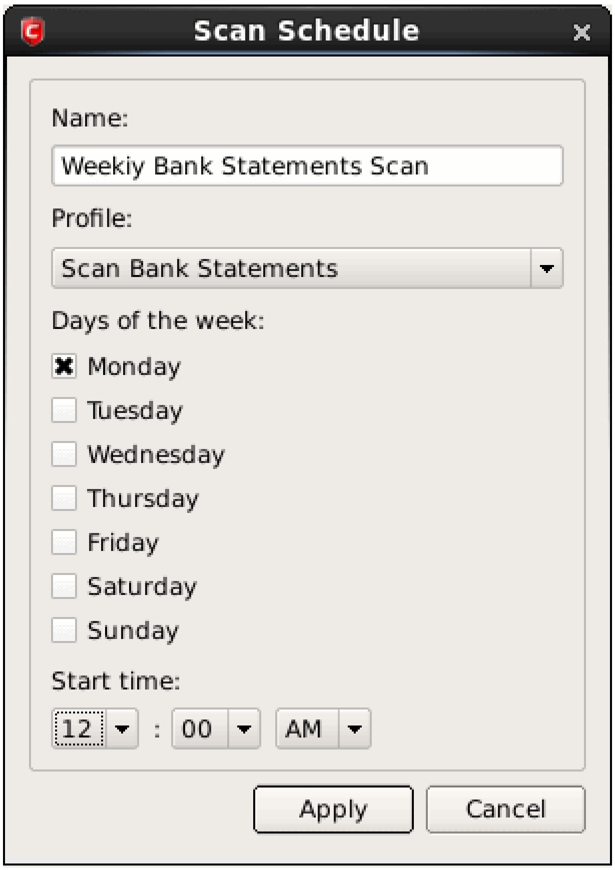
From the 'Scheduled Scans' panel, you can

- **Set a new scheduled scan**
- **Edit a pre-scheduled scan** and
- **Cancel a pre-scheduled scan**

The detection settings for the Scheduled Scans can be configured under the **Scheduled Scanning** tab of the **Scanner Settings** interface.

To add a new scan schedule

1. Click 'Add' from 'Scheduled Scans' interface. The 'Scan Schedule' panel will open.



Name:

Weekiy Bank Statements Scan

Profile:

Scan Bank Statements

Days of the week:

☒ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

Start time:

12 : 00 AM

2. Type a name for the newly scheduled scan in the 'Name' box.
3. Select a scanning profile from the list of preset scanning profiles by clicking at the drop-down arrow, in the 'Profile' box. (For more details on creating a custom Scan Profile that can be selected in a scheduled scan, see **Antivirus Tasks > Scan Profiles**.
4. Select the days of the week you wish to schedule the scanning from 'Days of the Week' check boxes.
5. Set the starting time for the scan in the selected days in the 'Start time' drop-down boxes.
6. Click 'Apply'.

Repeat the process to schedule more scans with different scan profiles.

To edit a Scheduled Scan

1. Select the schedule from the list.
2. Click 'Edit' in the 'Scheduled Scans' setting panel.
3. Edit the necessary fields in the 'Scan Schedule' panel.
4. Click 'Apply'.

To cancel a pre-scheduled scan

1. Select the Scan Schedule you wish to cancel in the 'Scheduled Scans' settings panel.
2. Click 'Remove'.

2.7. Scan Profiles

Creating a Scan Profile allows you to instruct Comodo Antivirus scan selected areas, folders or selected drives of your system. You will be asked to select a profile whenever you click the 'Scan Now' link on the Summary Screen.

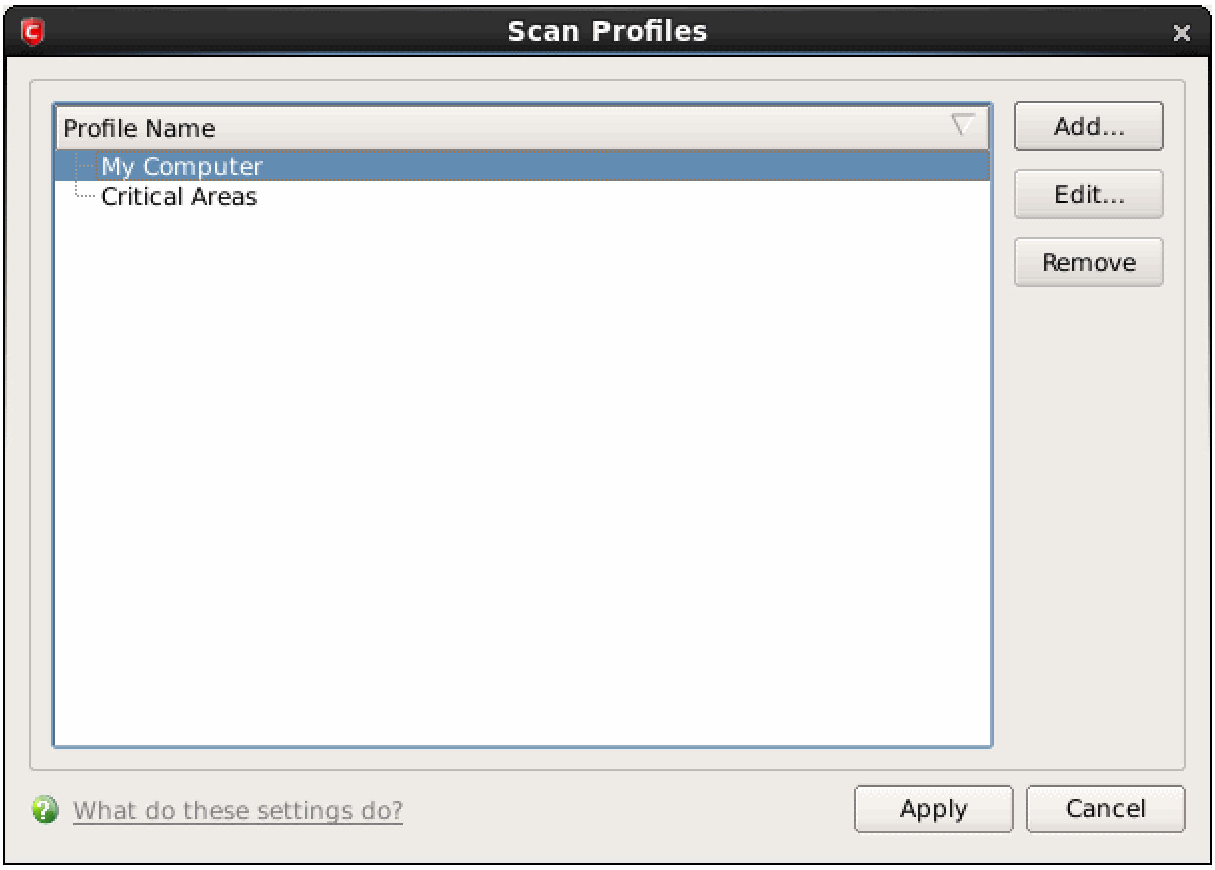
You can create custom scan profiles, to define selected disks or folders to be scanned and the created scan profile can be re-used for any desired scan event i.e. Run a Scan (On-Demand Scanning) and Scheduled Scans. You can create as many number of custom scan profiles as you wish according to the usage of your system. A Scan Profile allows you to scan only a selected area of your storage, saving time and resources.

- New scan profiles can be created by clicking the 'Create New Scan' button in the '**Run a Scan**' panel or by clicking the 'Add button' in the 'Scan Profiles' area.
- New scan profiles can then be referenced when creating a new '**Scheduled Scan**' and as the target of an on-demand scan in the '**Run a scan**' area.

Just to clarify, Antivirus scan profiles are purely concerned with the location of a scan, not the parameters of the scan. All scan profiles use the parameters as determined in the specific '**Scanner Settings**' tab of that type of scan.

To access the Scan Profiles interface

- Click 'Scan Profiles' from the main Antivirus Tasks interface.



Comodo Antivirus contains two default Scan Profiles 'My Computer' and 'Critical Areas'. These profiles are predefined and cannot be edited or removed.

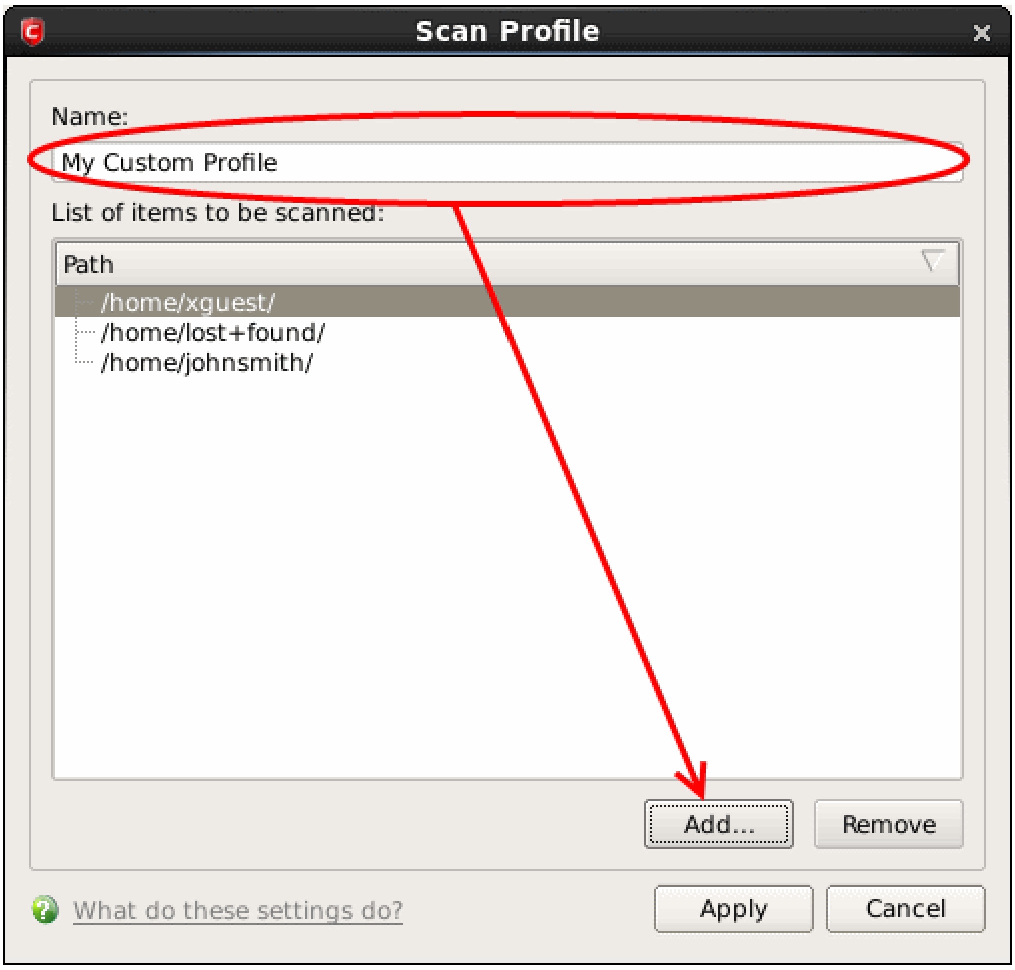
i. **My Computer *(Default)*** - When this profile is selected, Comodo Antivirus scans every local drive, folder and file on your system.

ii. **Critical Areas -** When this profile is selected, Comodo Antivirus runs a targeted scan of important operating system files and folders.

You can select any one of these Scan Profiles if you want to scan the respective areas.

To create a new scan profile from Scan Profiles option

1. Click 'Scan Profiles' from the main Antivirus Tasks interface.
2. Click 'Add'. The 'Scan Profile' dialog appears.
3. Type a name for the scan profile to be created in the 'Name' box and click 'Add'.



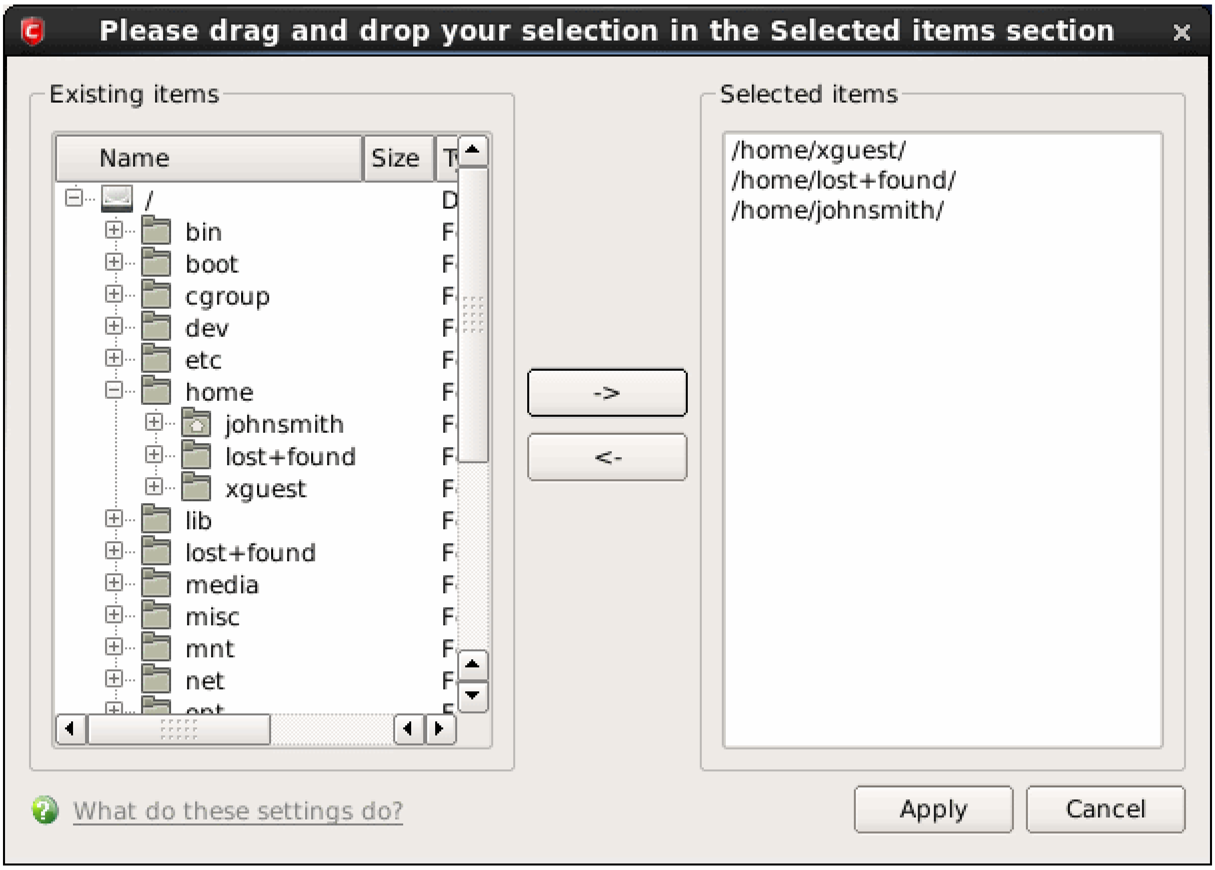
Name: My Custom Profile

List of items to be scanned:

/home/xguest/
/home/lost+found/
/home/johnsmith/

A configuration screen appears, prompting you to select the locations to be scanned when the newly created scan profile is selected. The left column displays all possible items (drives, folders and files) on your system for which scanning is available.

4. Browse to the folder location in the left column and select the folder.
5. Drag and drop all the files, folders and/or drives you require, into the right hand panel or select the files or folders and move them to right-hand pane by clicking the right arrow one by one. (If you want to revert a file, select the file from the left hand pane and click the left arrow).

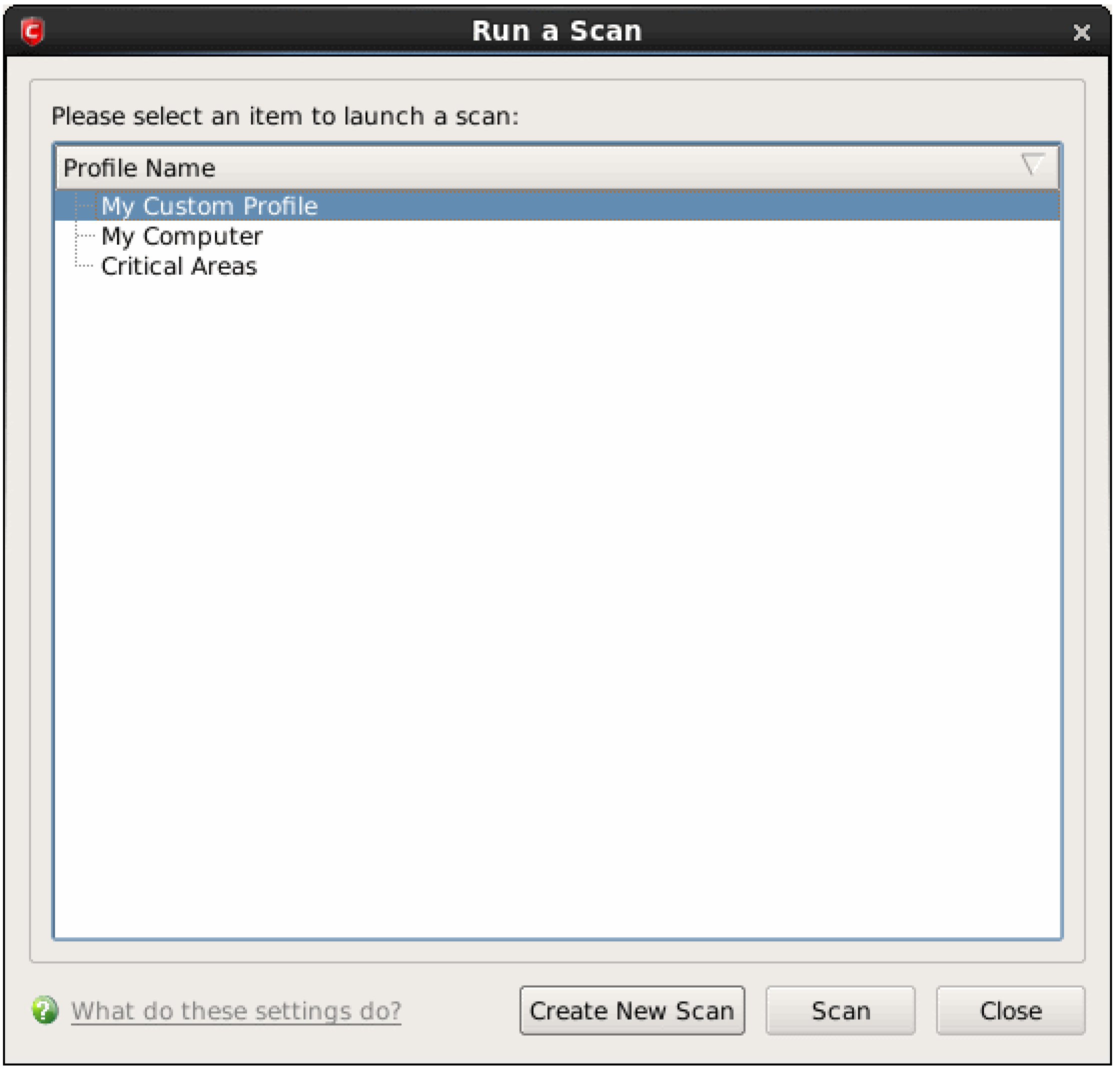


Selected items

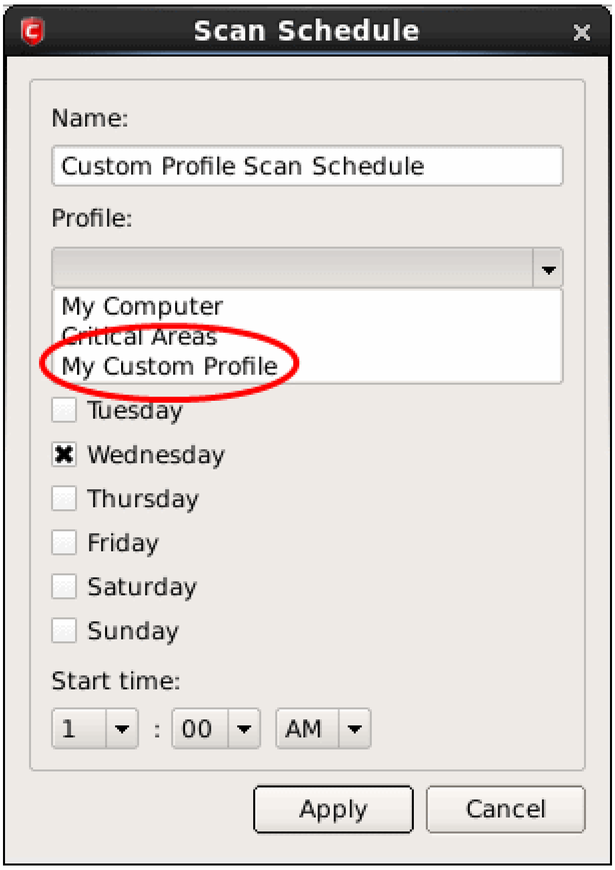
/home/xguest/
/home/lost+found/
/home/johnsmith/

6. Click 'Apply'.
7. Repeat the process to create more Scan Profiles.
8. Click 'Apply' in the Scan Profile interface for the created profiles to take effect.

You can see that the Scan Profile you have created, appearing as a target profile in the 'Run a Scan' panel**...**



...and is also available for selection during a scheduled scan in the drop-down.



Scan Schedule

Name: Custom Profile Scan Schedule

Profile:

My Computer
Critical Areas
My Custom Profile

☐ Tuesday
☒ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Start time: 1 : 00 AM

- To edit a Scan Profile, select the profile and click 'Edit'.
- To delete a Scan Profile, select the profile and click 'Remove'.

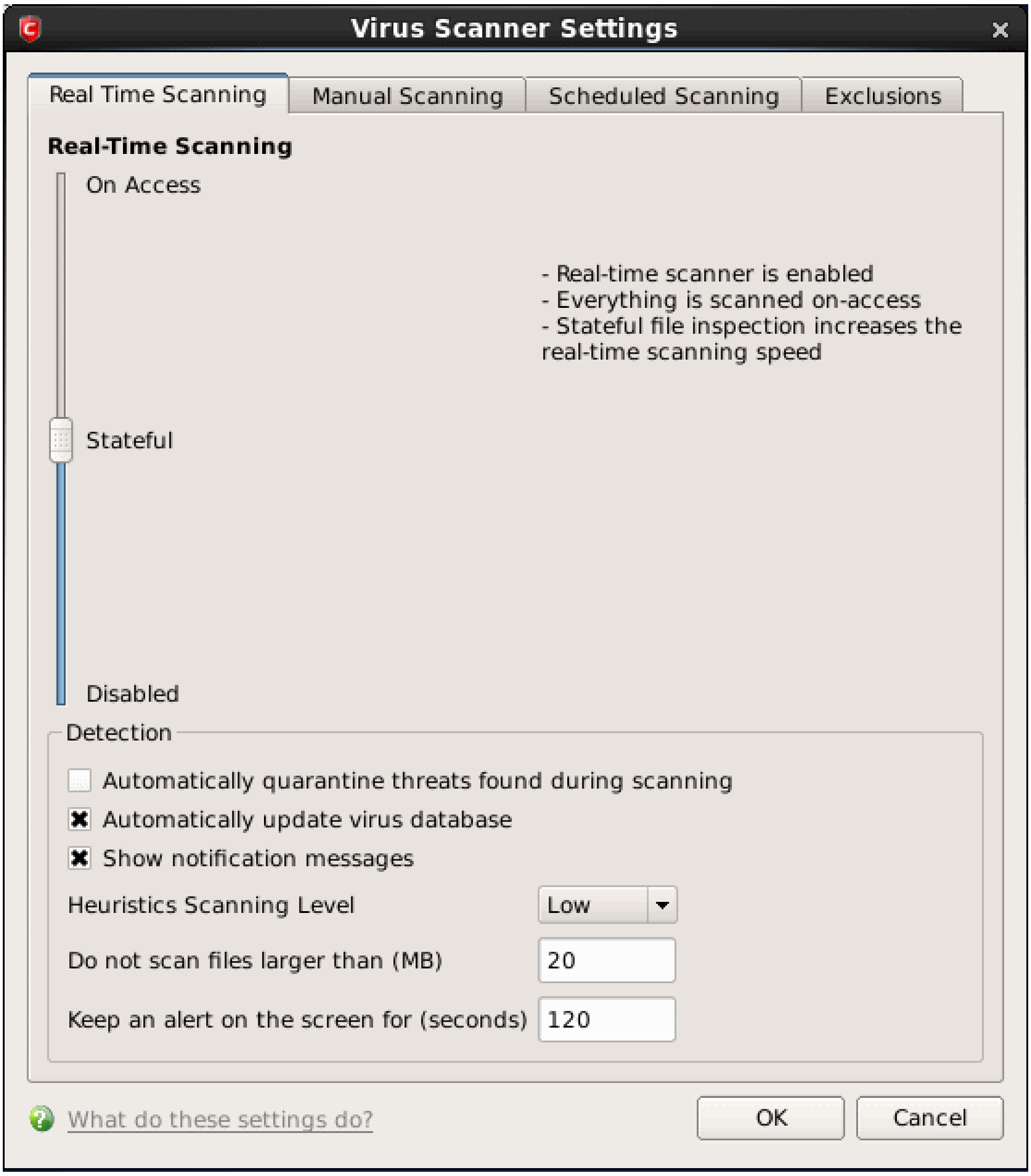
2.8. Scanner Settings

The Settings configuration panel allows you to customize various options related to Real Time Scanning (On-Access Scanning), Manual Scanning, Scheduled Scanning and Exclusions (a list containing the files you considered safe and ignored the alert during a virus scan).

- The settings made for each type of the scan applies to all future scans of that type.
- All items listed and all items added to the 'Exclusions' list is excluded from all future scans of all types.

To open Virus Scanner Settings panel

- Click on 'Scanner Settings' link in the Antivirus Tasks interface.



Real-Time Scanning

On Access
Stateful
Disabled

- Real-time scanner is enabled
- Everything is scanned on-access
- Stateful file inspection increases the real-time scanning speed

Detection

□ Automatically quarantine threats found during scanning

☒ Automatically update virus database

☒ Show notification messages

Heuristics Scanning Level: Low

Do not scan files larger than (MB): 20

Keep an alert on the screen for (seconds): 120

The options that can be configured using the settings panel are:

- **Real Time Scanning** - To set the parameters for on-access scanning;
- **Manual Scanning** - To set the parameters for manual Scanning (Run a Scan);
- **Scheduled Scanning** - To set the parameters for scheduled scanning;
- **Exclusions** - To see the list of ignored threats and to set the parameters for Exclusions.

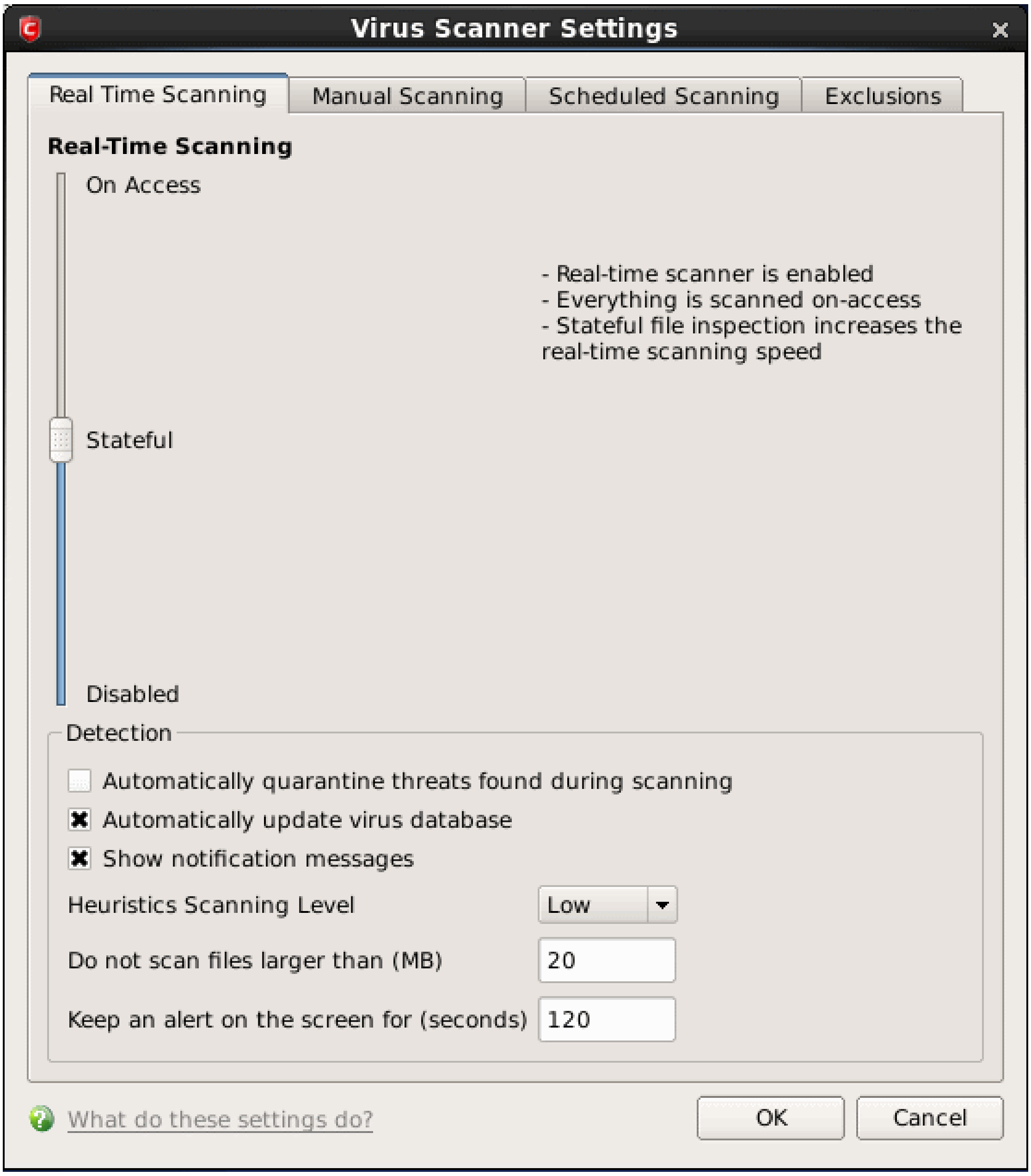
2.8.1. Real Time Scanning

The Real time Scanning (aka 'On-Access Scanning') is always ON and checks files in real time when they are created, opened or copied. (as soon as you interact with a file, Comodo Antivirus checks it). This instant detection of viruses assures you that your system is perpetually monitored for malware and enjoys the highest level of protection. You also have options to automatically remove the threats found during scanning and to update virus database before scanning. It is highly recommended that you keep the Real Time Scanner enabled to ensure your system remains continually free of infection.

The Real Time Scanning setting allows you to switch the On Access scanning between **Disabled**, **Stateful** and **On Access** and allows you to specify detection settings and other parameters that are deployed during on-access scans.

To set the Real Time Scanning level

- Click on the 'Real Time Scanning' tab in the 'Scanner Settings' panel.



Real-Time Scanning

On Access

- Real-time scanner is enabled
- Everything is scanned on-access
- Stateful file inspection increases the real-time scanning speed

Stateful

Disabled

Detection

☐ Automatically quarantine threats found during scanning

☒ Automatically update virus database

☒ Show notification messages

Heuristics Scanning Level: Low

Do not scan files larger than (MB): 20

Keep an alert on the screen for (seconds): 120

- Drag the real time Scanning slider to the required level. The choices available are **Disabled** (not recommended), **Stateful** *(default)* and **On Access**. The setting you choose here are also displayed in the Summary screen.
  - **On Access** - Provides the highest level of On Access Scanning and protection. Any file opened is scanned before it is run and the threats are detected before they get a chance to be executed.
  - **Stateful *(Default)*** **-** Comodo Antivirus is one of the most thorough and effective AV solutions available and it is also very fast. CAVL employs a feature called Stateful File Inspection for real time virus scanning to minimize the effects of on-access scanning on the system performance. Selecting the 'Stateful' option means CAVL scans only files that have not been scanned since the last virus update - greatly improving the speed, relevancy and effectiveness of the scanning.
  - **Disabled** - The Real time scanning is disabled. Antivirus does not perform any scanning and the threats cannot be detected before they impart any harm to the system.

Detection Settings

- **Automatically quarantine threats found during scanning** - When this check box is selected, the Antivirus moves the file detected to be containing the malware, to Quarantined Items. From the quarantined items the files can be restored or deleted at your will ***(Default = Disabled)***.

- **Automatically update virus database** - When this check box is selected, Comodo Antivirus checks for latest virus database updates from Comodo website and downloads the updates automatically, on system start-up and subsequently at regular intervals (***Default = Enabled).***

However, some people like to have control over what gets downloaded and when it gets downloaded Antivirus and program updates can sometimes be quite large (for example, 50 MB). If somebody has a slower connection (or tends to have many downloads going at the same time - movies, software etc.) then an automatic update for Comodo Antivirus can interfere with their other work. It can also slow down general web surfing - causing aggravation to the user. Furthermore, business users (or network administrators) may not wish to automatically download because it will take up to much bandwidth during the day. They may wish to download the updates in the evening. A user that deselect virus updates have to periodically select '**Update Virus Database**'.

- **Show notification messages** - Alerts are the pop-up notifications that appear in the lower right hand of the screen whenever the on-access scanner discovers a virus on your system. These alerts are a valuable source of real-time information that helps the user to immediately identify which particular files are infected or are causing problems. Disabling alerts does not affect the scanning process itself and Comodo Antivirus still continues to identify and deals with threats in the background. For more details on Antivirus alerts, **click here** ***(Default = Enabled).***

- **Heuristics Scanning Level** - Comodo AntiVirus employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

  - **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
  - **Low *(Default)*** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives**.** This setting combines an extremely high level of security and 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 the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

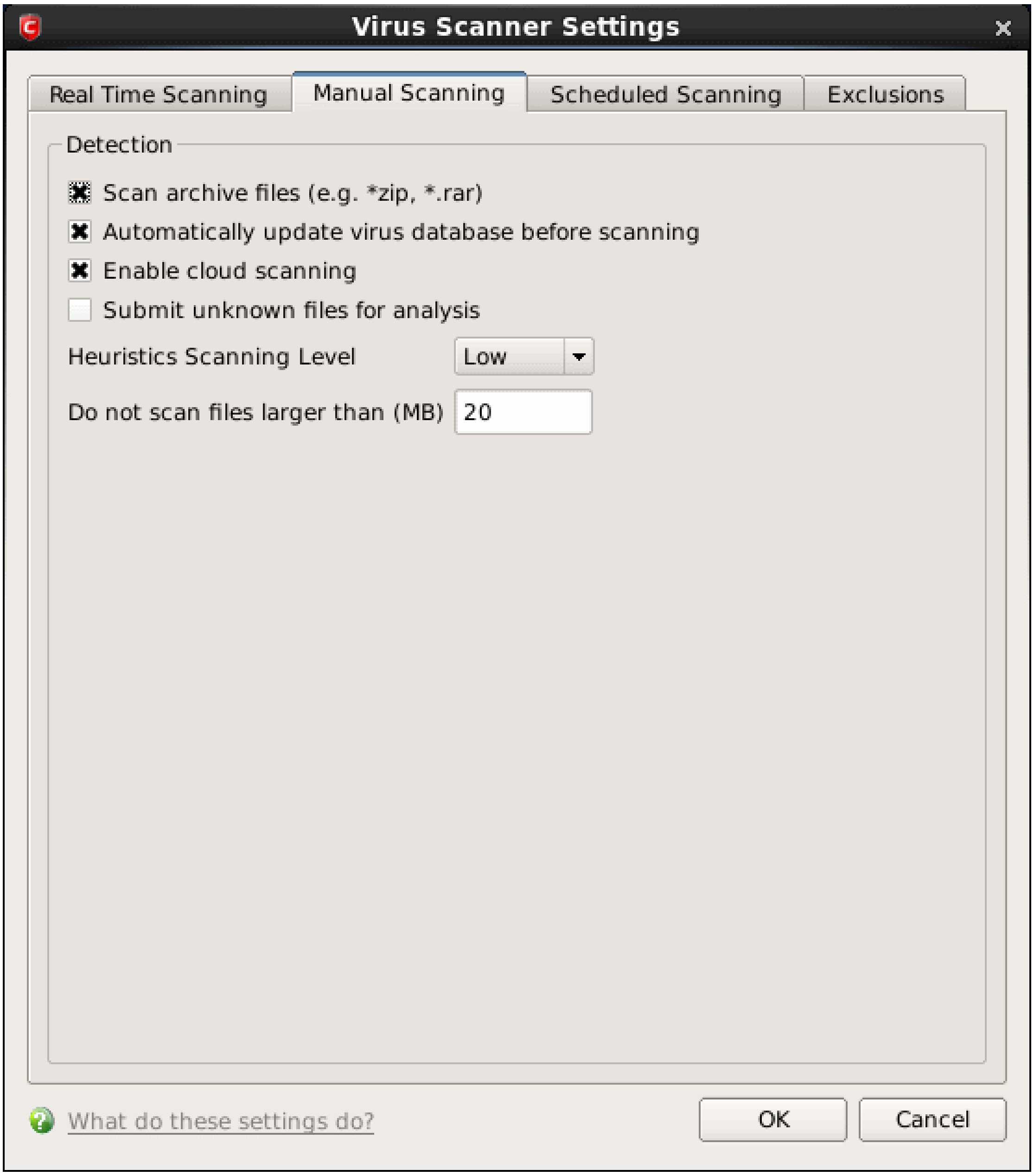
- **Do not scan files larger than -** This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. ***(Default = 20 MB)*** .

- **Keep an alert on the screen for** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen ***(Default = 120 seconds).***

Click 'OK' to apply your changes.

2.8.2. Manual Scanning

The Manual Scanning area allows you to set the parameters that will be implemented when you run an 'On Demand' scan on your computer. For example, these options will be used when you click 'Scan Now' from the main 'Summary' screen or 'Run A Scan' from the 'Antivirus Tasks' menu.



Virus Scanner Settings

Real Time Scanning | Manual Scanning | Scheduled Scanning | Exclusions

Detection

☒ Scan archive files (e.g. *zip, *.rar)

☒ Automatically update virus database before scanning

☒ Enable cloud scanning

☐ Submit unknown files for analysis

Heuristics Scanning Level: Low

Do not scan files larger than (MB): 20

- **Scan archive files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. You are alerted to the presence of viruses in compressed files before you even open them. These include RAR, ZIP and CAB archives ***(Default = Enabled)*** .
- **Automatically update virus database before scanning** - Instructs Comodo Antivirus to check for latest virus database updates from Comodo website and download the updates automatically before starting an on-demand scanning ***(Default = Enabled)*** .
- **Enable cloud scanning** - Instructs Comodo Antivirus to perform cloud based antivirus scanning. Selecting this option enables CAVL to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is outdated. ***(Default = Enabled)***.
- **Submit unknown files for analysis** - Files which are identified as 'unknown' i.e. the files are neither in the safe-list or black list, from the cloud based scanning to Comodo for analysis. The files will be analyzed by experts at Comodo and added to the white list or black list accordingly. This will help maintaining the white list and black list more up-to-date and benefit all the users of CAVL. ***(Default = Disabled)***
- **Heuristics Scanning Level** - Comodo AntiVirus employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that

matches a signature on the virus blacklist.

This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

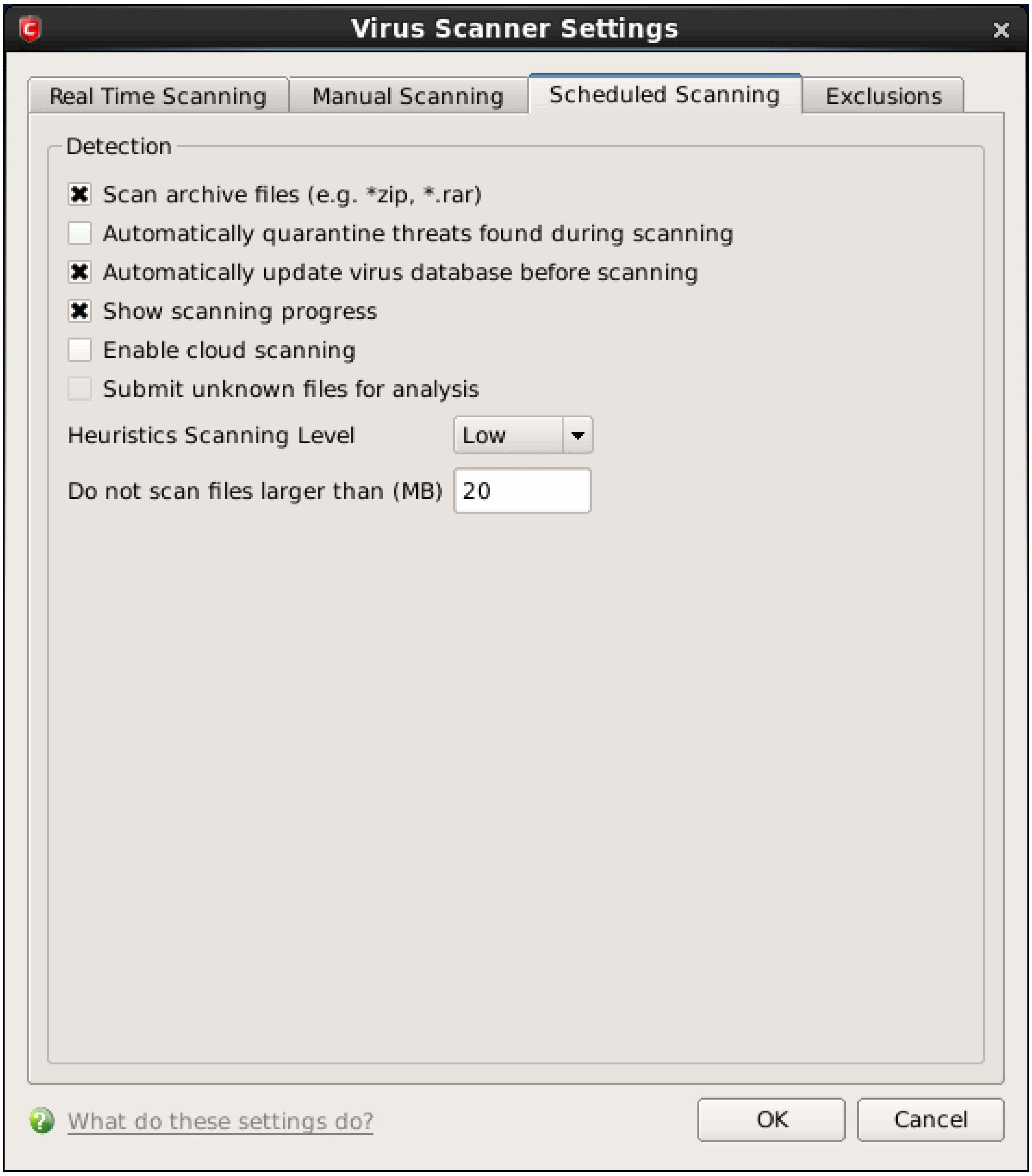
- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
- **Low *(Default)*** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives**.** This setting combines an extremely high level of security and 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 the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Do not scan files larger than -** This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. ***(Default = 20 MB)*** .

Click 'OK' to apply your changes.

2.8.3. Scheduled Scanning

The Scheduled Scanning settings area allows you to determine the scan parameters that will be implemented when a scheduled scan takes place.



Detection

☒ Scan archive files (e.g. *zip, *.rar)

□ Automatically quarantine threats found during scanning

☒ Automatically update virus database before scanning

☒ Show scanning progress

□ Enable cloud scanning

□ Submit unknown files for analysis

Heuristics Scanning Level: Low

Do not scan files larger than (MB): 20

You can choose to run scheduled scans at a certain time on a daily, weekly, monthly or custom interval basis. You can also choose which specific files, folders or drives are included in that scan by choosing the scan profiles.

The detection settings are as follows:

- **Scan archive files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. You are alerted to the presence of viruses in compressed files before you even open them. These include RAR, ZIP and CAB archives ***(Default = Enabled)*** .
- **Automatically quarantine threats found during scanning** - When this check box is selected, the Antivirus moves the file detected to be containing the malware, to Quarantined Items. From the quarantined items the files can be restored or deleted at your will ***(Default = Disabled)***.
- **Automatically update virus database before scanning** - Instructs Comodo Antivirus to check for latest virus database updates from Comodo website and download the updates automatically before starting an on-demand scanning ***(Default = Enabled)*** .
- **Show scanning progress** - When this check box is selected, a progress bar is displayed on start of a scheduled scan. Clear this box if you do not want to see the progress bar ***(Default = Enabled)***.
- **Enable cloud scanning** - Instructs Comodo Antivirus to perform cloud based antivirus scanning. Selecting this option enables CAVL to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting

zero-day malware even if your local anitvirus database is out-dated. ***(Default = Disabled)***.

- **Submit unknown files for analysis** - Files which are identified as 'unknown' i.e. the files are neither in the safe-list or black list, from the cloud based scanning to Comodo for analysis. The files will be analyzed by experts at Comodo and added to the white list or black list accordingly. This will help maintaining the white list and black list more up-to-date and benefit all the users of CAVL. ***(Default = Disabled)***
- **Heuristics Scanning Level** - Comodo AntiVirus employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

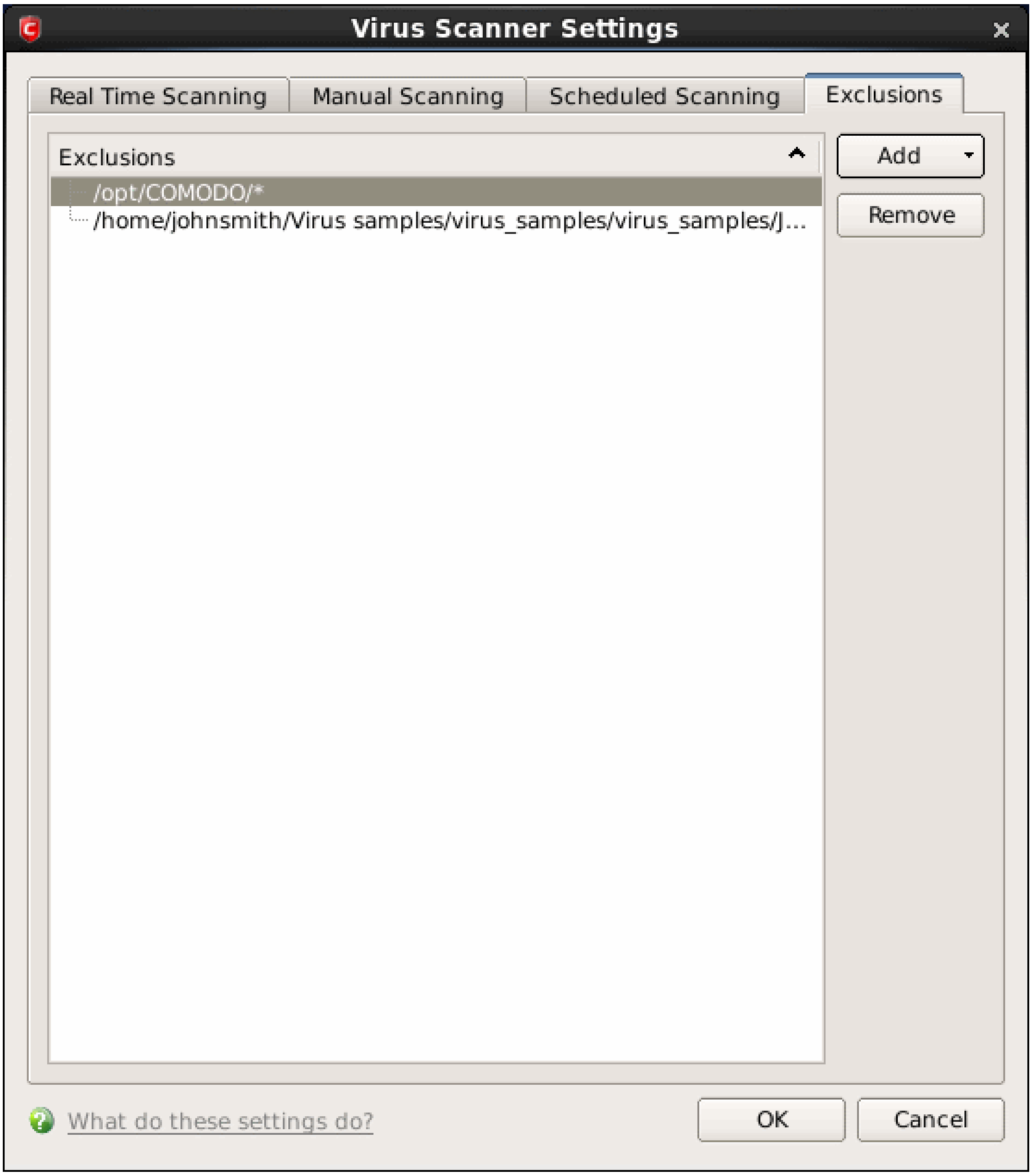
  The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

  - **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
  - **Low *(Default)*** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives*.* This setting combines an extremely high level of security and 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 the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Do not scan files larger than -** This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. ***(Default = 20 MB)*** .

Click 'OK' to apply your changes.

2.8.4. Exclusions

The Exclusions tab in the Scanner Settings panel displays a list of applications/files for which you have selected **Ignore** in the **Scan Results** window of Run a Scan option or added to the Exclusions from an antivirus alert.



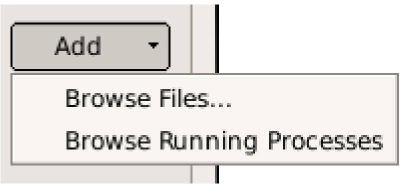
All items listed and all items added to the 'Exclusions' list is excluded from all future scans of all types.

Also, you can manually define trusted files or applications to be excluded from a scan .

To define a file/application as trusted and to be excluded from scanning

1. Click 'Add'.

You now have 2 methods available to choose the application that you want to trust - '**Browse Files...**' and '**Browse Running Processes**'.



- **Browse Files... -** This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.
- **Browse Running Processes -** As the name suggests, this option allows you to choose the target application from a

list of processes that are currently running on your PC.

When you have chosen the application using one of the methods above, the application name appears along with its location.

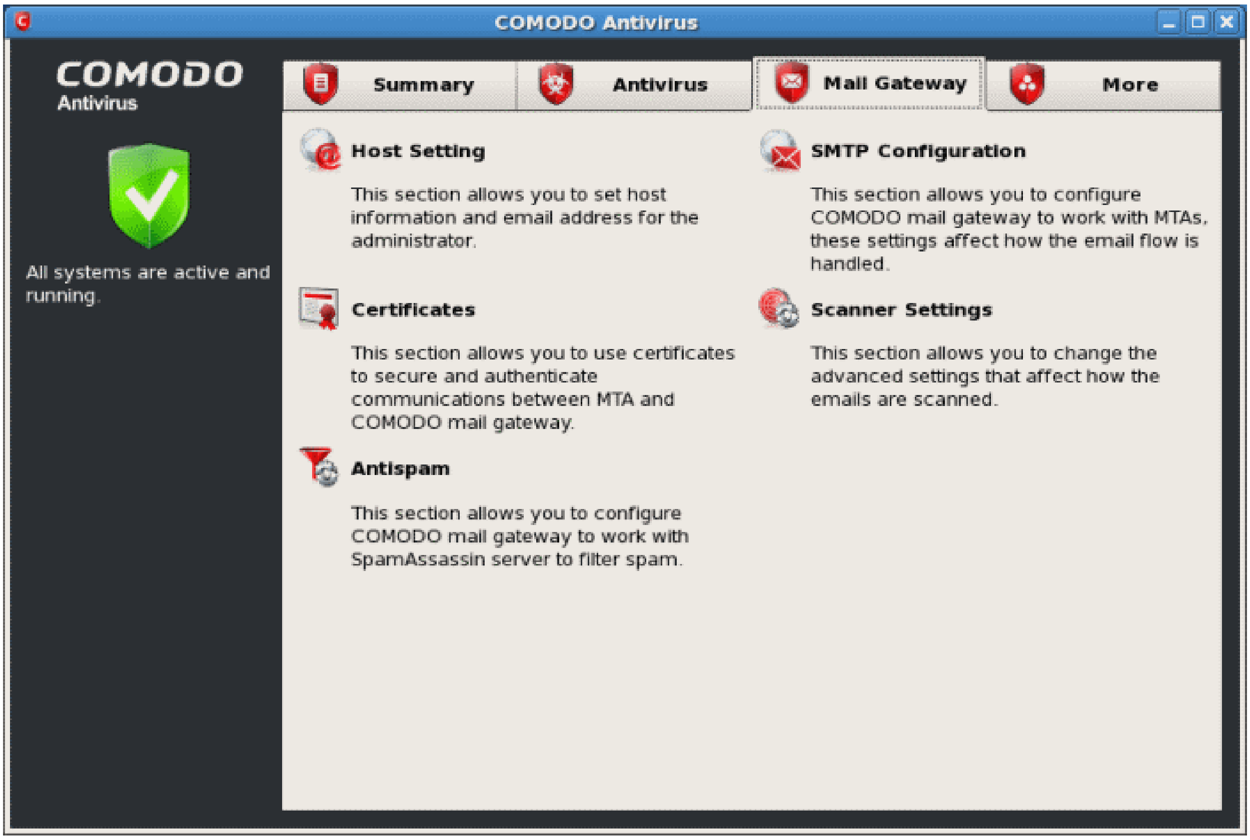
2. Click 'OK' for the settings to take effect.

3. Mail Gateway Tasks – Introduction

Online fraudsters and cyber-criminals use emails as an important delivery system to infect users' computers with viruses and spam. In a corporate environment, cleaning up the infected emails is a costly affair in addition to the time spent in doing that. The Mail Gateway component in CAVL is an effective mail scanning agent that is capable of isolating spam mails and virus attachments before passing them to Mail Transfer Agent (MTA) for delivery to the recipients. The Mail Gateway can support the following open source MTAs:

- Sendmail 8.14.3
- qmail 1.03
- Postfix 2.5.x or higher
- Exim 4.x

The Mail Gateway Tasks area can be accessed at all times by clicking the Mail Gateway tab from the main interface.



All systems are active and running.

Host Setting

This section allows you to set host information and email address for the administrator.

SMTP Configuration

This section allows you to configure COMODO mail gateway to work with MTAs, these settings affect how the email flow is handled.

Certificates

This section allows you to use certificates to secure and authenticate communications between MTA and COMODO mail gateway.

Scanner Settings

This section allows you to change the advanced settings that affect how the emails are scanned.

Antispam

This section allows you to configure COMODO mail gateway to work with SpamAssassin server to filter spam.

The Mail Gateway screen allows you to quickly and easily configure all aspects of mail gateway component of CAVL. Click the links below to see detailed explanations of each area in this section.

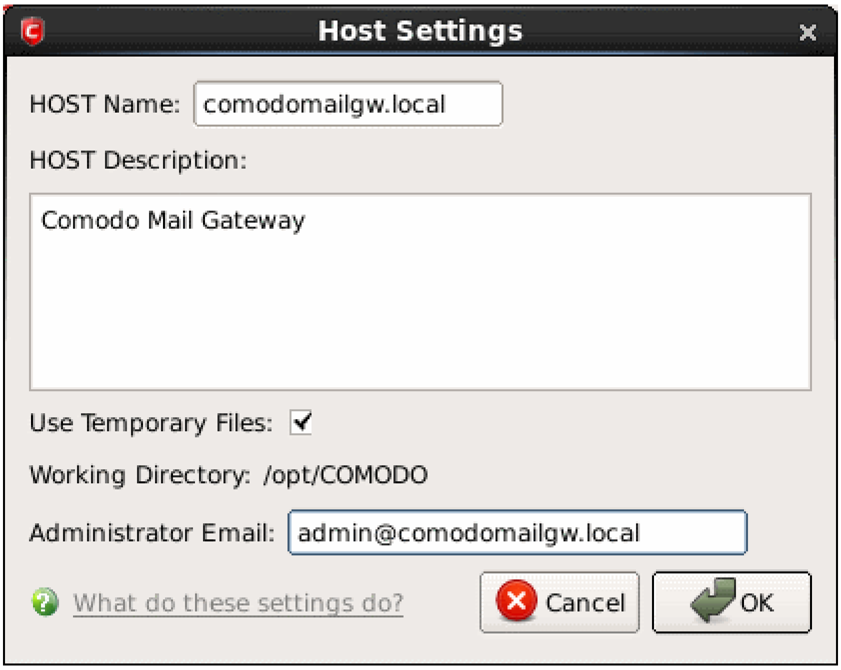
- Host Setting
- Certificates
- Antispam
- SMTP Configuration
- View Mail Events
- Scanner Settings

3.1. Host Setting

The Host Settings interface allows you to configure the host name of the mail server.

To access the Host Settings interface

- Click 'Host Settings' from the Mail Gateway tab in the main interface.



Host Settings

HOST Name: comodomailgw.local

HOST Description:

Comodo Mail Gateway

Use Temporary Files: ☑

Working Directory: /opt/COMODO

Administrator Email: admin@comodomailgw.local

- **Host Name** - Enter the host name of the email gateway server.
- **Host Description** - Enter a description for the host.
- **User Temporary Files** - Select this checkbox if you want to CAVL should use temporary files.
- **Working Directory** - Displays the CAVL's working directory.
- **Administrator Email -** Enter the email of the administrator.

3.2. Certificates

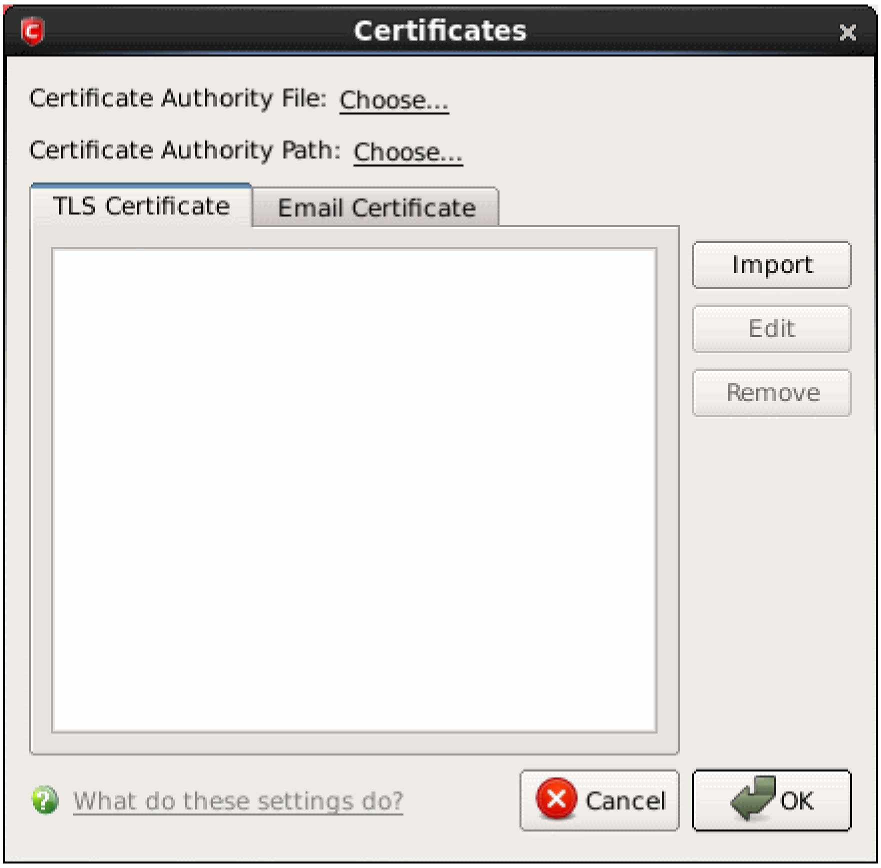
Unsecured email messages are rather like sending a postcard written in pencil - they can be intercepted, read or edited by anyone along the way. To avoid this, every message sent should be encrypted and signed using a digital certificate. The certificates use private and public key technology to authenticate and encrypt data as well as secure all email communications, usernames, and passwords.

TLS certificates are used for authentication between Mail Transfer Agent and Mail Gateway. Emails certificates are stored in Mail Gateway and used to verify digital signature as well as for encrypting and decrypting emails. However, if an email contains virus it will not be encrypted.

You can use a self-signed certificate or a signed certificate that a Certificate Authority (CA) such as Comodo issues.

To import certificates

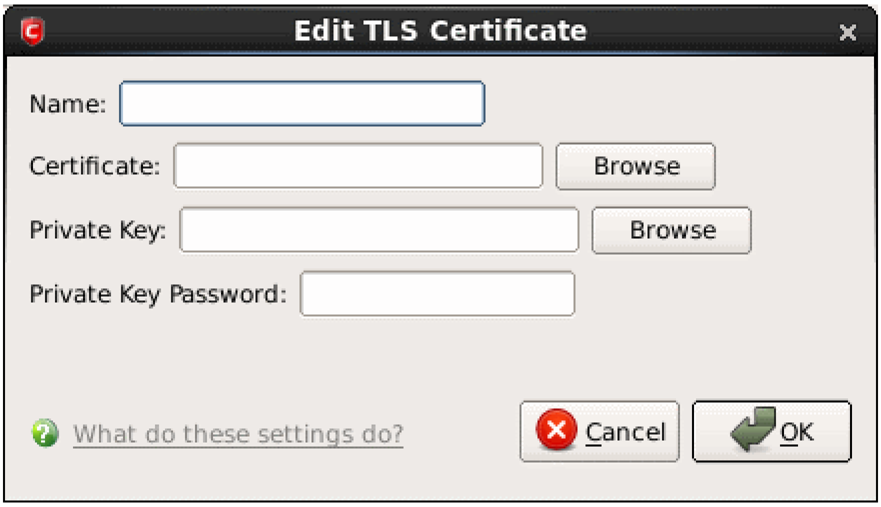
- Click 'Certificates' from the Mail Gateway tab in the main interface.


Certificates
Certificate Authority File: Choose...
Certificate Authority Path: Choose...
TLS Certificate
Email Certificate
Import
Edit
Remove
What do these settings do?
Cancel
OK

- Select TLS Certificate or Email Certificate tab.
- **Certificates Authority File** - Click "Choose..." to select a Certificates Authority File.
- **Certificates Authority Path** - Click "Choose..." to select a Certificates Authority Path.

Edit TLS Certificate

- Click the 'Import' button.



- **Name** - Enter the name of the certificate. This name will be used for referencing in SMTP configuration.
- **Certificate** - Click the 'Browse' button beside the field and navigate to the location where the certificate is stored and click 'Open'.
- **Private Key** - Click the 'Browse' button beside the field and navigate to the location where the private key is stored and click 'Open'.

To apply for an email certificate, a user has to generate two keys, a Private Key and a Public Key on their machine. These keys are generated by your operating system during the application for a certificate using an encryption algorithm. The Private Key should not be shared with anyone and you the Public Key to anyone. The two keys are cryptographically related and anything encrypted by the public key CAN ONLY be decrypted by the corresponding private key and similarly anything encrypted by the private key CAN ONLY be decrypted by the corresponding public key. Using the two key for emails ensures authentication, privacy and integrity.

- **Private Key Password** - This field is the passphrase for the private key, or empty if you use unencrypted private key.

To edit an existing certificate

- Select the certificate and click 'Edit' to edit the property from the Edit TLS Certificate dialog box.

To delete a certificate

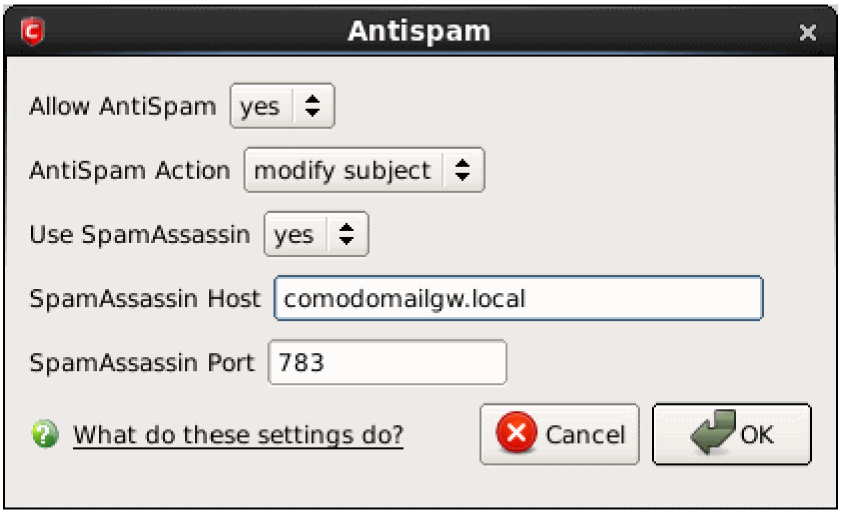
- Select the item and Click 'Remove'.

3.3. Antispam

Antispam feature in CAVL blocks spam emails automatically thus enabling users and administrators to save time and effort in removing them manually. This also helps to prevent your system from being attacked by various email borne malware and viruses. Comodo Antispam uses SpamAssassin, a open-source Apache project.

To configure Antispam with SpamAssassin

- Click 'Antispam' from the Mail Gateway tab in the main interface.


Antispam

Allow AntiSpam: yes

AntiSpam Action: modify subject

Use SpamAssassin: yes

SpamAssassin Host: comodomailgw.local

SpamAssassin Port: 783

- **Allow AntSpam** - Select 'Yes' from the drop-down to enable Antispam.
- **AntiSpam Action** - Select the action to be carried out when a spam is detected.
  - **Modify Subject** - Modifies the subject of the spam.
- **Use SpamAssassin** - Select 'Yes' to use SpamAssassin.

SpamAssassin is a open-source software and based on various spam-detection technologies such as Bayesian filtering, DNS-based and fuzzy-checksum-based spam detection, blacklists, external programs and online databases. It is so versatile that the program can be structured with a mail server or several mail programs. Individual users also can integrate this program with their mailboxes. This highly configurable program can be used to support per-user preferences even if used as a system-wide filter.

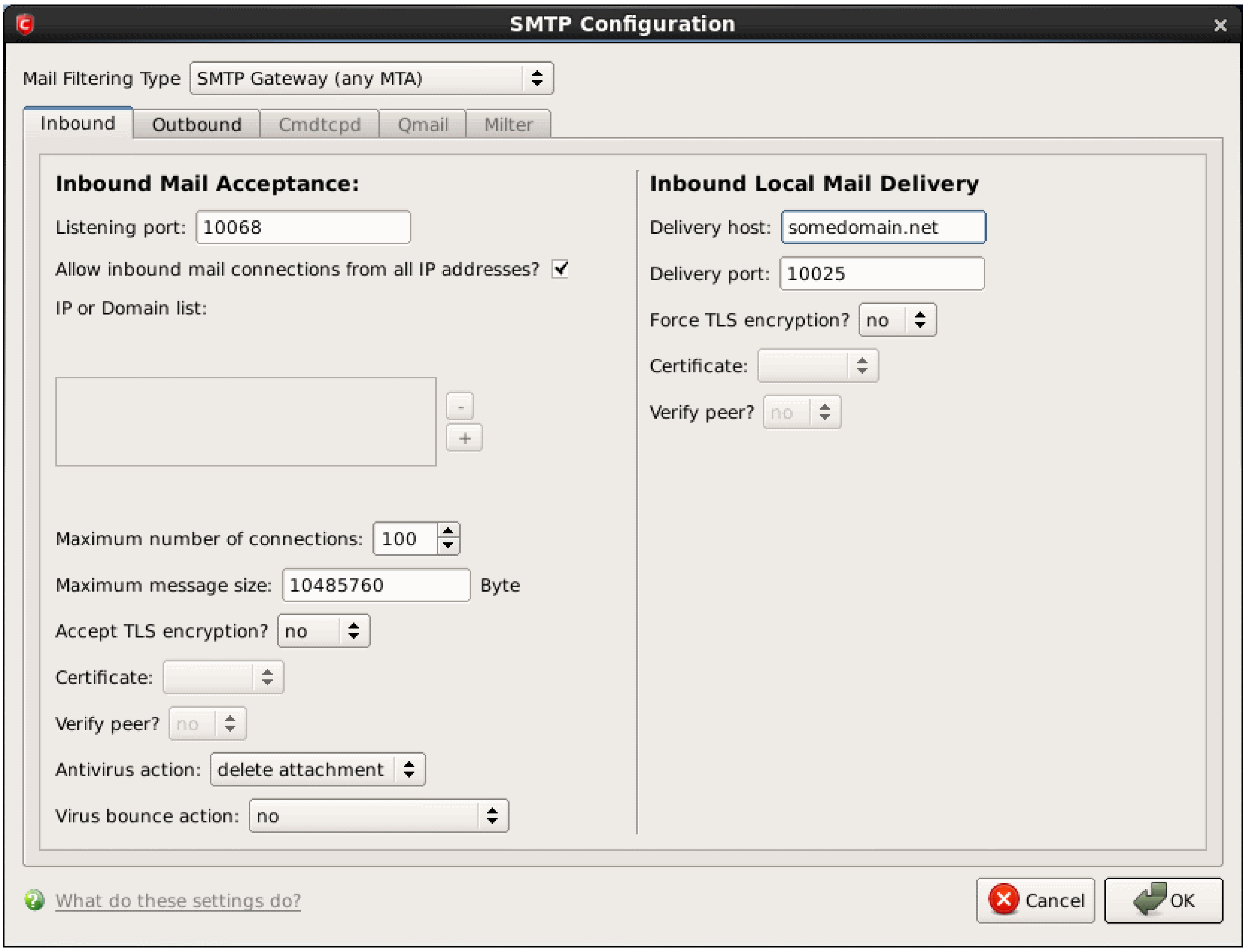
- **SpamAssassin Host** - Enter the hostname of the SpamAssassin server.
- **SpamAssassin Port** - Enter the listening port of the SpamAssassin server.

3.4. SMTP Configuration

The SMTP configuration screen in CAVL allows you to configure the mail filtering process. Filters can be set to monitor both inbound an outbound mails with or without attachments as well as to remove spam and computer viruses. It also supports other MTAs such as Cmdtcpd, Qmail and Milter.

To access SMTP Configuration interface

- Click 'SMTP Configuration' from the Mail Gateway tab in the main interface.



Mail Filtering Type: SMTP Gateway (any MTA)

Inbound Mail Acceptance:

Listening port: 10068

Allow inbound mail connections from all IP addresses? ☑

IP or Domain list:

Maximum number of connections: 100

Maximum message size: 10485760 Byte

Accept TLS encryption? no

Certificate:

Verify peer? no

Antivirus action: delete attachment

Virus bounce action: no

Inbound Local Mail Delivery

Delivery host: somedomain.net

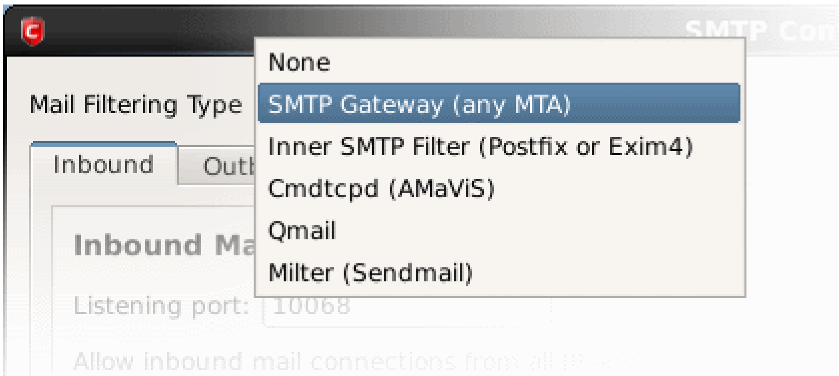
Delivery port: 10025

Force TLS encryption? no

Certificate:

Verify peer? no

You can choose the filtering type by clicking the drop-down button beside the 'Mail Filtering Type' selection box.



If you choose 'None' from the drop-down, the SMTP configuration is disabled and no mails will be filtered. The type of mail filter selected here will be displayed in the **Summary** screen.

Click on the following links for details:

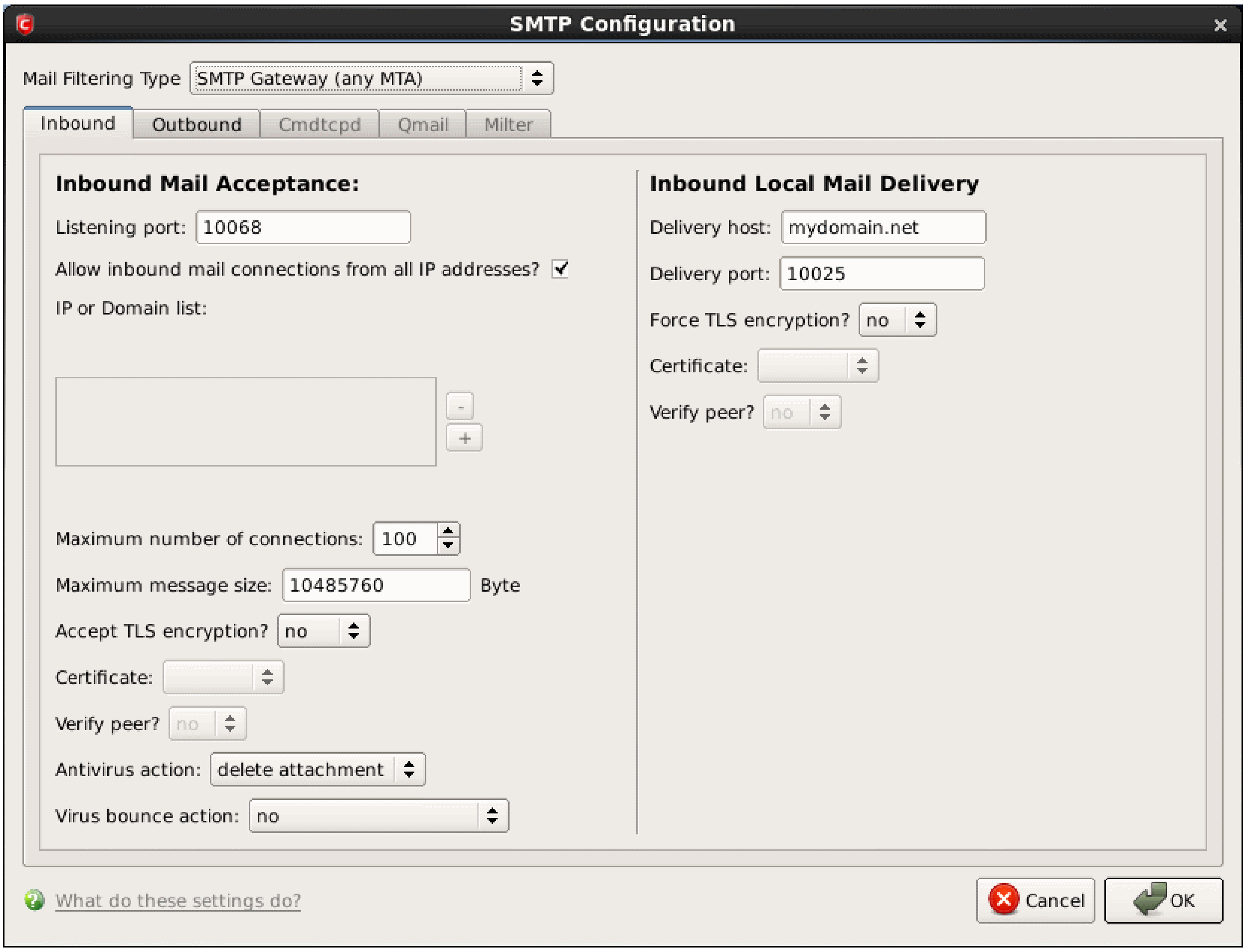
- **SMTP Gateway (any MTA)**

- **Inner SMTP Filter**
- **Cmdtcpd**
- **Qmail**
- **Milter**

3.4.1. SMTP Gateway (any MTA)

The SMTP Gateway filtering interface allows you to configure the settings for filtering all incoming and outgoing mails for your domain, irrespective of the Mail Transfer Agent (MTA) you are using. The mails will be checked for spam, viruses and so on, before passing on to the mail server for delivery to the recipients.

To configure filter settings for all inbound and outbound mails, select 'SMTP Gateway (any MTA)' from the 'Mail Filtering Type' drop-down box.



SMTP Configuration

Mail Filtering Type: SMTP Gateway (any MTA)

Inbound Mail Acceptance:

Listening port: 10068

Allow inbound mail connections from all IP addresses? ☑

IP or Domain list:

Maximum number of connections: 100

Maximum message size: 10485760 Byte

Accept TLS encryption? no

Certificate:

Verify peer? no

Antivirus action: delete attachment

Virus bounce action: no

Inbound Local Mail Delivery

Delivery host: mydomain.net

Delivery port: 10025

Force TLS encryption? no

Certificate:

Verify peer? no

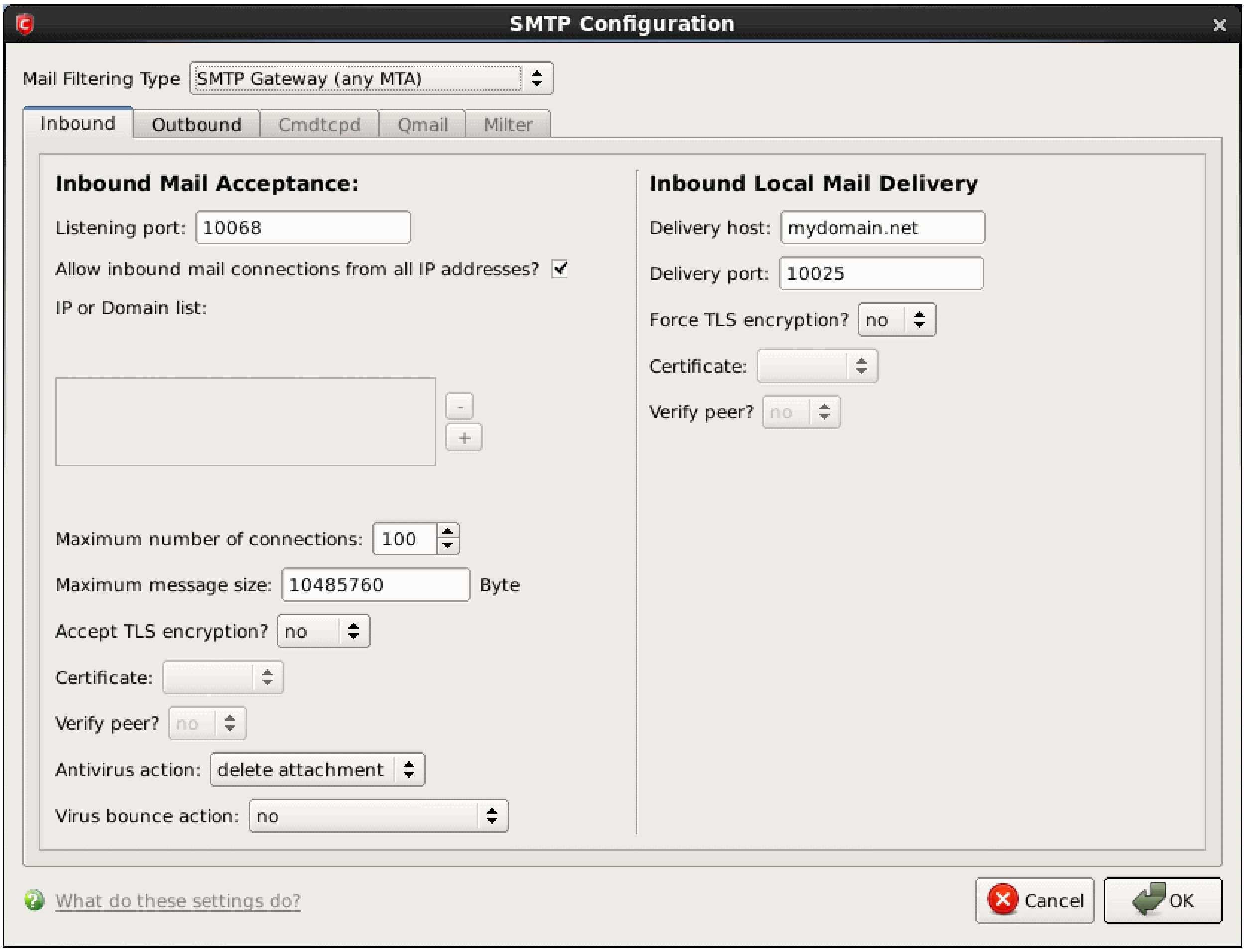
Click the links below for more information

- **Configuring for Inbound Mail Filtering**
- **Configuring for Outbound Mail Filtering**

3.4.1.1. Configuring for Inbound Mail Filtering

By default, the Inbound filtering interface will be displayed on selecting 'SMTP Gateway (any MTA)' from the 'Mail Filtering Type' drop-down. If not, click 'Inbound' tab from the configuration panel to open the interface.

Note: If you are using Postfix or Exim4 MTA, it is recommended to configure your inbound mail filtering through Inner SMTP Filter interface. Refer to the section **Inner SMTP Filter** for more details.



SMTP Configuration

Mail Filtering Type: SMTP Gateway (any MTA)

Inbound Mail Acceptance:

Listening port: 10068

Allow inbound mail connections from all IP addresses? ☑

IP or Domain list:

Maximum number of connections: 100

Maximum message size: 10485760 Byte

Accept TLS encryption? no

Certificate:

Verify peer? no

Antivirus action: delete attachment

Virus bounce action: no

Inbound Local Mail Delivery

Delivery host: mydomain.net

Delivery port: 10025

Force TLS encryption? no

Certificate:

Verify peer? no

Inbound Mail Acceptance

- **Listening Port** - Specify the listening port of the Comodo Mail Gateway's MTA.

Note: If Comodo Mail Gateway and mail server are on the same host, this listening port should be different from the mail server's listening port (default is 25 for SMTP).

- **Allow inbound mail connections from all IP address?** - If this box is checked, Mail Gateway will accept connections from all IP addresses. If unchecked, Mail Gateway will only accept connections from the "IP or Domain list" given in the box. This box is selected by default.
- **IP or Domain list -** This field enables you to restrict Comodo Mail Gateway to accept connections only from a set of hosts by specifying a list of allowed hosts. This box is enabled only if the **Allow inbound mail connections from all IP address?** is unchecked. Click on the + button and then double-click on the shaded area in the field. Enter the domain name or IP Address in the field. Repeat the process to add more domains.
- **Maximum number of connections** - Specify the maximum number of connections which Comodo Mail Gateway can accept..
- **Maximum message size** - Set a maximum limit (in Bytes) for the size of received messages that Comodo Mail Gateway should accept.
- **Accept TLS encryption** - Specify whether Transport Layer Security (TLS) encryption is required for the connections to Mail Gateway, from the drop-down.
  - **Must -** Comodo Mail Gateway will reject all non secure connections.
  - **Can -** Comodo Mail Gateway will support secure connection on demand of client.
  - **No** - Comodo Mail Gateway will not support secure connection.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** - Set it to yes if you want mail gateway to verify authenticity of a server certificate, otherwise mail gateway

will only use secure connection without verifying.

- **Antivirus action** - Comodo Mail Gateway receives emails and then scans the attachments. If attachments contain virus, Mail Gateway will do a specified action, like modifying its subject to indicate it contains malicious attachments or delete the attachment and then pass the modified email on to the mail server. Specify the action to be taken on the mails identified with virus attachments:
  - **Modify Subject** - Adds a note to the subject of the mail. An example of modified subject: **[VIRUS: 008gangsir.cn.exe infected by Malware] Bank Statements**
  - **Delete Attachment** - Deletes the virus attachment.
- **Virus bounce action** - Bounce e-mail (sometimes referred to as bounce mail) is electronic mail that is returned to the sender because it cannot be delivered for some reason. Select the bounce action to be taken on mails identified with virus attachments:
  - **No** - The email will not be returned to the sender
  - **Bounce** - The email will be returned to the sender
  - **Bounce without original** - The email header will be returned to the sender without the original content and the attachments

Note: The From address on a spam maybe is forged, so we suggest you set it to 'no'.

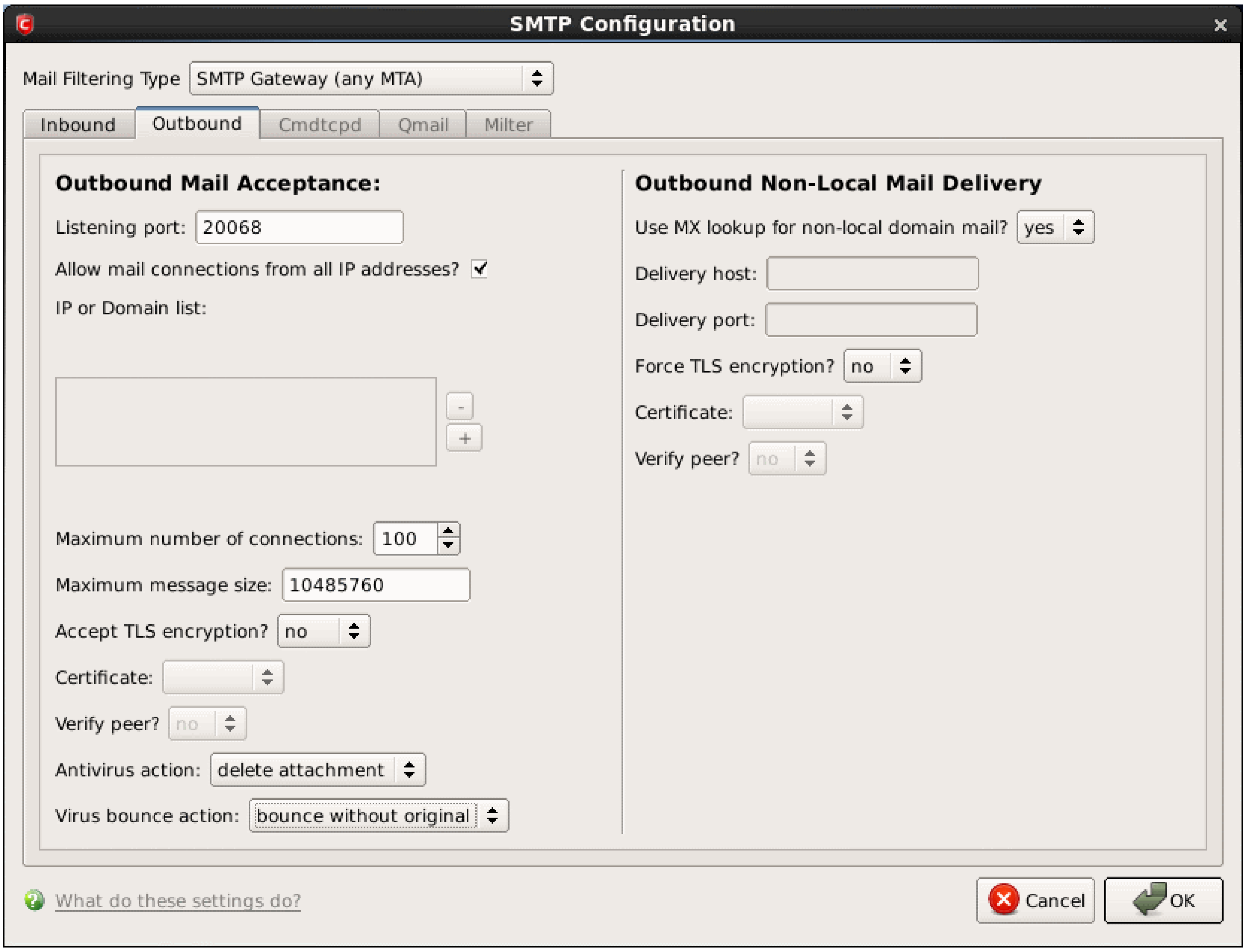
Inbound Local Mail Delivery

- **Delivery host** - Specify the mail server host or the mail server's IP address to which the mail gateway should pass the scanned mails.
- **Delivery port** - Specify the listening port of the mail server.
- **Force TLS encryption ?** - Specify whether Comodo Mail Gateway should use only TLS secured connections. Default value is 'no'.
  - **Yes** - Comodo Mail Gateway will reject non secure connections.
  - **No** - Comodo Mail Gateway will support secure connection if server supports it.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** – Specify whether or not to verify the authenticity of a server certificate. Select 'Yes' or 'No'. Default value is 'no'.
  - **Yes** - Comodo Mail Gateway will verify authenticity of inner mail server's certificate.
  - **No** - Comodo Mail Gateway will only use secure connection without verifying.

Click 'OK' for the changes to take effect.

3.4.1.2. Configuring for Outbound Mail Filtering

To configure for filtering the outbound mails from your domain, click the 'Outbound' tab of the configuration panel.



SMTP Configuration

Mail Filtering Type: SMTP Gateway (any MTA)

Outbound Mail Acceptance:

Listening port: 20068

Allow mail connections from all IP addresses? ☑

IP or Domain list:

Maximum number of connections: 100

Maximum message size: 10485760

Accept TLS encryption? no

Certificate:

Verify peer? no

Antivirus action: delete attachment

Virus bounce action: bounce without original

Outbound Non-Local Mail Delivery

Use MX lookup for non-local domain mail? yes

Delivery host:

Delivery port:

Force TLS encryption? no

Certificate:

Verify peer? no

- **Listening Port** - Specify the listening port of the Comodo Mail Gateway's MTA.

Note: If Comodo Mail Gateway and mail server are on the same host, this listening port should be different from the mail server's listening port (default is 25 for SMTP).

- **Allow outbound mail connections from all IP address?** - If this box is checked, Mail Gateway will accept connections from all IP addresses. If unchecked, Mail Gateway will only accept connections from the "IP or Domain list" given in the box. This box is selected by default.
- **IP or Domain list** - This field enables you to restrict Comodo Mail Gateway to accept connections only from a set of hosts by specifying a list of allowed hosts. This box is enabled only if the **Allow outbound mail connections from all IP address?** is unchecked. Click on the + button and then double-click on the shaded area in the field. Enter the domain name or IP Address of the allowed domain in the field. Repeat the process to add more domains.
- **Maximum number of connections** - Specify the maximum number of connections which Comodo Mail Gateway can accept..
- **Maximum message size** - Set a maximum limit (in Bytes) for the size of received messages that Comodo Mail Gateway should accept.
- **Accept TLS encryption** - Specify whether Transport Layer Security (TLS) encryption is required for the connections to Mail Gateway, from the drop-down:
  - **Must -** Comodo Mail Gateway will reject all non secure connections.
  - **Can -** Comodo Mail Gateway will support secure connection on demand of client.
  - **No** - Comodo Mail Gateway will not support secure connection.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** - Set it to yes if you want mail gateway to verify authenticity of a server certificate, otherwise mail gateway will only use secure connection without verifying.

- **Antivirus action** - Comodo Mail Gateway receives emails and then scans the attachments. If attachments contain virus, Mail Gateway will do a specified action, like modifying its subject to indicate it contains malicious attachments or delete the attachment and then pass the modified email on to the mail server. Specify the action to be taken on the mails identified with virus attachments:
    - **Modify Subject** - Adds a note to the subject of the mail. An example of modified subject: **[VIRUS: 008gangsir.cn.exe infected by Malware] Bank Statements**
    - **Delete Attachment** - Deletes the virus attachment.
- **Virus bounce action** - Bounce e-mail (sometimes referred to as bounce mail) is electronic mail that is returned to the sender because it cannot be delivered for some reason. Select the bounce action to be taken on mails identified with virus attachments:
    - **No** - The email will not be returned to the sender
    - **Bounce** - The email will be returned to the sender
    - **Bounce without original** - The email header will be returned to the sender without the original content and the attachments

Outbound Local Mail Delivery

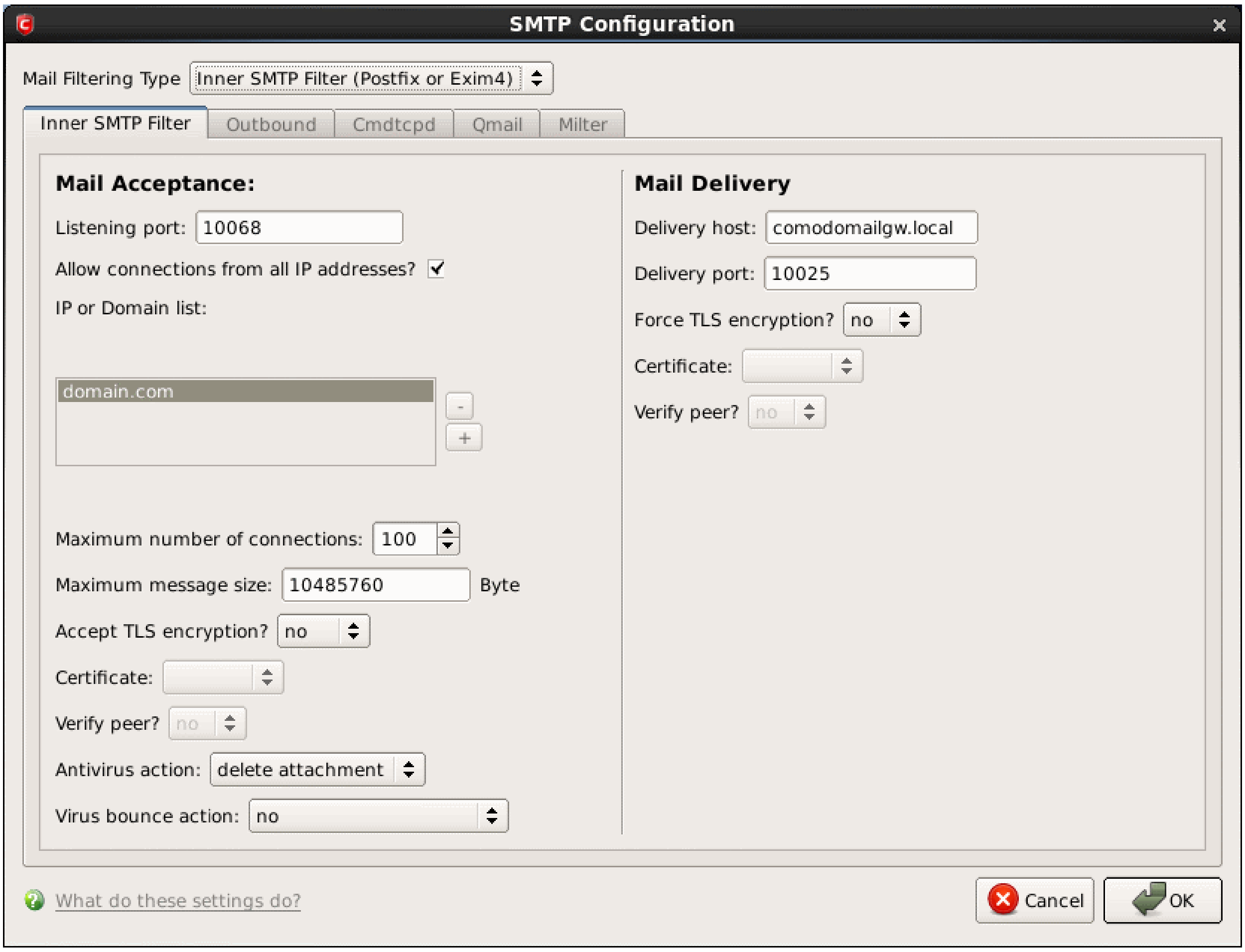
- **Use MX lookup for non-local domain mail?** - Select 'no' if you want to manually specify a delivery host. Default is 'yes'.
- **Delivery host** - Specify the host name or the IP address of the mail server to which the mail gateway should pass the scanned mails.
- **Delivery port** - Specify the listening port of the mail server.
- **Force TLS encryption ?** - Specify whether Comodo Mail Gateway should use only TLS secured connections. Default value is 'no'.
    - **Yes** - Comodo Mail Gateway will reject non secure connections.
    - **No** - Comodo Mail Gateway will support secure connection if server supports.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** – Specify whether or not to verify the authenticity of a server certificate. Select 'Yes' or 'No'. Default value is 'no'.
    - **Yes** - Comodo Mail Gateway will verify authenticity of inner mail server's certificate.
    - **No** - Comodo Mail Gateway will only use secure connection without verifying.

Click 'OK' for the changes to take effect.

3.4.2. Inner SMTP Filter

If you are using Postfix or Exim4 Mail Transfer Agent (MTA) then Inner SMTP Filter interface allows you to configure the filtering for the inbound mails. The mails will be checked for spam, viruses and so on, before being passed on to the mail server for delivery to the recipients.

To configure filter settings for all inbound and outbound mails, select 'Inner SMTP Filter (Postfix or Exim4)' from the 'Mail Filtering Type' drop-down box.



SMTP Configuration

Mail Filtering Type: Inner SMTP Filter (Postfix or Exim4)

Mail Acceptance:

Listening port: 10068

Allow connections from all IP addresses? ☑

IP or Domain list:

domain.com

Maximum number of connections: 100

Maximum message size: 10485760 Byte

Accept TLS encryption? no

Certificate:

Verify peer? no

Antivirus action: delete attachment

Virus bounce action: no

Mail Delivery

Delivery host: comodomailgw.local

Delivery port: 10025

Force TLS encryption? no

Certificate:

Verify peer? no

Mail Acceptance

- **Listening Port** - Specify the listening port of the Comodo Mail Gateway's MTA.

Note: If Comodo Mail Gateway and mail server are on the same host, this listening port should be different from the mail server's listening port (default is 25 for SMTP).

- **Allow inbound mail connections from all IP address?** - If this box is checked, Mail Gateway will accept connections from all IP addresses. If unchecked, Mail Gateway will only accept connections from the "IP or Domain list" given in the box. This box is selected by default.
- **IP or Domain list -** This field enables you to restrict Comodo Mail Gateway to accept connections only from a set of hosts by specifying a list of allowed hosts. This box is enabled only if the **Allow inbound mail connections from all IP address?** is unchecked. Click on the + button and then double-click on the shaded area in the field. Enter the domain name or IP Address in the field. Repeat the process to add more domains.
- **Maximum number of connections** - Specify the maximum number of connections which Comodo Mail Gateway can accept..
- **Maximum message size** - Set a maximum limit (in Bytes) for the size of received messages that Comodo Mail Gateway should accept.
- **Accept TLS encryption** - Specify whether Transport Layer Security (TLS) encryption is required for the connections to Mail Gateway, from the drop-down.
  - **Must -** Comodo Mail Gateway will reject all non secure connections.
  - **Can -** Comodo Mail Gateway will support secure connection on demand of client.
  - **No** - Comodo Mail Gateway will not support secure connection.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** - Set it to yes if you want mail gateway to verify authenticity of a server certificate, otherwise mail gateway

will only use secure connection without verifying.

- **Antivirus action** - Comodo Mail Gateway receives emails and then scans the attachments. If attachments contain virus, Mail Gateway will do a specified action, like modifying its subject to indicate it contains malicious attachments or delete the attachment and then pass the modified email on to the mail server. Specify the action to be taken on the mails identified with virus attachments:
  - **Modify Subject** - Adds a note to the subject of the mail. An example of modified subject: **[VIRUS: 008gangsir.cn.exe infected by Malware] Bank Statements**
  - **Delete Attachment** - Deletes the virus attachment.
- **Virus bounce action** - Bounce e-mail (sometimes referred to as bounce mail) is electronic mail that is returned to the sender because it cannot be delivered for some reason. Select the bounce action to be taken on mails identified with virus attachments:
  - **No** - The email will not be returned to the sender
  - **Bounce** - The email will be returned to the sender
  - **Bounce without original** - The email header will be returned to the sender without the original content and the attachments

Note: The From address on a spam maybe is forged, so we suggest you set it to 'no'.

Mail Delivery

- **Delivery host** - Specify the mail server host or the mail server's IP address to which the mail gateway should pass the scanned mails.
- **Delivery port** - Specify the listening port of the mail server.
- **Force TLS encryption ?** - Specify whether Comodo Mail Gateway should use only TLS secured connections. Default value is 'no'.
  - **Yes** - Comodo Mail Gateway will reject non secure connections.
  - **No** - Comodo Mail Gateway will support secure connection if server supports it.
- **Certificate** - Choose a certificate for encryption, imported into Comodo Mail Gateway through the **Certificates** dialog.
- **Verify peer** – Specify whether or not to verify the authenticity of a server certificate. Select 'Yes' or 'No'. Default value is 'no'.
  - **Yes** - Comodo Mail Gateway will verify authenticity of inner mail server's certificate.
  - **No** - Comodo Mail Gateway will only use secure connection without verifying.

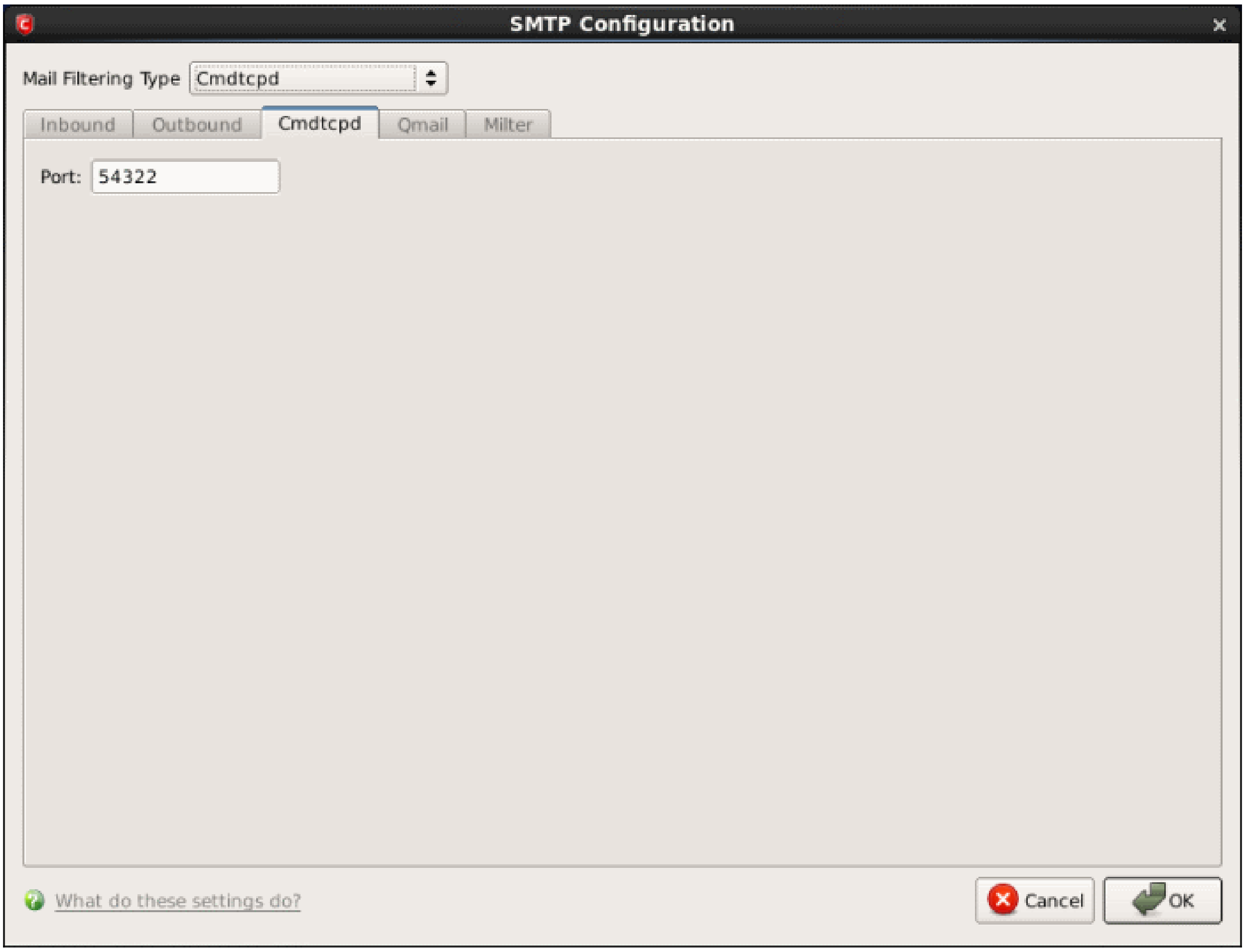
Click 'OK' for the changes to take effect.

3.4.3. Cmdtcpd

Comodo Mail Gateway can be used with '**amavisd-new',** a high-performance interface between a MTA and content checkers such as CAVL and/or SpamAssassin.

To use amavisd-new with Comodo Mail Gateway

- Install **amavisd-new**
- Configure mail server working with **amavisd-new.** For more details refer the site **http://www.ijs.si/software/amavisd/**
- Select 'Cmdtcpd' from the 'Mail Filtering Type' drop-down box.



Mail Filtering Type: Cmdtcpd

Port: 54322

- **Port** – Specify the listening port of amavisd-new.

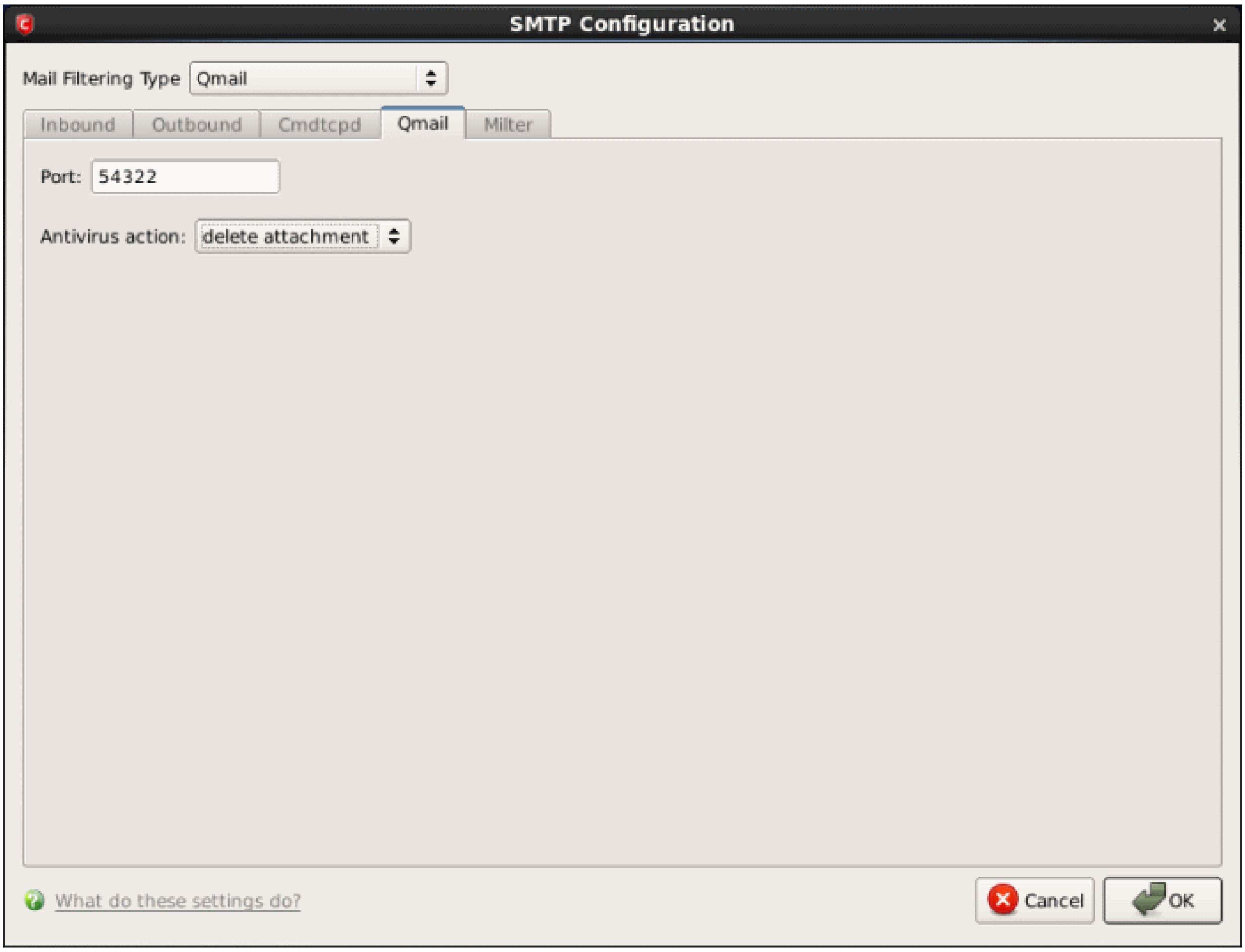
Click 'OK' for the changes to take effect.

3.4.4. Qmail

If you are using Qmail as the mail transfer agent, then you should select this type of mail filtering from the SMTP configuration interface.

To use Qmail as mail filtering type

- Select 'Qmail' from the 'Mail Filtering Type' drop-down box.



Mail Filtering Type: Qmail

Port: 54322

Antivirus action: delete attachment

- **Port** - Specify the listening port of Qmail.
- **Antivirus action** - Specifies the action when the message contains virus. You have two choices:
  - **Modify Subject** - Adds a note to the subject of the mail.
  - **Delete Attachment** - Deletes the virus attachment.

After clicking 'OK' for the changes to take effect, the following commands should be performed:

First, stop the qmail service.

- $sudo service qmail stop

Keep the the file name qmail-queue.org as below, do NOT modify or delete it.

- $sudo cp /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.orig
- $sudo cp /opt/COMODO/qmail-queue-cmg /var/qmail/bin/qmail-queue
- $sudo service qmail start

3.4.5. Milter

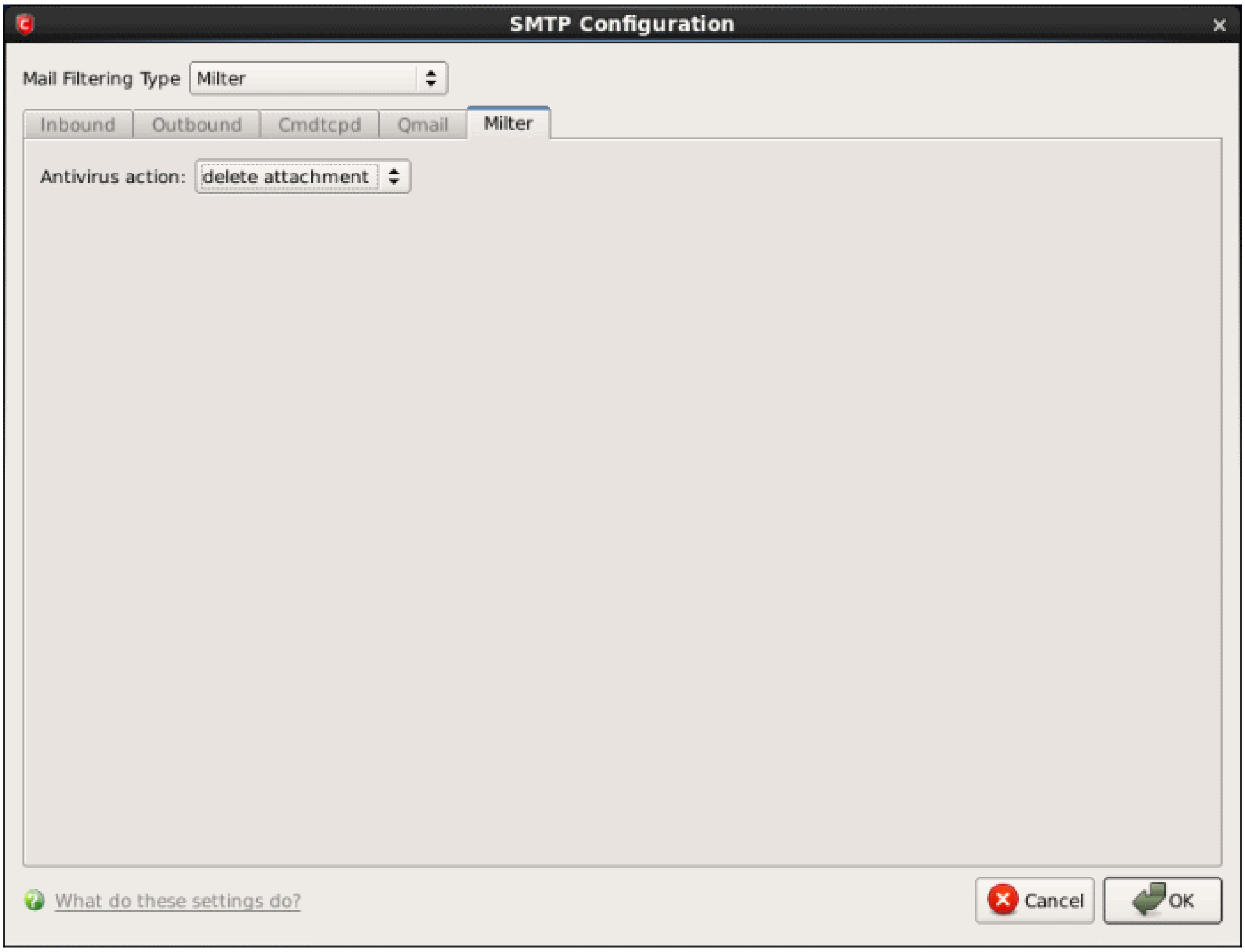
Comodo Mail Gateway can be used as a Milter (Mail Filter) application for e-mail filtering. This allows administrators to efficiently filter virus infected mails and set default actions.

Sendmail configuration

Append the following line to configuration file /etc/mail/sendmail.mc:
INPUT_MAIL_FILTER(`ComodoMailGatewayFilter',`S=local:/var/run/milter-cmg.sock, F=T, T=S:60s;R:60s;E:5m')

To use Milter as mail filtering type

- Select 'Milter' from the 'Mail Filtering Type' drop-down box.



Mail Filtering Type: Milter

Antivirus action: delete attachment

- **Antivirus action** - Specifies the action when the message contains virus. You have two choices:
    - **Modify Subject** - Adds a note to the subject of the mail.
    - **Delete Attachment** - Deletes the virus attachment.

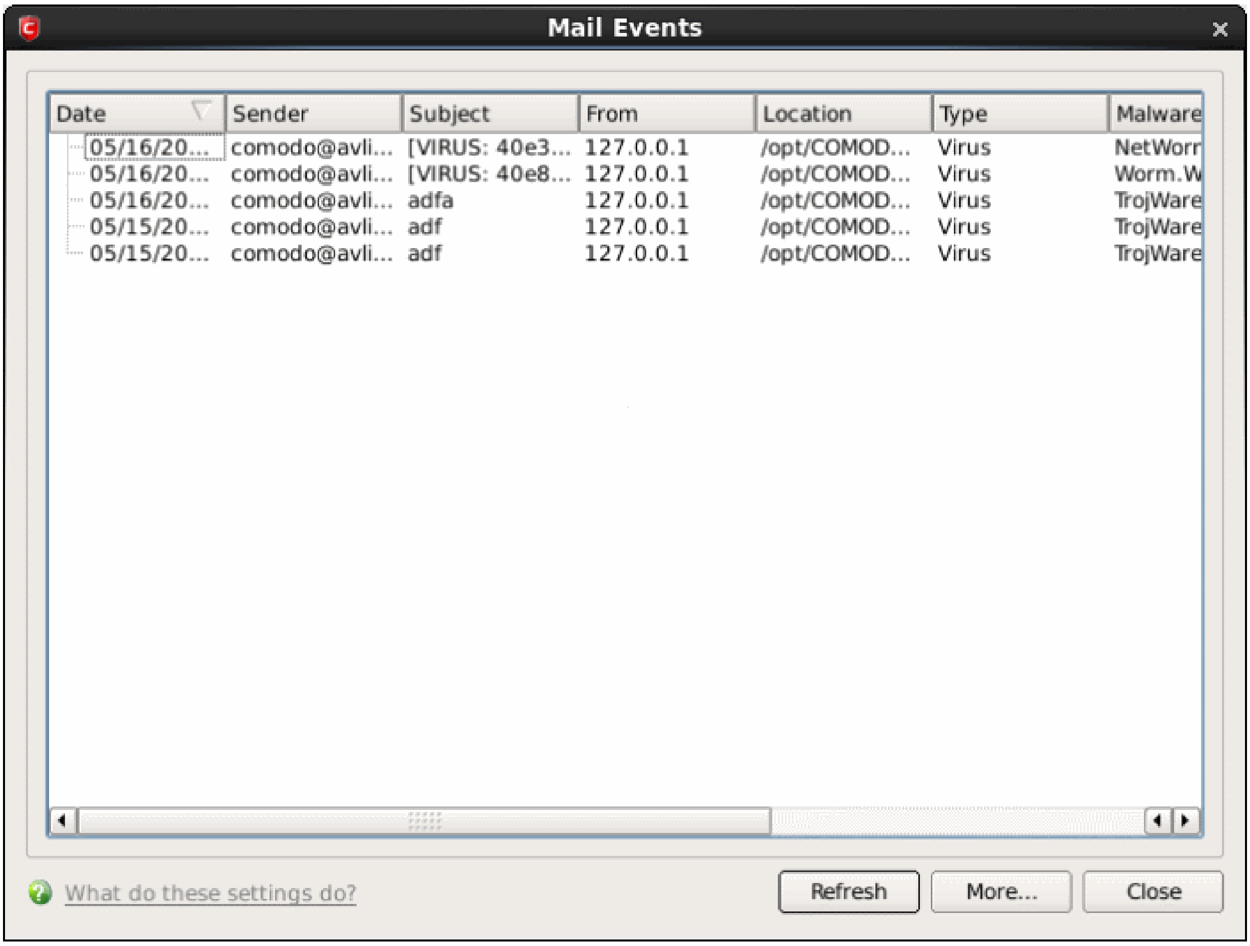
Click 'OK' for the changes to take effect.

3.5. View Mail Events

The 'Mail Events' area contains logs of all actions taken by Mail Gateway. A 'Mail Event' is triggered whenever a mail is filtered for spam or an action is taken for a email with attachment that contains virus or malware.

To view a log of Mail Events

- Click on the results displayed under the 'Infections' or 'Spam' column in the **Summary** screen.



Date	Sender	Subject	From	Location	Type	Malware
05/16/20...	comodo@avli...	[VIRUS: 40e3...	127.0.0.1	/opt/COMOD...	Virus	NetWorr
05/16/20...	comodo@avli...	[VIRUS: 40e8...	127.0.0.1	/opt/COMOD...	Virus	Worm.W
05/16/20...	comodo@avli...	adfa	127.0.0.1	/opt/COMOD...	Virus	TrojWare
05/15/20...	comodo@avli...	adf	127.0.0.1	/opt/COMOD...	Virus	TrojWare
05/15/20...	comodo@avli...	adf	127.0.0.1	/opt/COMOD...	Virus	TrojWare

Column Description

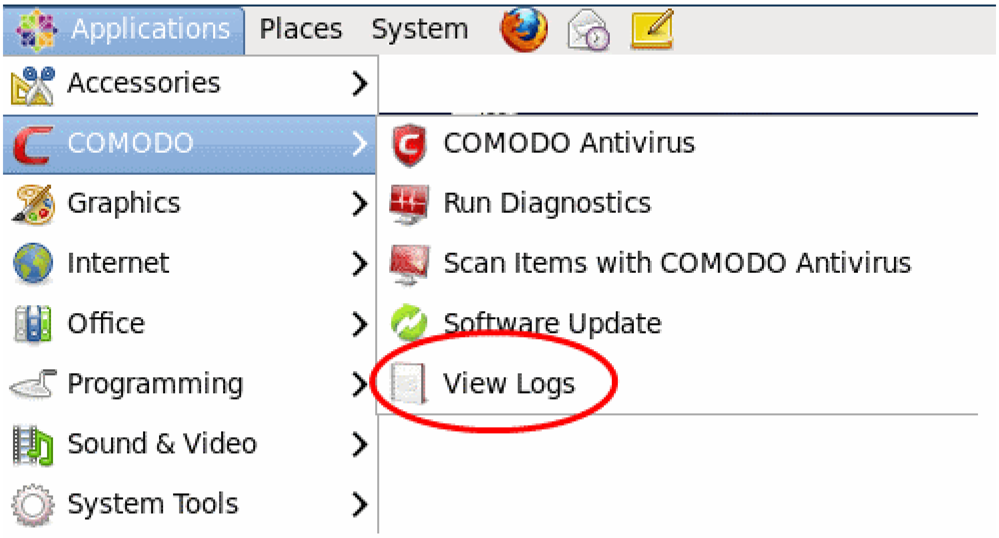
- **Date** - Indicates the date of the event.
- **Sender** - Displays the name of the email sender.
- **Subject** - Displays the subject line of the email.
- **From** - Displays the IP address of the sender.
- **Location** - Indicates the location where the application detected with a threat is stored.
- **Type** - Displays whether mail contains virus or spam.
- **Malware Name** - Name of the malware event that has been detected.
- **Spam -** Indicates the size of spam mail.
- **Action** - Indicates action taken against the malware.
- **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.

Comodo Mail Gateway Log Viewer Module

- Click 'More ...' to load the full Comodo Mail Gateway Log Viewer module.

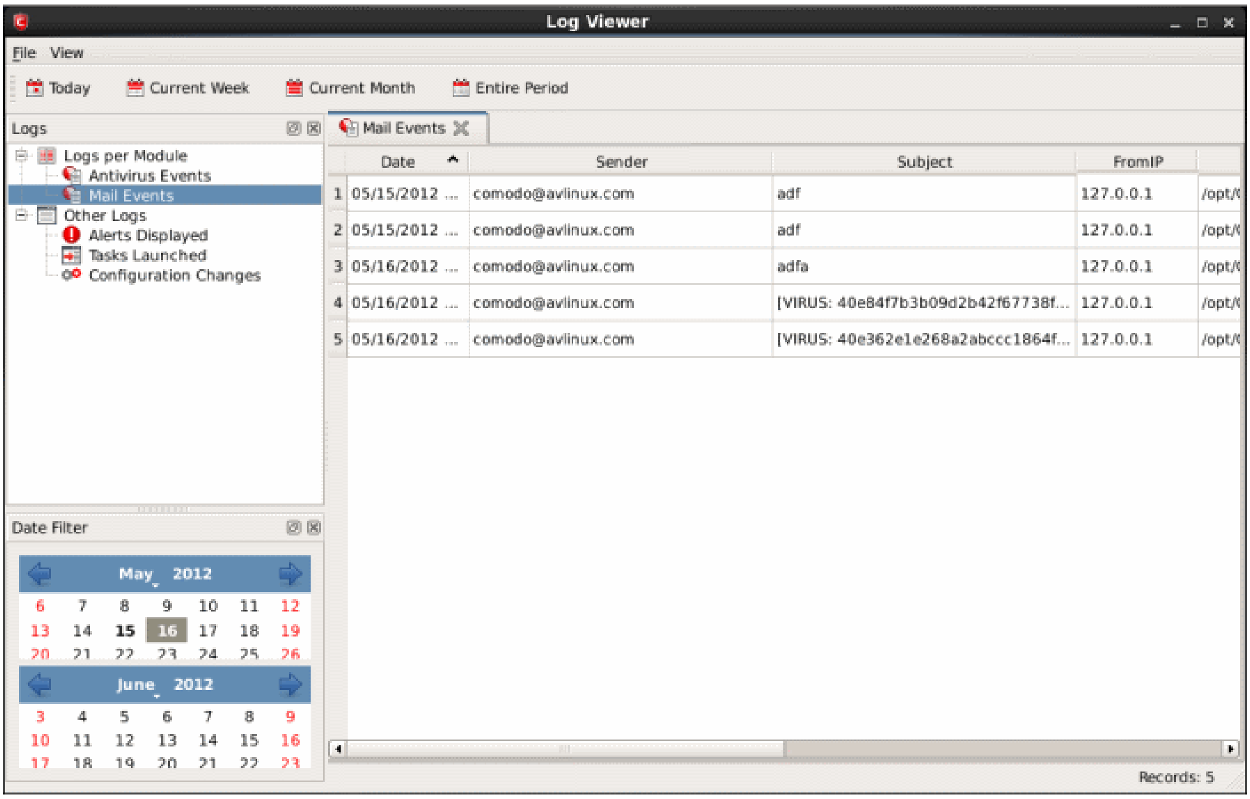
OR

- Click 'View Logs' in the Applications menu in the panel to load the full Log Viewer module.



This window contains a full history of logged events in two categories: Logs per Module and Other Logs.

It also allows you to build custom log files based on **specific filters** and to **export log files** for archiving or troubleshooting purposes.



	Date	Sender	Subject	FromIP	
1	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/
2	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/
3	05/16/2012 ...	comodo@avlinux.com	adfa	127.0.0.1	/opt/
4	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e84f7b3b09d2b42f67738f...	127.0.0.1	/opt/
5	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e362e1e268a2abccc1864f...	127.0.0.1	/opt/

Records: 5

The Log Viewer Module is divided into three sections. The top panel displays a set of handy, predefined time **Filters**. The left panel the types of Logs. The right hand side panel displays the actual events that were logged for the time period you selected in the top panel and the type of log selected in the left panel (or the events that correspond to the filtering criteria you selected).

The Logs per Module option contains the logged events of Antivirus modules and Other Logs options contains logged events of the following:

- **Alerts Displayed:** Displays the list of various alerts that were displayed to the user, the response given by the user to those alerts and other related details of the alert.
- **Tasks Launched:** Displays the various Antivirus tasks such as updates and scans that have taken place. This area will contain a log of all on demand and scheduled AV scans and the result of that scan.

- **Configuration Changes:** Displays a log of all configuration changes made by the user in the CAVL application.

Filtering Log Files

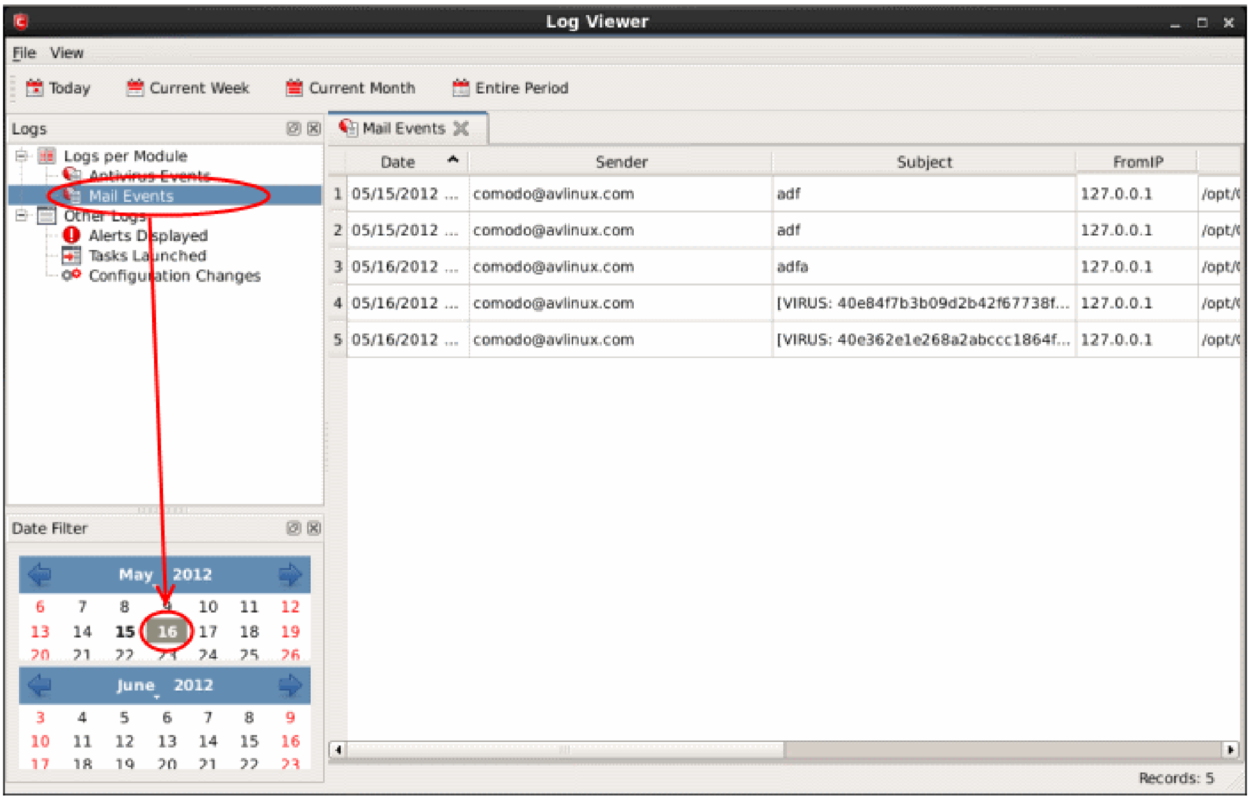
Comodo Antivirus allows you to create custom views of all logged events according to user defined criteria.

Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. (The current week is calculated from Monday to Sunday that holds the current date.)
- **Current Month -** Displays all logged events during the month that holds the current date.
- **Entire Period -** Displays every event logged since CAVL was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).

The example below shows an example display when the Mail Events for 'Today' are displayed.



	Date	Sender	Subject	FromIP	
1	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/(
2	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/(
3	05/16/2012 ...	comodo@avlinux.com	adfa	127.0.0.1	/opt/(
4	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e84f7b3b09d2b42f67738f...	127.0.0.1	/opt/(
5	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e362e1e268a2abccc1864f...	127.0.0.1	/opt/(

Records: 5

Note: The type of events logged by the Antivirus modules of CAVL differ from each other. This means that the information and the columns displayed in the right hand side panel change depending on which type of log you have selected in the top and left hand side panel. For more details on the data shown in the columns, see **View Antivirus Events**.

User Defined Filters:

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. The type of filters available for Mail logs differ to those available for Antivirus logs. The table below provides a summary of available filters and their meanings:

Available Filters - Logs per Module	
Antivirus Filter	**Mail Filters**
Action - Displays events according to the response (or action taken) by the Antivirus	**Sender** - Displays events according to the name of the sender
Location - Displays only the events logged from a specific location	**Subject -** Displays only the events according to the subject in the mail
Malware Name - Displays only the events logged corresponding to a specific malware	**From IP** - Displays only the events with a specific From IP address
Status - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'	**Location** - Displays only the events logged from a specific location
	Type - Displays only the events logged corresponding to specific type of mailware in the mail
	Malware Name - Displays only the events logged corresponding to a specific malware
	Spam - Displays only the events logged corresponding to a specific spam mail
	Action - Displays events according to the response (or action taken) by CAVL
	Status - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

Creating Custom Filters

Custom Filters can be created through the Advanced Filter Interface. You can open the Advanced Filter interface either by using the View option in the menu bar or using the context sensitive menu.

- Click View > Advanced Filter to open the 'Advanced Filter' configuration area.

  Or

- Right click on any event and select 'Advanced Filter' option to open the corresponding configuration area.

The 'Advanced Filter' configuration area is displayed in the top half of the interface whilst the lower half displays the Events, Alerts, Tasks or Configuration Changes that the user has selected from the upper left pane. If you wish to view and filter event logs for other modules then simply click log name in the tree on the upper left hand pane.

The Advanced Log filter displays different fields and options depending on the log type chosen from the left hand pane (Antivirus, Mail).

This section will deal with Advanced Event Filters related to 'Mail Events' and will also cover the custom filtering that can be applied to the 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes'). The Antivirus Advanced Event Filters is dealt in the respective section.

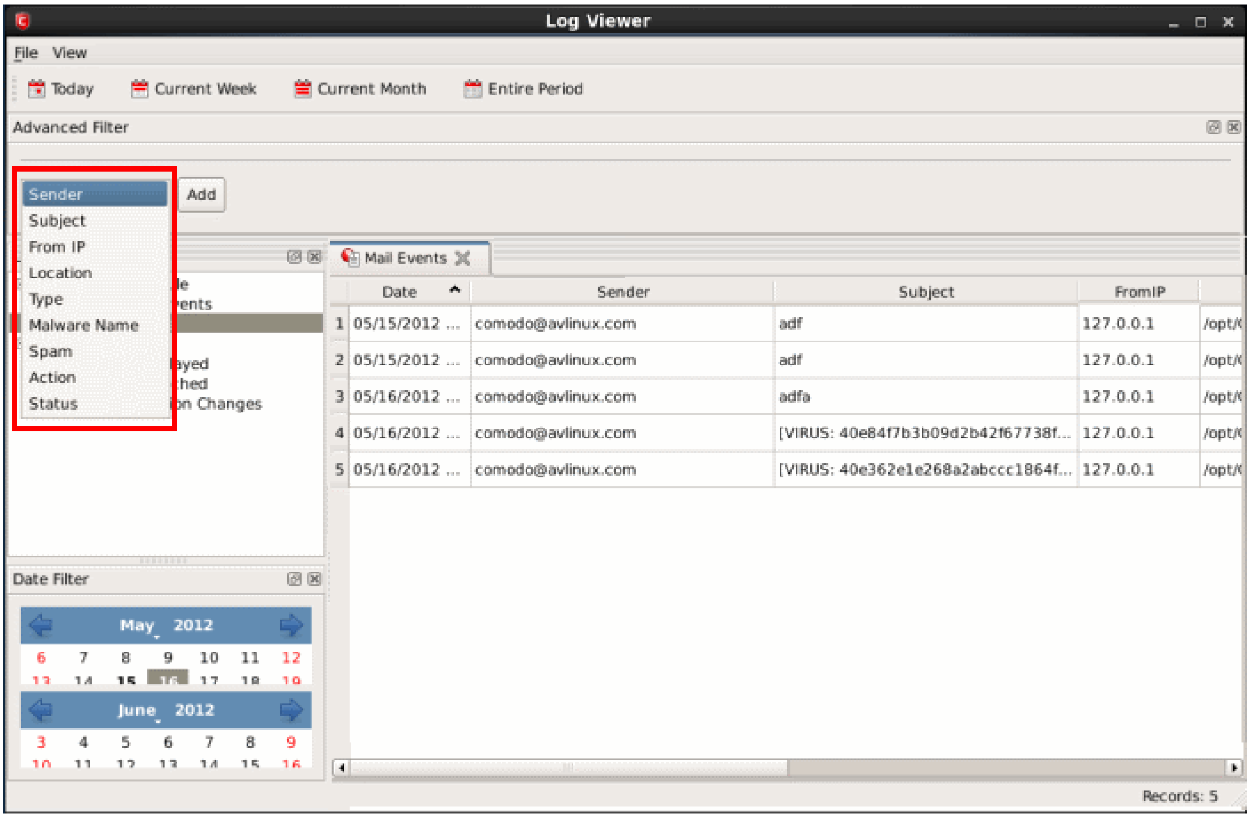
Mail Events - Advanced Filters

To configure Advanced Filters for Mail events

1. Select 'View > Advanced Filter'
2. Select 'Mail Events' under 'Logs Per Module'

You have 9 categories of filter that 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.

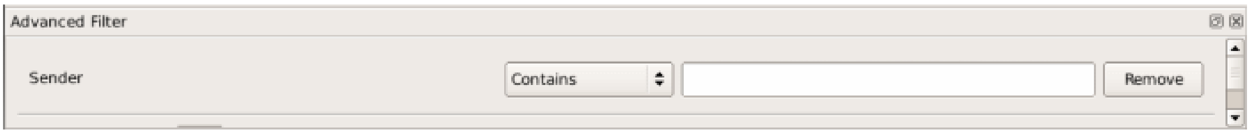
3. Click the 'Add' button when you have chosen the category upon which you wish to filter.



	Date	Sender	Subject	FromIP	
1	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/(
2	05/15/2012 ...	comodo@avlinux.com	adf	127.0.0.1	/opt/(
3	05/16/2012 ...	comodo@avlinux.com	adfa	127.0.0.1	/opt/(
4	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e84f7b3b09d2b42f67738f...	127.0.0.1	/opt/(
5	05/16/2012 ...	comodo@avlinux.com	[VIRUS: 40e362e1e268a2abccc1864f...	127.0.0.1	/opt/(

Following are the options available in the 'Add' drop-down:

i. **Sender:** Selecting the 'Sender' option displays a drop-down field and text entry field.



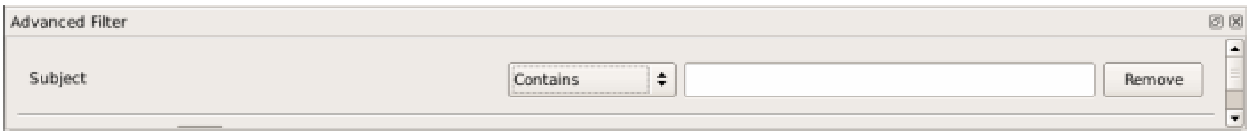
a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

For example, if you select 'Contains' option from the drop-down field and enter the word 'john' in the text field, then all events containing the word 'john' in the Sender field will be displayed directly underneath. If you select 'Does Not Contain' option from the drop-down field and enter the word 'Borg' in the text field, then all events that do not have the word 'Borg' will be displayed directly underneath.

ii. **Subject:** Selecting the 'Subject' option displays a drop-down field and text entry field.



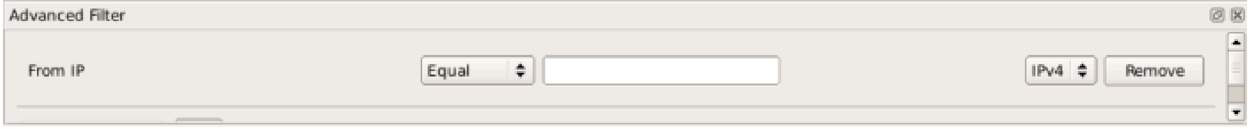
a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Sender' option for better understanding.

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



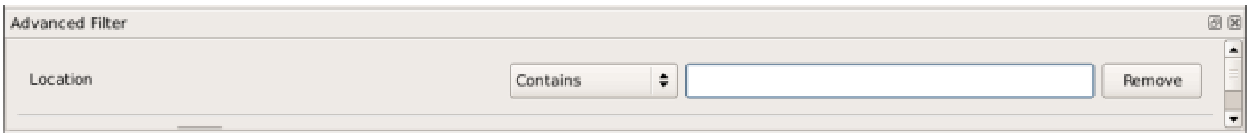
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Select 'IPv4' or 'IPv6' from the drop-down box.

c) Enter the sender's IP address that needs to be filtered.

The filtered entries are shown directly underneath.

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



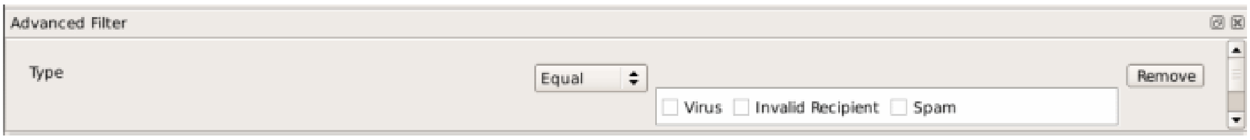
a) Select 'Contains' or 'Does Not Contain' option from the drop-down box.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Sender' option for better understanding.

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

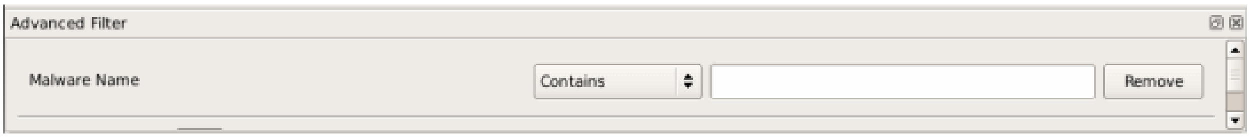


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- **Virus** - Displays mails that contain virus
- **Invalid Recipient** - Displays mails that were addressed to invalid recipients
- **Spam** - Displays spam mails

vi. **Malware Name:** Selecting the 'Malware' option displays a drop-down box and text entry field.



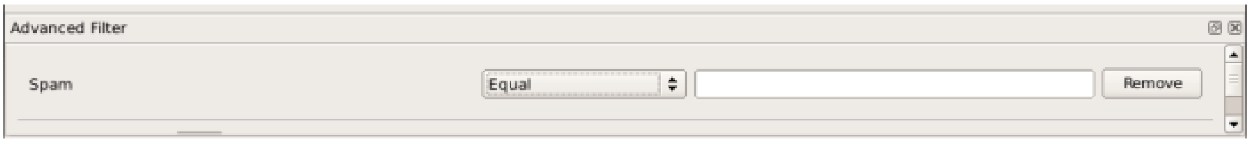
a) Select 'Contains' or 'Does Not Contain' option from the drop-down box.

b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Sender' option for better understanding.

vii. **Spam:** Selecting the 'Spam' option displays a drop-down box and text entry field.

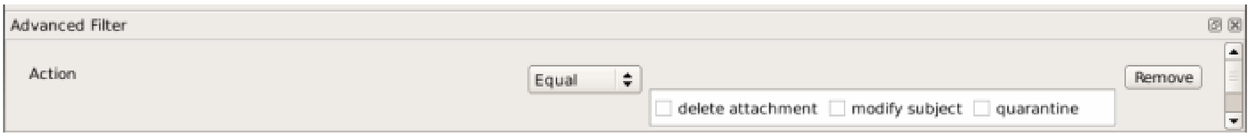


a) Select one of the options in the drop-down box: 'Equal', 'Greater than', 'Greater than or Equal', 'Less than', 'Less than or Equal' or 'Not Equal'.

b) Now enter the size in MB of the spam mail in the field.

The filtered entries are shown directly underneath.

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



a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

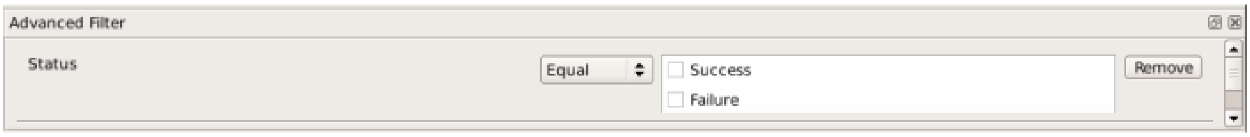
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- **Delete Attachment:** Displays events where the mail attachment with virus was deleted
- **Modify Subject:** Displays events where the subject line of the mail was modified
- **Quarantine:** Displays events where the mail was quarantined

The filtered entries are shown directly underneath.

For example, if you checked the 'Quarantine' box then selected 'Equal', you would see only those Events where the mails were quarantined.

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



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:

- **Success:** Displays Events that successfully executed (for example, the mail was successfully quarantined)
- **Failure:** Displays Events that failed to execute (for example, the spam mail was not quarantined)

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Sender' option for better understanding.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, the option to select the next filter type automatically appears. You can also remove a filter type by clicking the 'Remove' option at the end of every filter option.

Other Logs - Advanced Filters

Refer to Antivirus Tasks-Introduction > View Antivirus Events > Log Viewer > Creating Custom Filters > **Other Logs – Advanced Filters** for the process of Creating Custom Filters for Alerts Displayed, Task Launched and Configuration Changes.

Date Filter

Click here to know more about Date Filter functionality.

Exporting Log Files to HTML

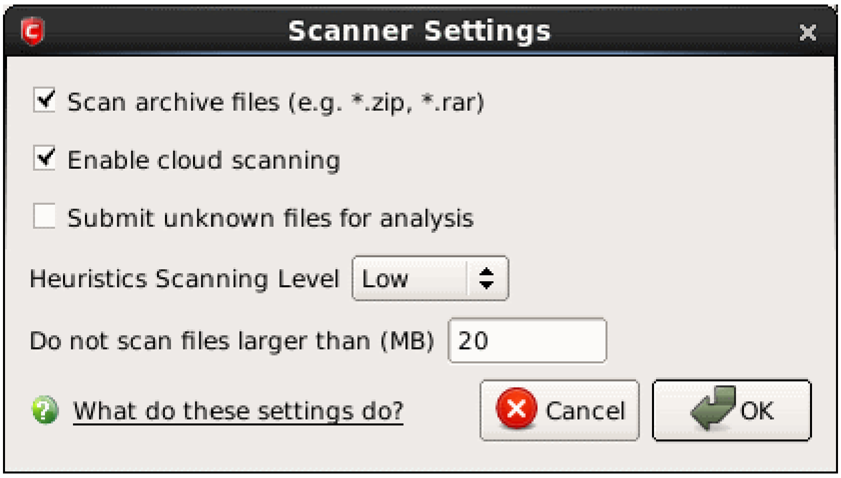
Click here to know more about exporting log files to HTML.

3.6. Scanner Settings

The Scanner Settings interface in Mail Gateway allows you to configure the settings to scan email attachments such as .zip, and .rar files, enable cloud scanning of suspicious emails and submit unknown files for analysis to Comodo.

To configure scanner settings

- Click 'Scanner Settings' from the Mail Gateway tab in the main interface.



☑ Scan archive files (e.g. *.zip, *.rar)

☑ Enable cloud scanning

□ Submit unknown files for analysis

Heuristics Scanning Level: Low

Do not scan files larger than (MB): 20

- **Scan archive files (e.g. *Zip, *.rar)** - Select this box for the Antispam to scan archive files.
- **Enable cloud scanning** - Select this box and Antispam will upload files or file's feature to Comodo server, and scan these files on server.
- **Submit unknown files for analysis** - Select this box and files which are identified as 'unknown' i.e. the files are neither in the safe-list or black list, from the cloud based scanning to Comodo for analysis.
- **Heuristics Scanning Level -** Select a level for Heuristics Scanning.

  Comodo AntiVirus employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

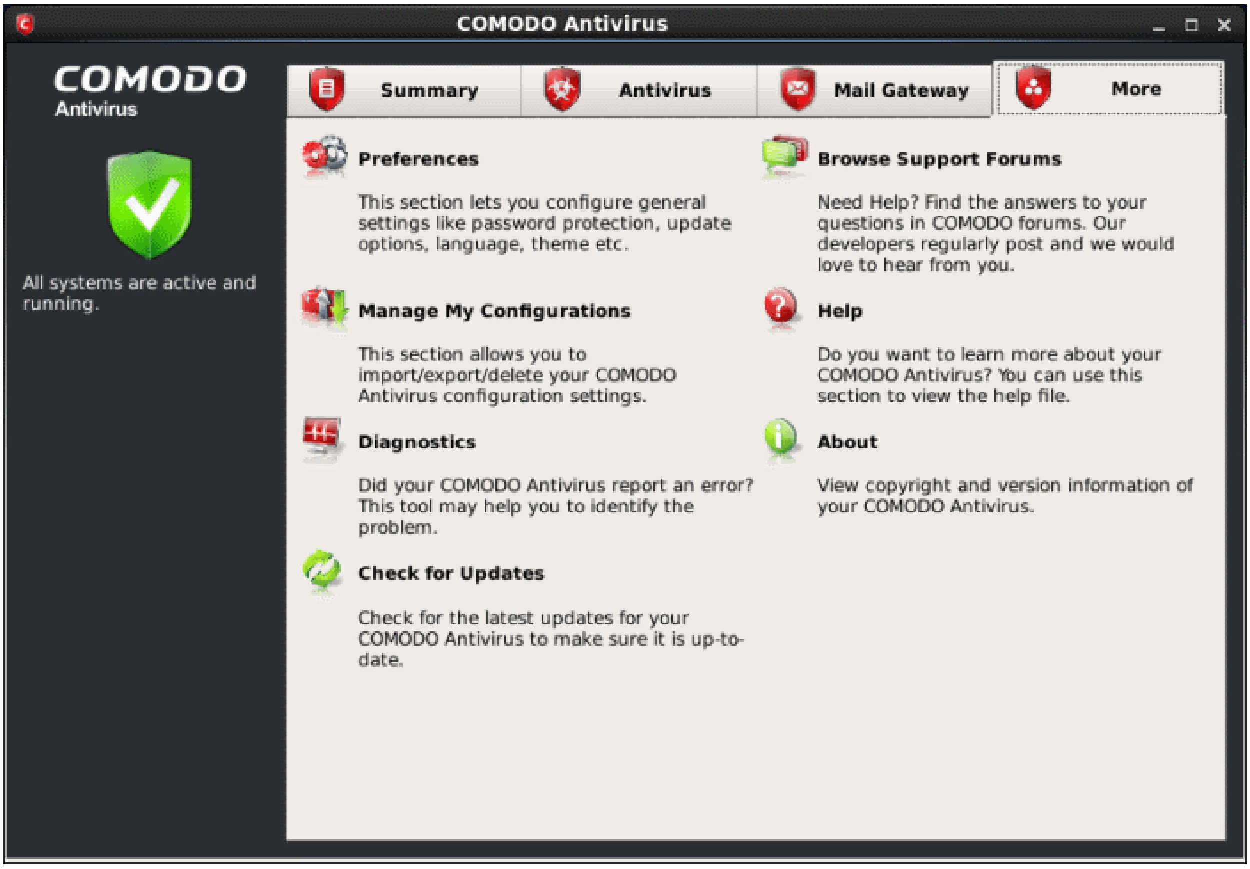
  The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

  - **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
  - **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives**.** This setting combines an extremely high level of security and 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 the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Do not scan files larger than -** This box allows you to set a maximum size (in MB) for the individual files to be scanned. Files larger than the size specified here, are not scanned.

4. More Options – Introduction

The **More Options** interface contains several areas relating to overall configuration as well as handy utilities and shortcuts to help enhance and improve your experience with CAVL.

It can be accessed at all times by clicking on the 'More' tab from the main interface.



COMODO Antivirus

COMODO Antivirus

All systems are active and running.

Preferences

This section lets you configure general settings like password protection, update options, language, theme etc.

Browse Support Forums

Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.

Manage My Configurations

This section allows you to import/export/delete your COMODO Antivirus configuration settings.

Help

Do you want to learn more about your COMODO Antivirus? You can use this section to view the help file.

Diagnostics

Did your COMODO Antivirus report an error? This tool may help you to identify the problem.

About

View copyright and version information of your COMODO Antivirus.

Check for Updates

Check for the latest updates for your COMODO Antivirus to make sure it is up-to-date.

Click the links below to see detailed explanations of each area in this section.

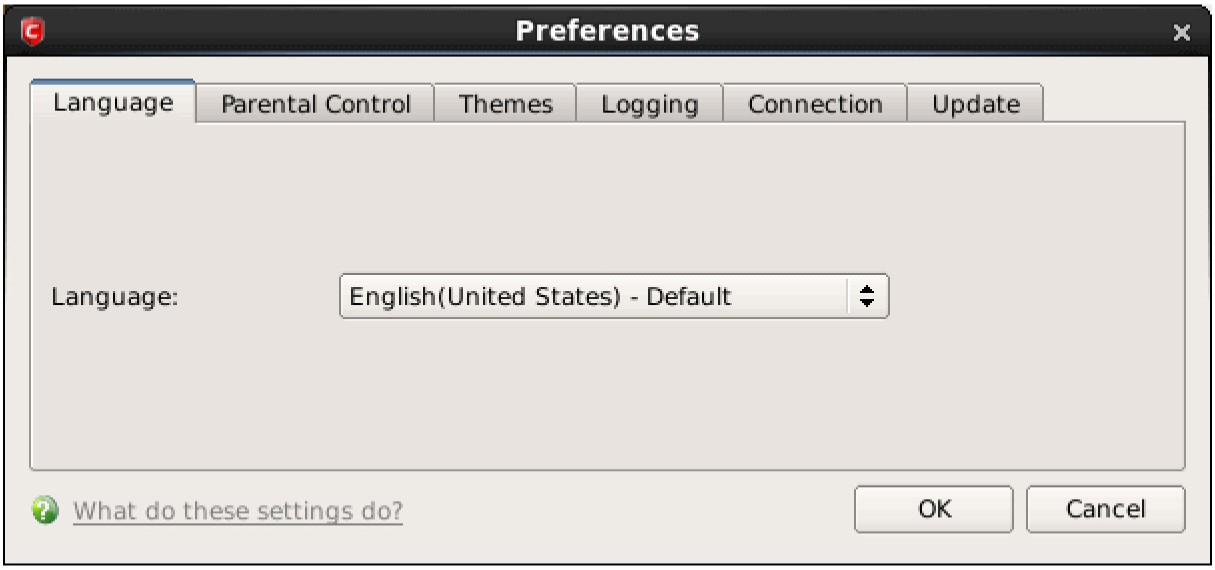
- **Preferences:** Allows the user to configure general CAVL settings (password protection, update options, language, theme and so on.)
- **Manage My Configurations:** Allows the user to manage, import and export their CAV configuration profile.
- **Diagnostics:** Helps to identify any problems with your installation.
- **Check For Updates:** Launches the CAVL updater.
- **Browse Support Forums:** Links to Comodo User Forums.
- **Help:** Launches the online help guide.
- **About:** Displays version and copy-right information about the product.

4.1. Preferences

The **Preferences** menu in **More** section allows you to configure various options related to the operation of CAVL.

To open Preferences dialog box

- Click 'Preferences' in 'More' screen.



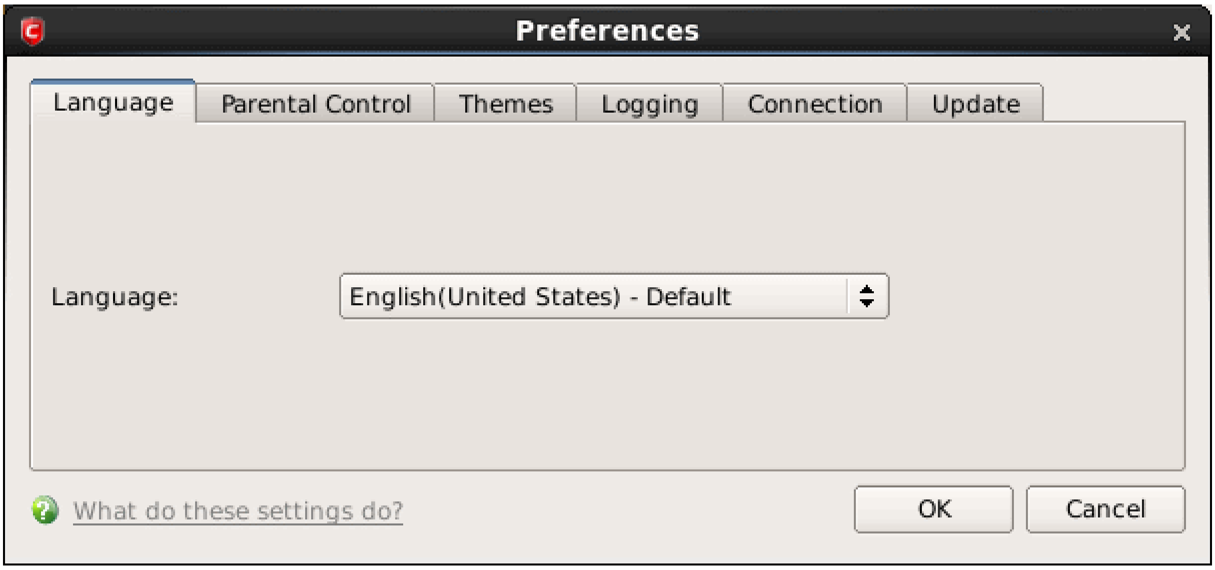
Language: English(United States) - Default

It has the following tabs to make your settings:

- Language
- Parental Control
- Themes
- Logging
- Connection
- Update

4.1.1. Language

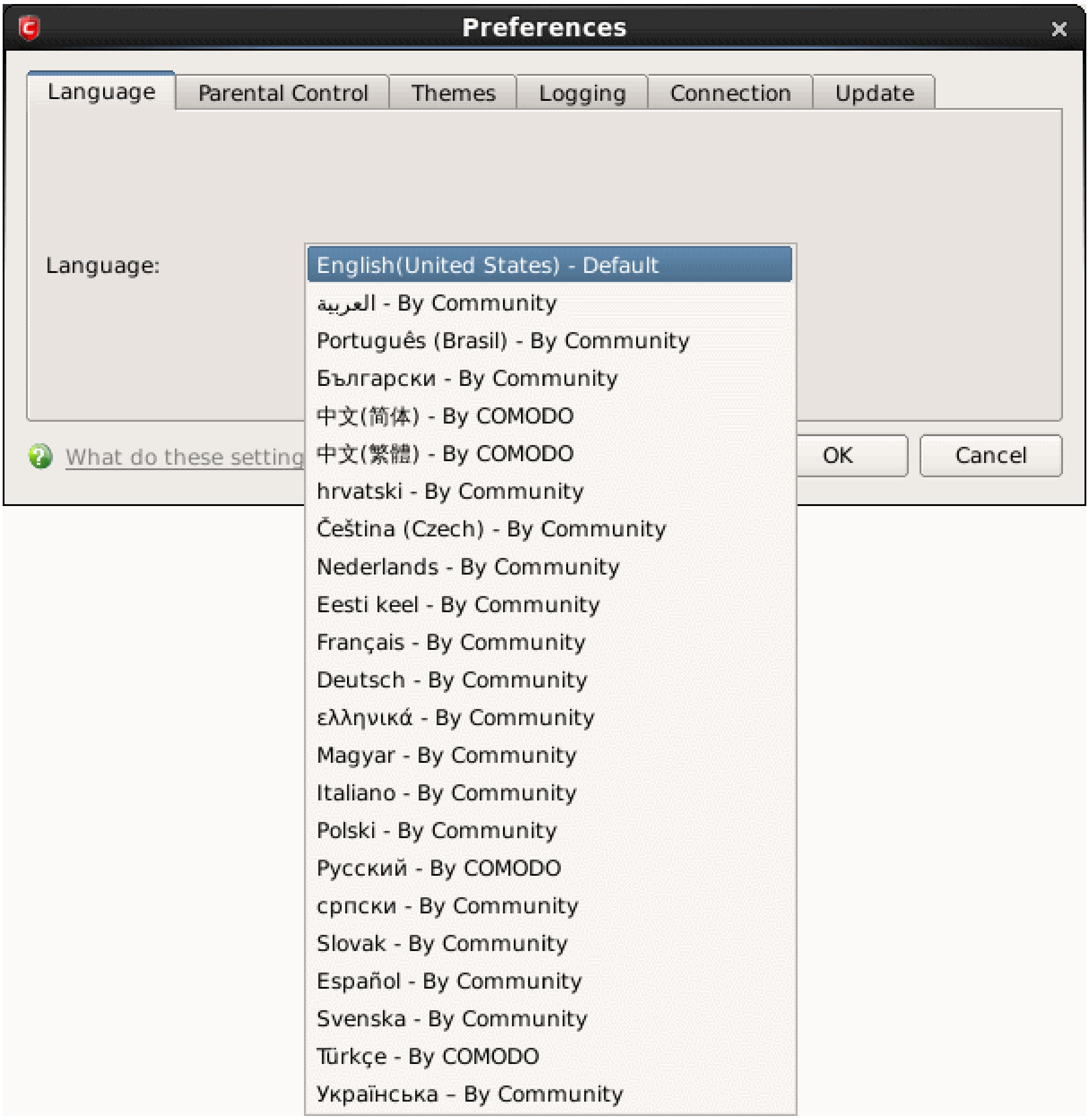
The Language tab allows you to choose the interface language and customize the look and feel of CAVL according to your preferences. Use the drop-down menu to switch between installed themes.



Language: English(United States) - Default

Language Settings

Comodo Antivirus is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu ***(Default = English (United States))***.

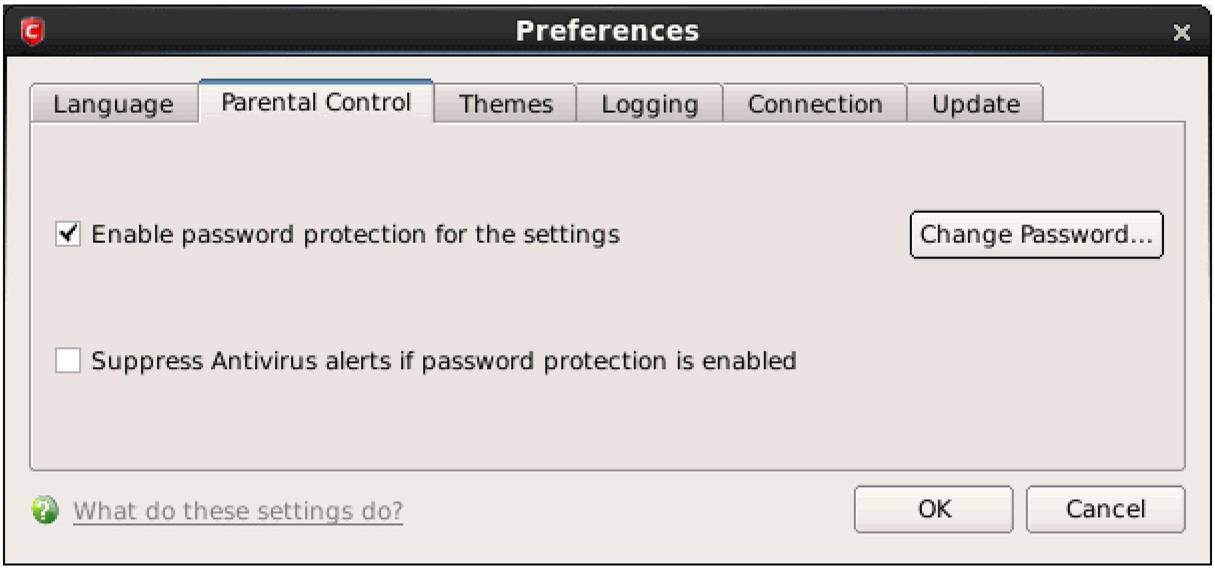


Language: English(United States) - Default

In order for your language to take effect, you must restart the CAVL application.

4.1.2. Parental Control Settings

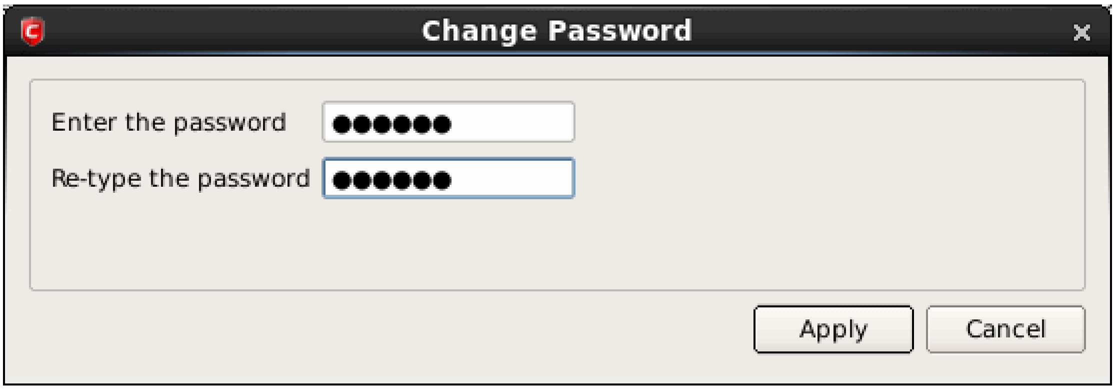
The 'Parental Control' tab allows you to configure password protection for CAVL.



☑ Enable password protection for the settings

□ Suppress Antivirus alerts if password protection is enabled

- **Enable password protection for settings** - Selecting this option activates password protection for all important configuration sections and wizards within the interface. If you choose this option, you must first specify and confirm a password by clicking the 'Change Password... ' button. You are asked for this password every time you try to access important configuration areas (**Antivirus** and **Mail Gateway** Tasks area require this password before allowing you to view or modify their settings).



Enter the password ●●●●●●

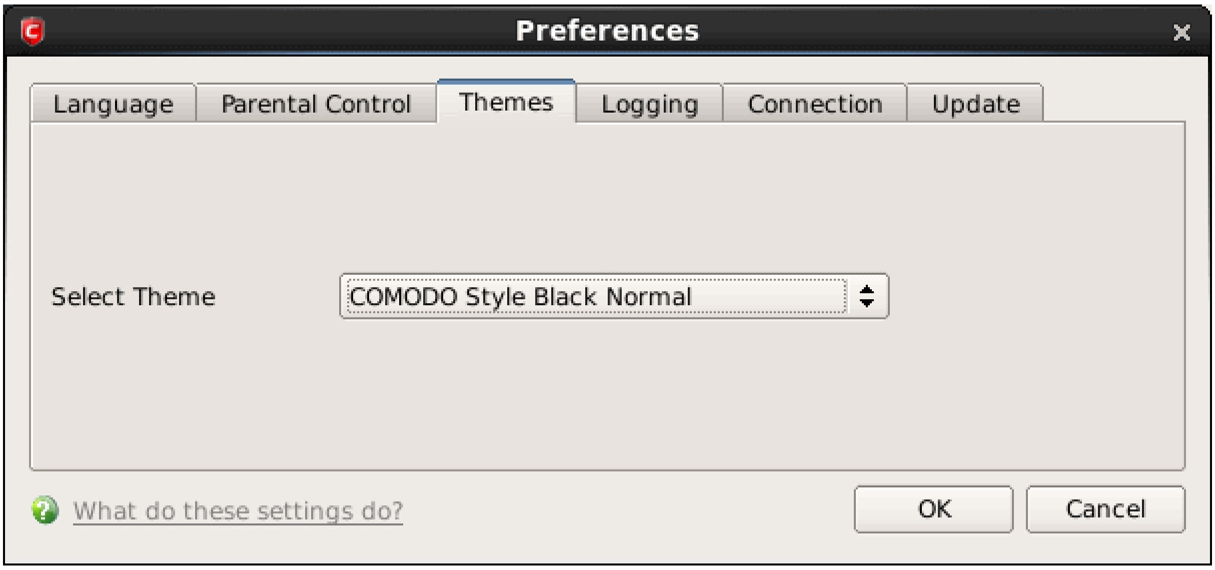
Re-type the password ●●●●●●

This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats.

- **Suppress Antivirus alerts when password protection is enabled** - If selected, no Antivirus Alerts are displayed when password protection is enabled. Parents and network admins may want to enable this setting if they do not want users to be made aware when an Antivirus alert has been triggered. For example, a virus program may be attempting to copy itself and infect user's computer without permission or knowledge of the user. Usually, the Antivirus would generate an alert and ask the user how to proceed. If that user is a child or an inexperienced user then they may unwittingly click 'allow' just to 'get rid' of the alert and/or gain access to the website in question - thus exposing the machine to attack. Selecting this option blocks the activity of the virus but does not generate an alert.

4.1.3. Themes

The Themes tab allows you to customize the look and feel of CAVL according to your preferences. Use the drop-down menu to switch between installed themes.



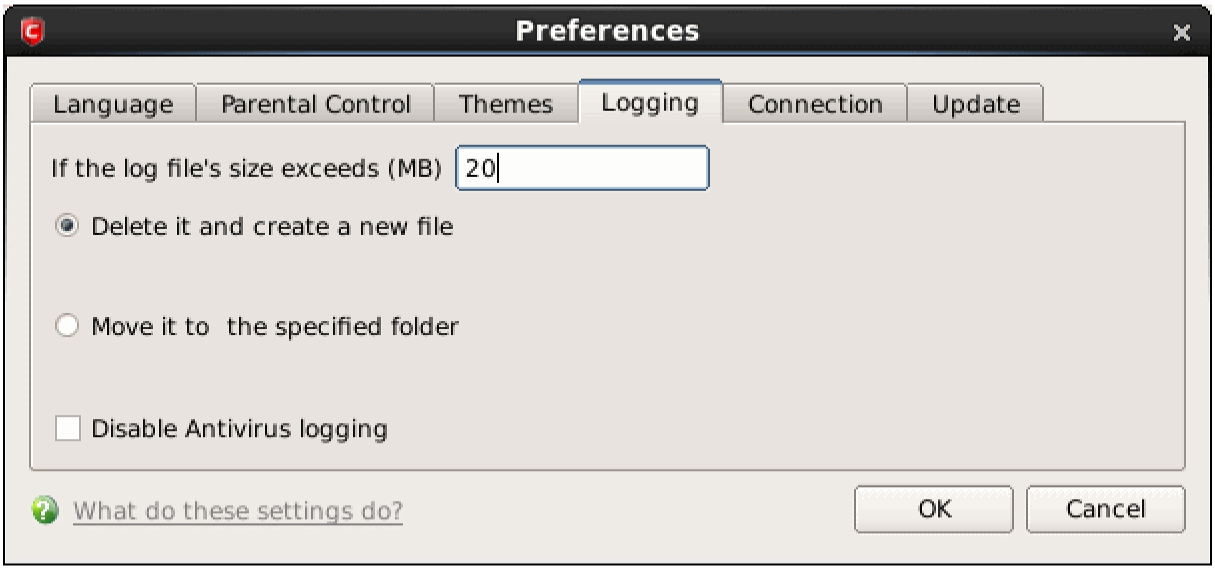
Select Theme: COMODO Style Black Normal

In order for your theme choices to take effect, you must restart the CAVL application.

4.1.4. Log Settings

By default, CAVL maintains a log of all the Antivirus and Mail events, which can be accessible by clicking 'View Antivirus Events' from the Antivirus Tasks interface.

The 'Logging' tab of the 'Preferences' interface allows you to configure how CAVL should behave once this log file reaches a certain size and also allows you to disable the logging of specific types of event.



If the log file's size exceeds (MB): 20

● Delete it and create a new file

○ Move it to the specified folder

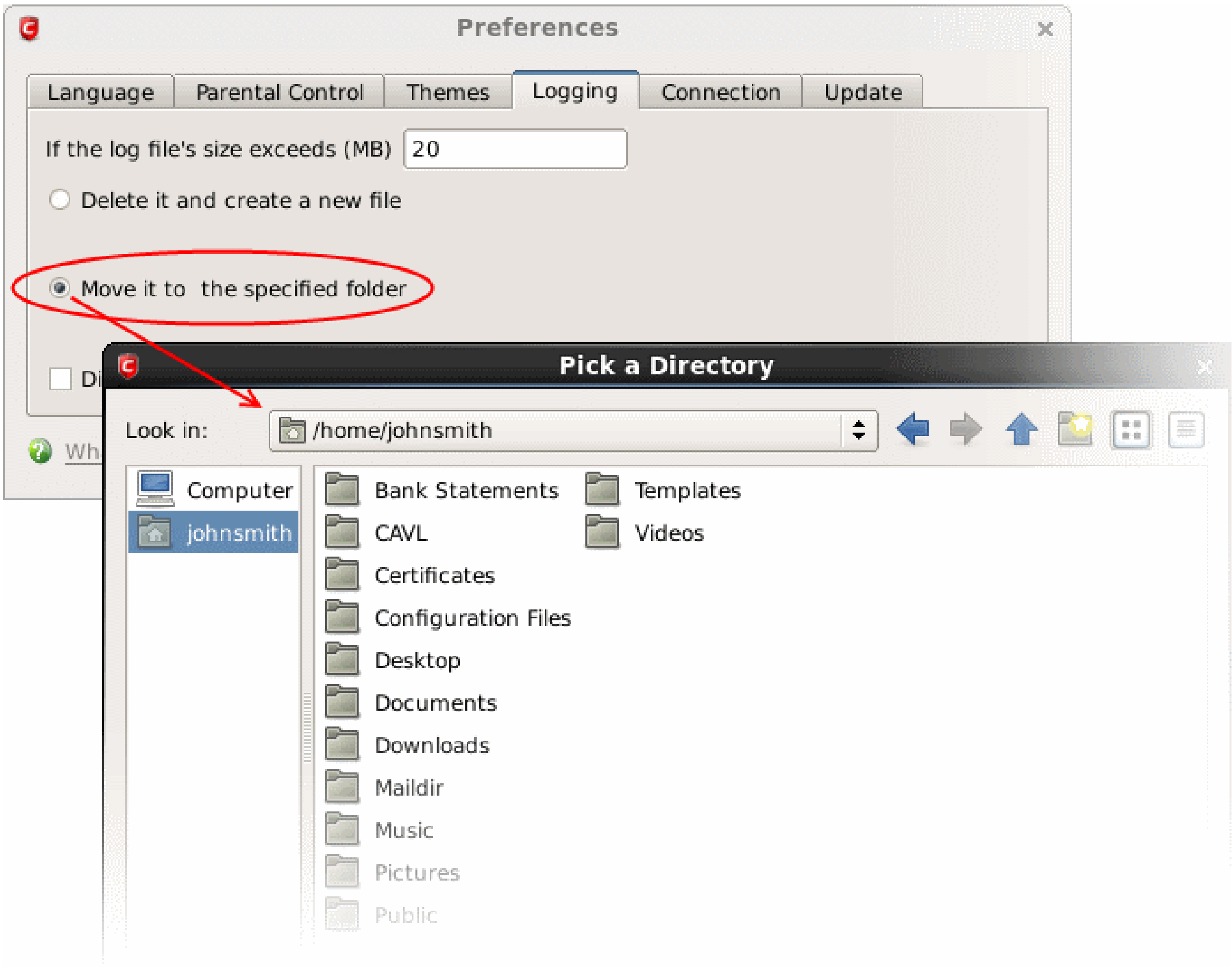
□ Disable Antivirus logging

If the log file's size exceeds (MB): Enables you to configure for deleting or moving the log file if it reaches a specified size in MB. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.

- Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' ***(Default = 20MB).***

If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new file'.** Once the log file reaches the maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant ***(Default = Enabled).***

If you want to save the log file even if it reaches the maximum size, select **'Move it to the specified folder'** and select a destination folder for the log file ***(Default = Disabled).***



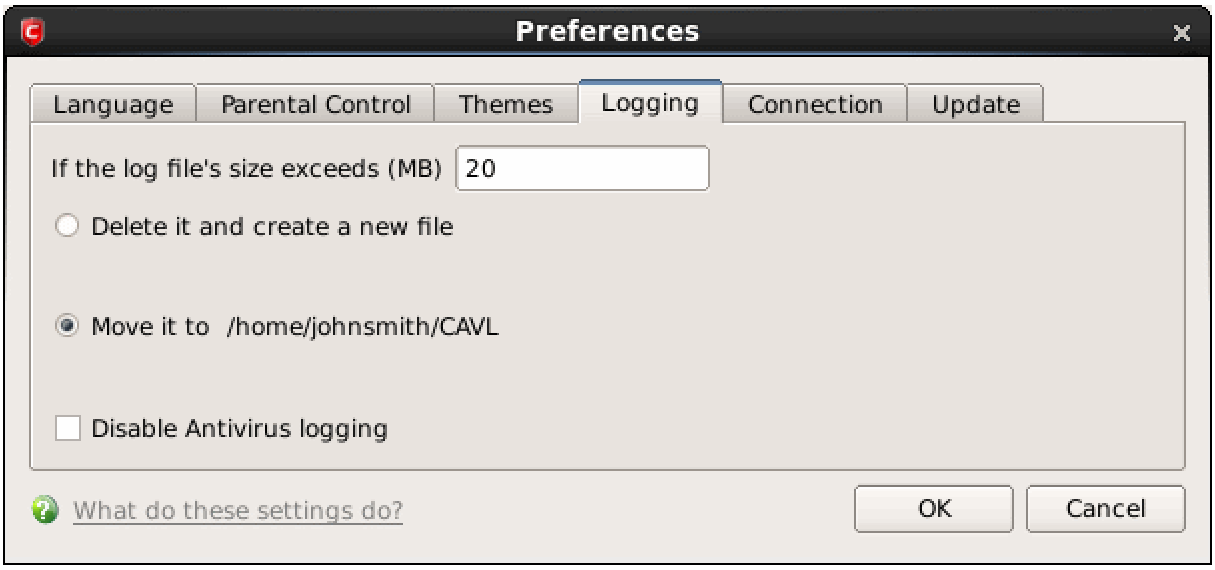
If the log file's size exceeds (MB) 20

○ Delete it and create a new file

● Move it to the specified folder

Look in: /home/johnsmith

The selected folder path will appear beside 'Move it to'.



If the log file's size exceeds (MB) 20

○ Delete it and create a new file

● Move it to /home/johnsmith/CAVL

□ Disable Antivirus logging

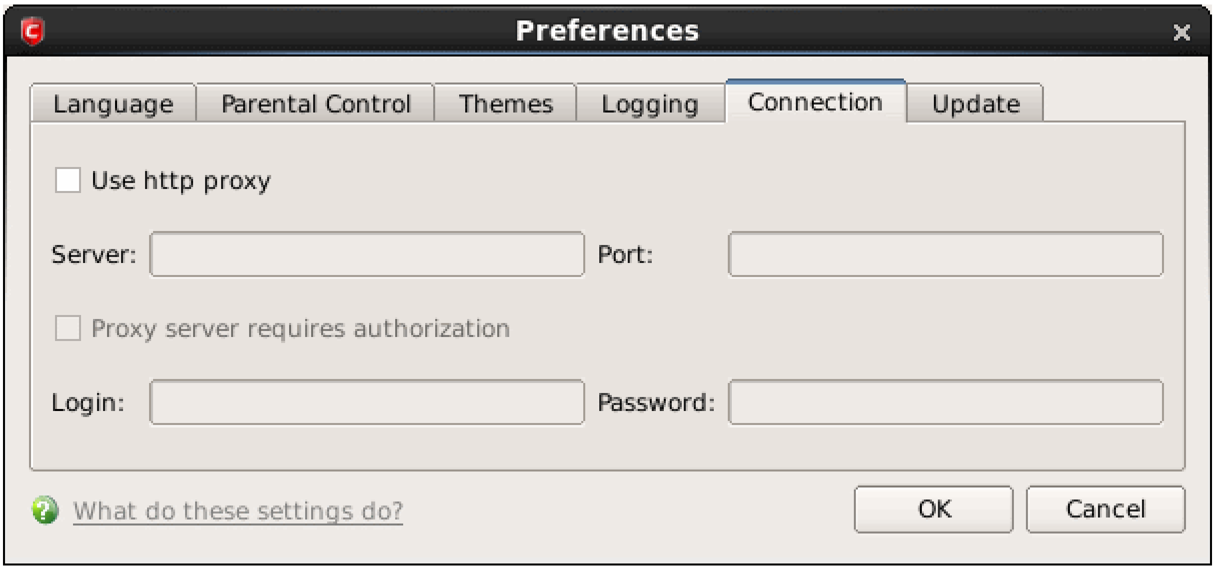
Check Boxes:

The check boxes allow you to disable logging of events according to your preferences.

- **Disable Antivirus logging** – Instructs Comodo Antivirus to not to log Antivirus events ***(Default = Disabled).***

4.1.5. Connection Settings

The Connection tab allows you to configure how CAVL should connect to Comodo servers for receiving program updates etc. If you are using a Proxy server in your network and if you want CAVL to use the Proxy Server, the Proxy settings can be configured through this settings interface.



□ Use http proxy

Server: Port:

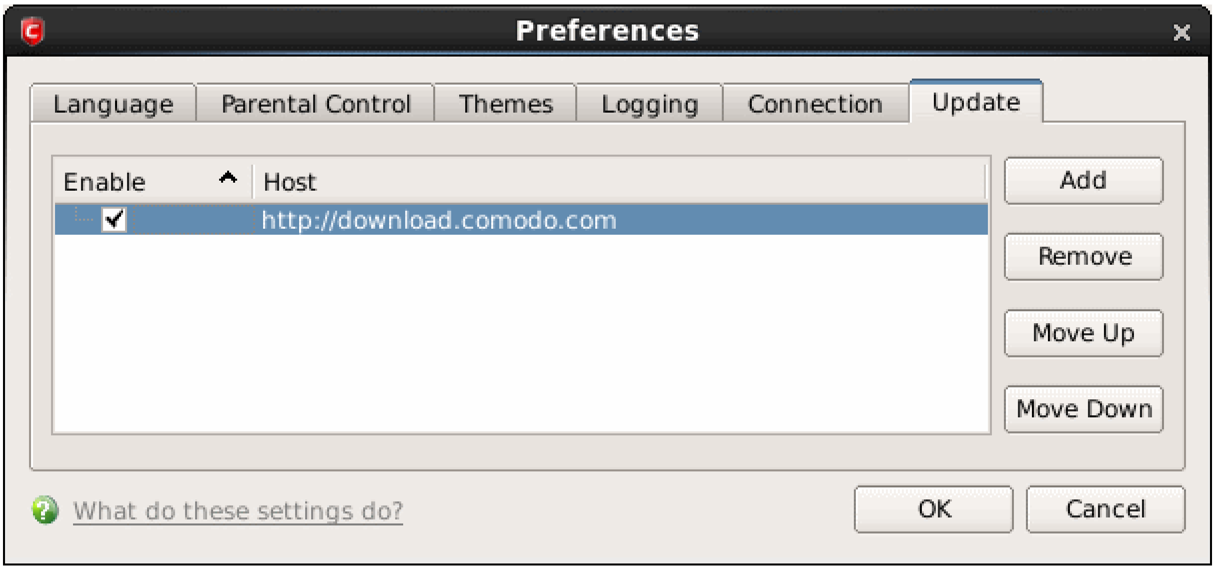
□ Proxy server requires authorization

Login: Password:

- Select **'Use http proxy'** if you want CAVL to use the Proxy Server. Enter the proxy server IP address or name in the 'Server' text box and enter the port number in the 'Port' text box ***(Default = Disabled)***.
- If your Proxy Server needs authentication, Select **'Proxy server requires authorization'**. Type your Login ID in the 'Login' text box and enter the password in the 'Password' text box ***(Default = Disabled).***

4.1.6. Update Settings

The Update tab allows you enable/disable the CAVL program updates and to select the host from which the updates are to be downloaded. By default, the URL of the Comodo Server is entered as an available host.



Enable	Host
☑	http://download.comodo.com

- If you want to download the updates always from the Comodo servers, you can leave the setting as it is (***Default = Enabled)***.
- If you are connected to a local network and the CAVL program updates are available at an HTTP Server or at any of the other computers in your network running Comodo Offline Updater, you can add the computers as hosts in this area.
- To add a host click 'Add' and enter the URL or IP address of the host in the next row that appears.

- Repeat the process for adding multiple hosts.
- Select the host by using the Move Up and Move Down buttons.
- CAVL will automatically check the host specified here and download the updates from the host even when you are offline.
- Click 'OK' for your settings to take effect.

Note: CAVL program updates can also be checked manually. Click More Options > Check For Updates if you wish to update manually. **Click here** to view the section of this guide on manual updates.

4.2. Manage My Configurations

CAVL allows you to maintain, save and export multiple configurations of your security settings. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple computers. If you are upgrading your system and there is a need to un-install and re-install CAVL, you can export your configuration settings to a safe place before un-installation. After re-installation, you can import the configuration settings to take effect in your newly installed CAVL.

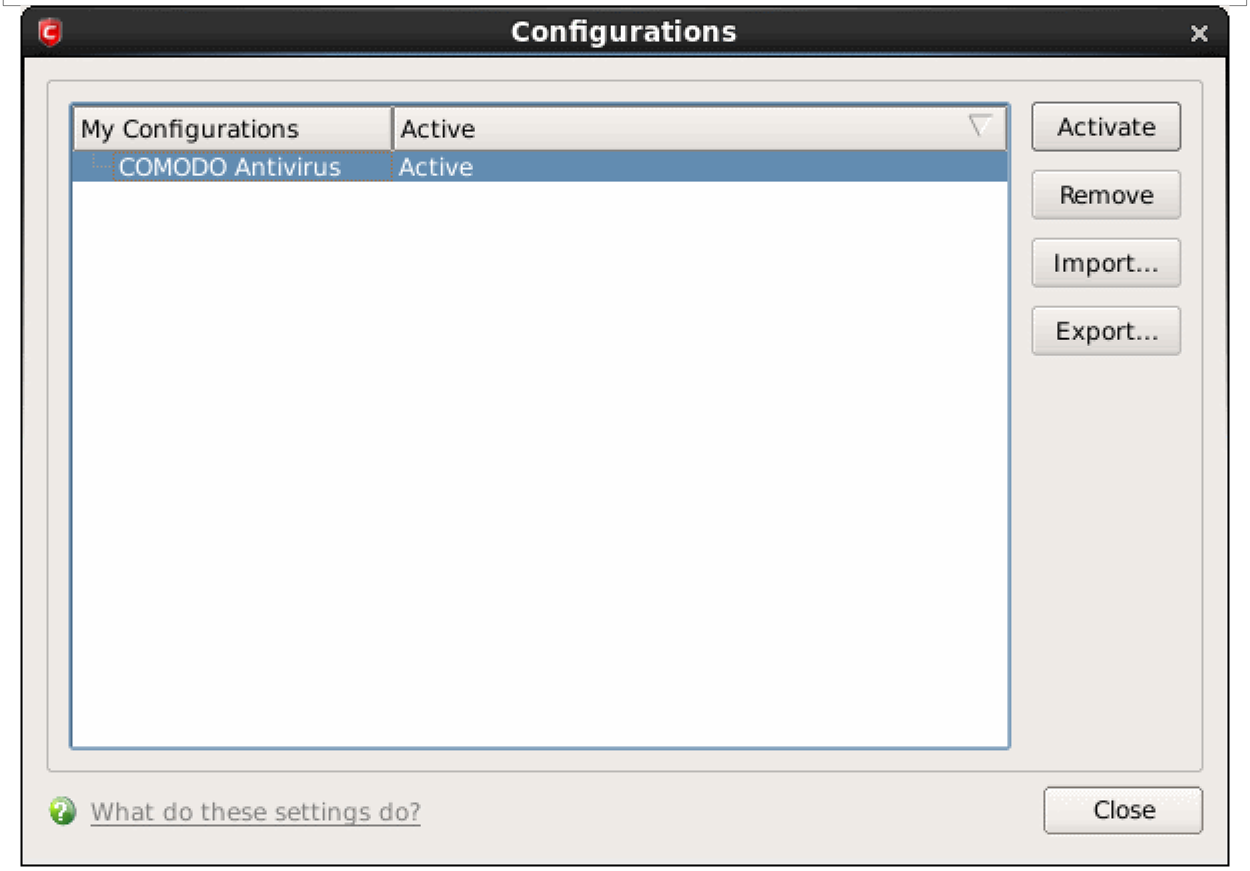
This feature is also a great time saver for anyone with more than one computer because it allows you to quickly implement your security settings on other computers that you own without having to manually re-configure them. Click on the link given below for details on preset configuration and custom configuration.

- **Comodo Preset Configurations**
- **Importing/Exporting and Managing Personal Configurations**

4.2.1. Comodo Preset Configuration

CAVL ships with a preset configuration, Comodo Antivirus, that strike a good balance between security and usability. The profile that is currently in use is the 'Active' profile.

Important Note: Any changes you make to settings over the course of time are recorded in (and will update) the 'active' profile. Exporting the active profile will, therefore, export your settings as they currently stand.



My Configurations	Active
COMODO Antivirus	Active

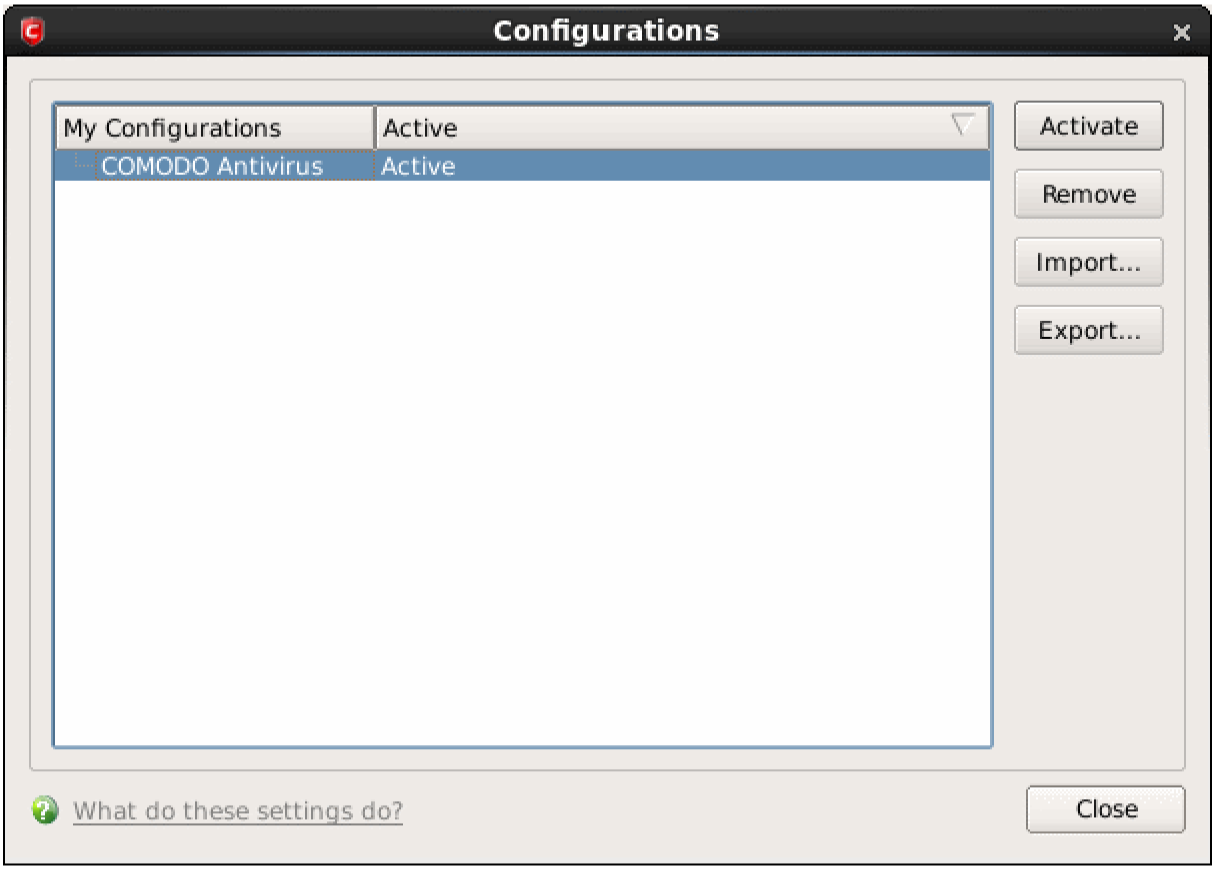
Before modification, the 'Comodo Antivirus' profile has the following default settings:

- Logging - ON
- Max. Log File Size - 20 MB
- Do not scan files larger than - 20 MB
- Real Time Scanning - Stateful
- Automatically update virus database (Real Time Scanning) - ON
- Automatically update virus database before scanning - ON
- Enable Cloud Scanning (Manual Scanning) - ON

4.2.2. Importing/Exporting and Managing Personal Configurations

To access Configuration interface

1. Navigate to 'More > Manage My Configurations



My Configurations	Active
COMODO Antivirus	Active

The interface the following preset configuration

- Comodo Antivirus

The currently active configuration is indicated as 'Active' in this interface.

2. Click the area on which you would like more information:

- **Export my configuration to a file**
- **Import a saved configuration from a file**

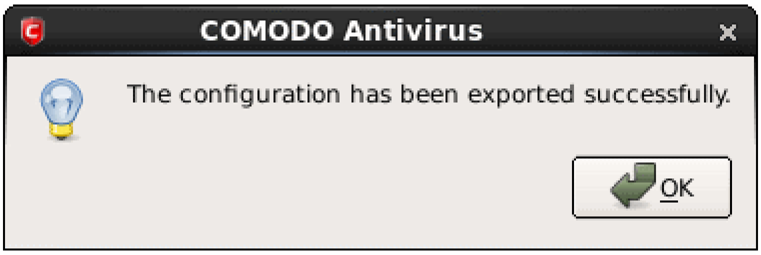
- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

Export my configuration to a file

To export your currently active configuration

1. Click the 'Export' button.
2. Type a file name for the profile (e.g. 'My CAV Profile') and save to the location of your choice.

A confirmation dialog appears for the successful export of the configuration.



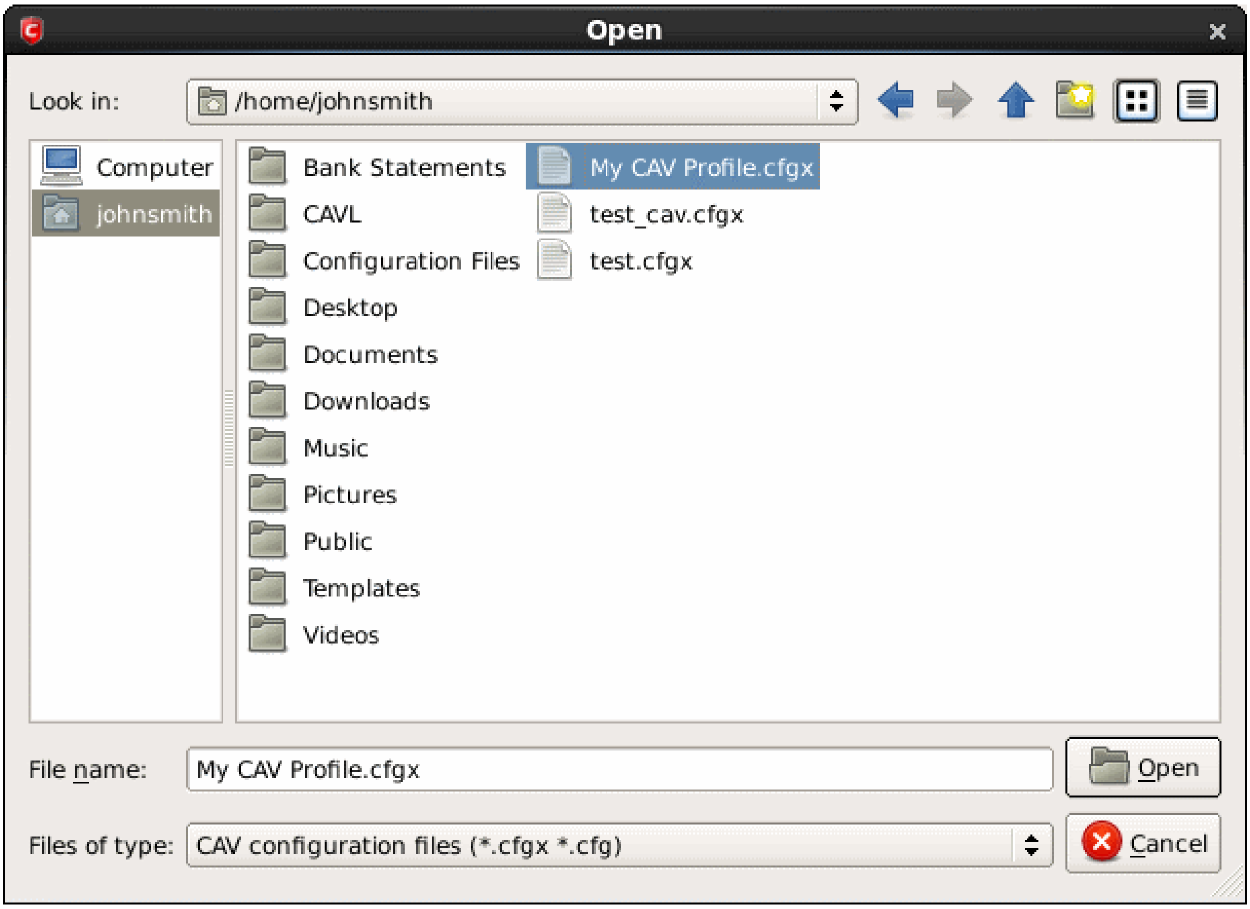
The configuration has been exported successfully.

Import a saved configuration from a file

Importing a configuration profile allows you to store any profile within Comodo Antivirus. Any profiles you import do not become active until you **select them for use**.

To import a profile

1. Click the 'Import' button.
2. Browse to the location of the saved profile and click 'Open'.



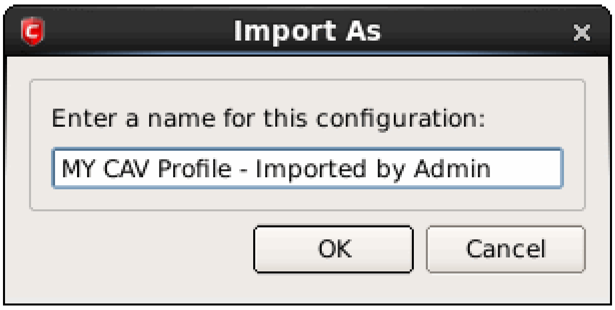
Look in: /home/johnsmith

My CAV Profile.cfgx

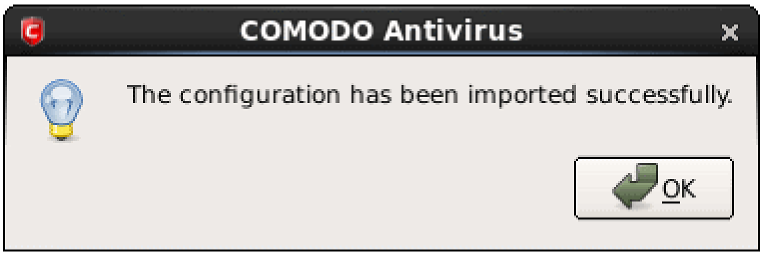
File name: My CAV Profile.cfgx

Files of type: CAV configuration files (*.cfgx *.cfg)

3. In the 'Import As' dialog that appears, assign a name for the profile you wish to import and click 'Ok'.

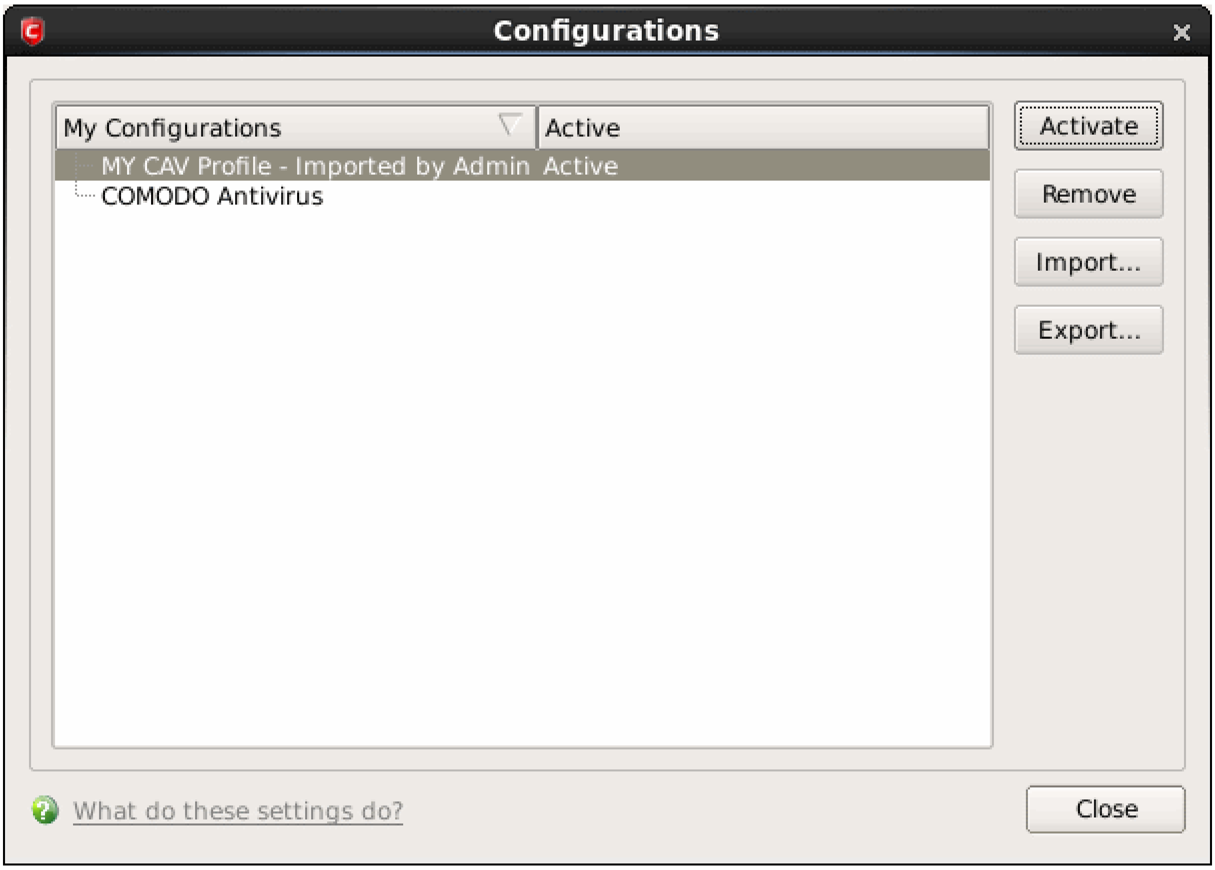

Import As
Enter a name for this configuration:
MY CAV Profile - Imported by Admin
OK
Cancel

A confirmation dialog appears indicating the successful import of the profile.



The configuration has been imported successfully.

Once imported, the configuration profile is available for deployment by **selecting it**.



My Configurations	Active
MY CAV Profile - Imported by Admin	Active
COMODO Antivirus	

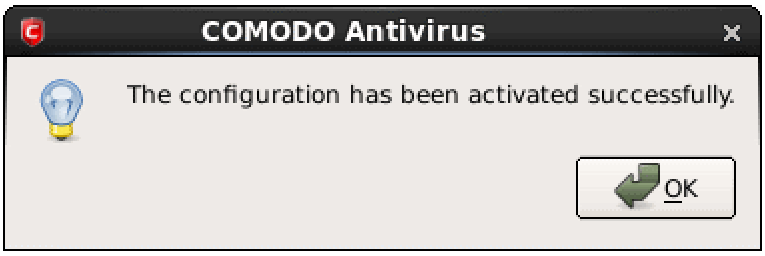
Select and Implement a different configuration profile

The Activate option allows you to quickly switch between configuration profiles.

To select a different configuration

1. Click on the profile you want to select and activate.
2. Click the 'Activate' button.

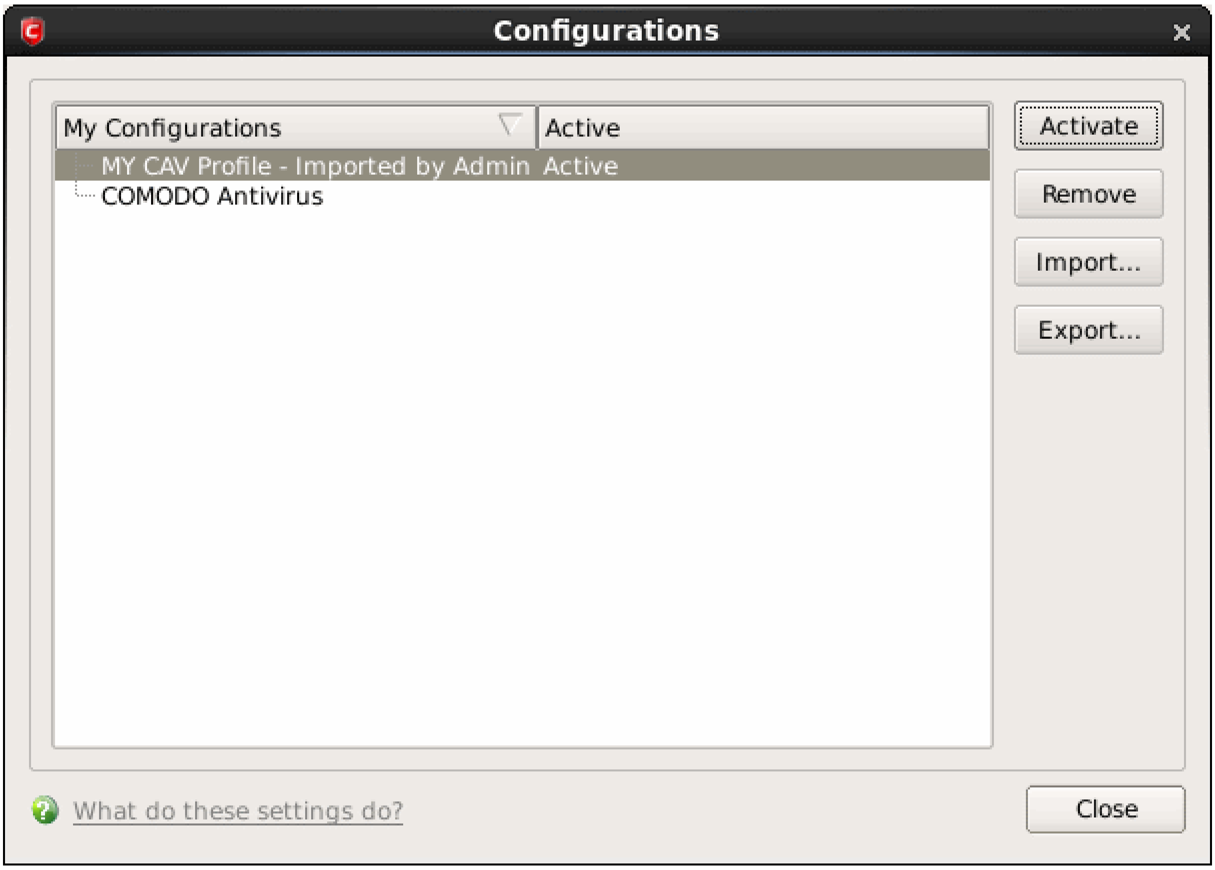
A confirmation dialog appears.



COMODO Antivirus

The configuration has been activated successfully.

The selected configuration is activated.



Configurations

My Configurations	Active
MY CAV Profile - Imported by Admin	Active
COMODO Antivirus	

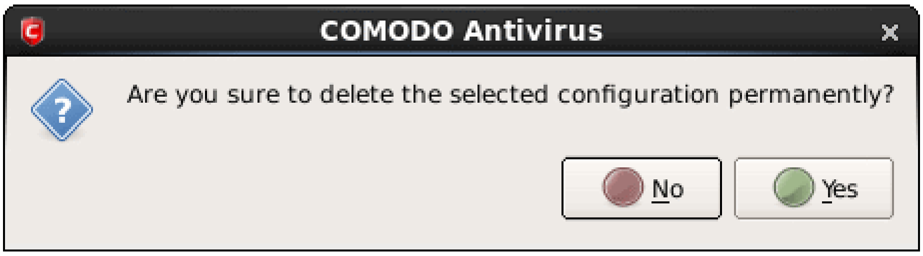
.

Delete an inactive configuration profile

You can remove any unwanted configuration profiles using the 'Remove' button. You cannot delete the profile that Comodo Antivirus is currently using - only the inactive ones. For example if the COMODO Antivirus is the active profile, you can only delete the inactive profiles.

To remove an unwanted profile

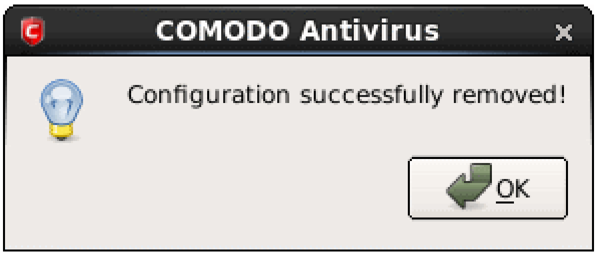
1. Select the profile and click 'Remove' button. A confirmation dialog appears.



COMODO Antivirus

Are you sure to delete the selected configuration permanently?

2. Click 'Yes' if you are sure to delete. The selected profile is removed from the list and a confirmation dialog appears.


COMODO Antivirus

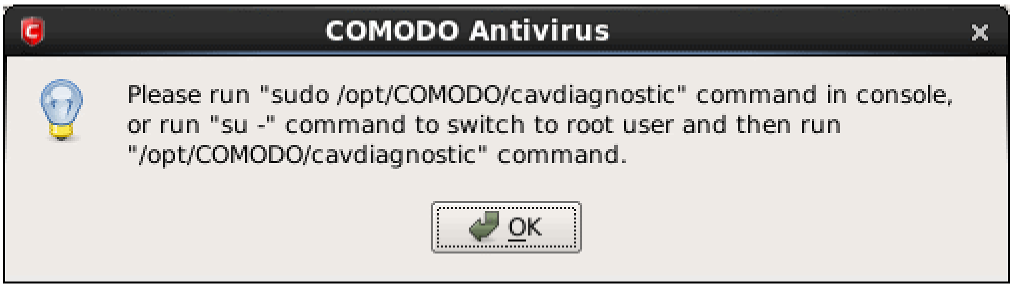
Configuration successfully removed!

4.3. Diagnostics

Comodo Antivirus has it's own integrity checker. This checker scans your system to make sure that the application is installed correctly. It checks your computer's:

- File System - To check that all of Comodo's system files are present and have been correctly installed.
- Checks for the presence of software that is known to have compatibility issues with Comodo Antivirus.

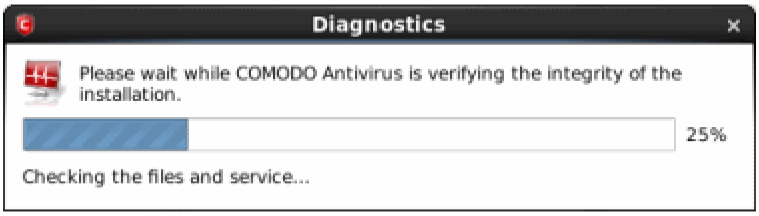
The diagnostics can be run only by the root user (Admin user). If you are not a root user, then a dialog will appear to run a command as root user.


COMODO Antivirus

Please run "sudo /opt/COMODO/cavdiagnostic" command in console, or run "su -" command to switch to root user and then run "/opt/COMODO/cavdiagnostic" command.

- Enter the command as root user in the terminal and press 'Enter'.

The progress of the integrity scan will be displayed.


Diagnostics

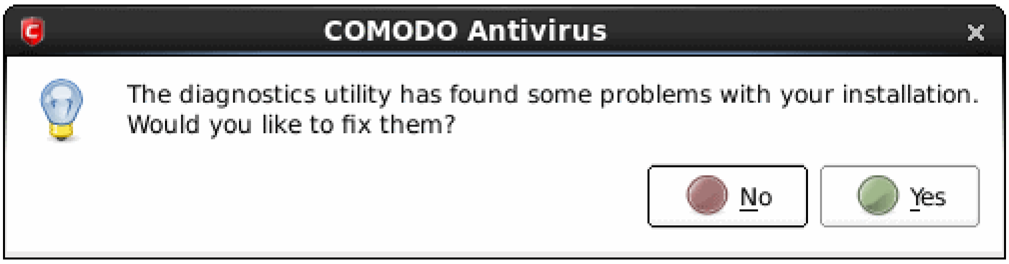
Please wait while COMODO Antivirus is verifying the integrity of the installation.

25%

Checking the files and service...

The results of the scan are shown in the following pop-up window. If your installation does not have any errors a dialog is displayed stating that diagnostics utility did not find any problem with the installation.

If the diagnostics utility has found some errors in the installation, the following dialog is displayed.

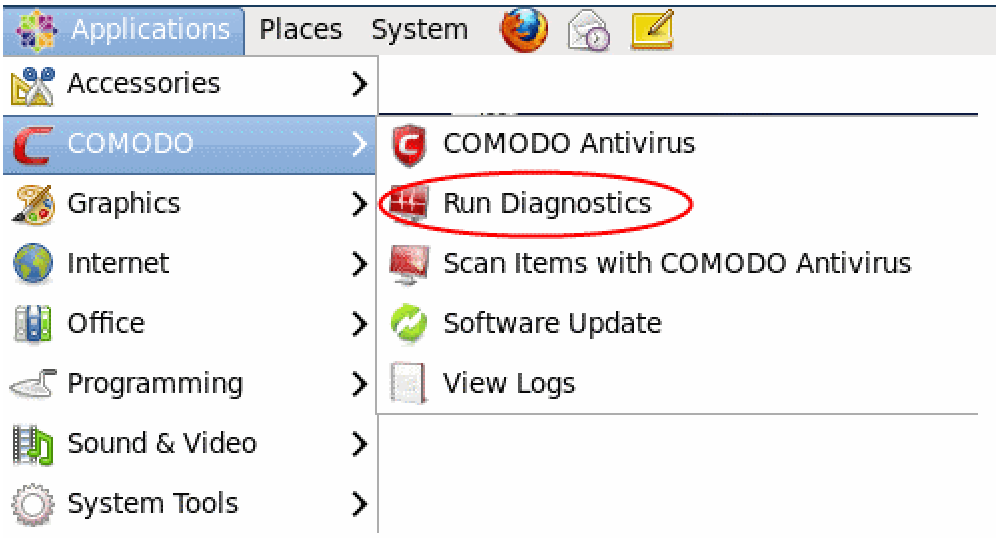

COMODO Antivirus

The diagnostics utility has found some problems with your installation. Would you like to fix them?

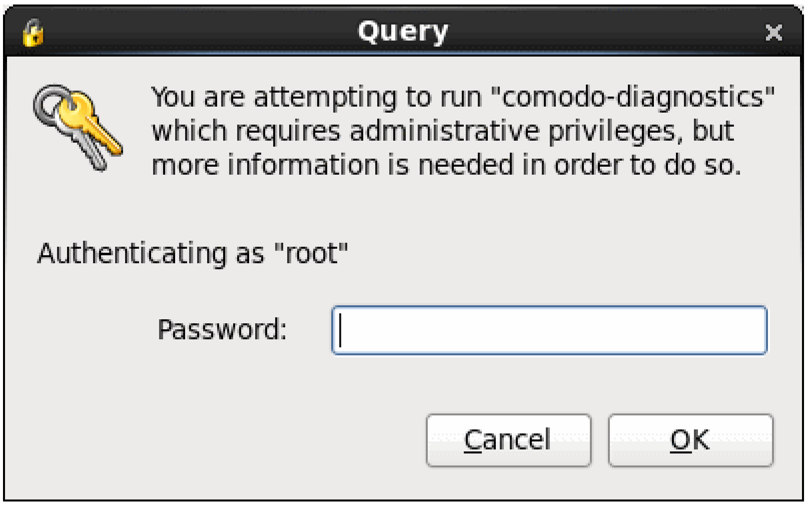
- Click 'Yes'.

The diagnostics utility automatically fixes the problems and prompts you to restart the computer.

The diagnostics also can be run using the Applications menu in the panel.



The diagnostics can be run only by the root user (Admin user). If you are not a root user, then a dialog will appear to enter root password.



Query

You are attempting to run "comodo-diagnostics" which requires administrative privileges, but more information is needed in order to do so.

Authenticating as "root"

Password:

- Enter the password and click 'OK'

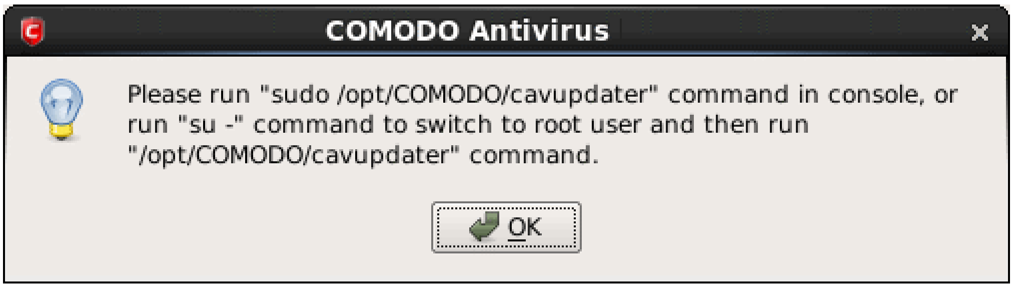
The integrity check will begin as explained above.

Restart your computer for the changes to take effect.

4.4. Check for Updates

Updates on CAVL can be downloaded and installed at any time by clicking the 'Check for Updates' link in 'More' Options interface.

The updater checker can be run only by the root user (Admin user). If you are not a root user, then a dialog will appear to run a command as root user.

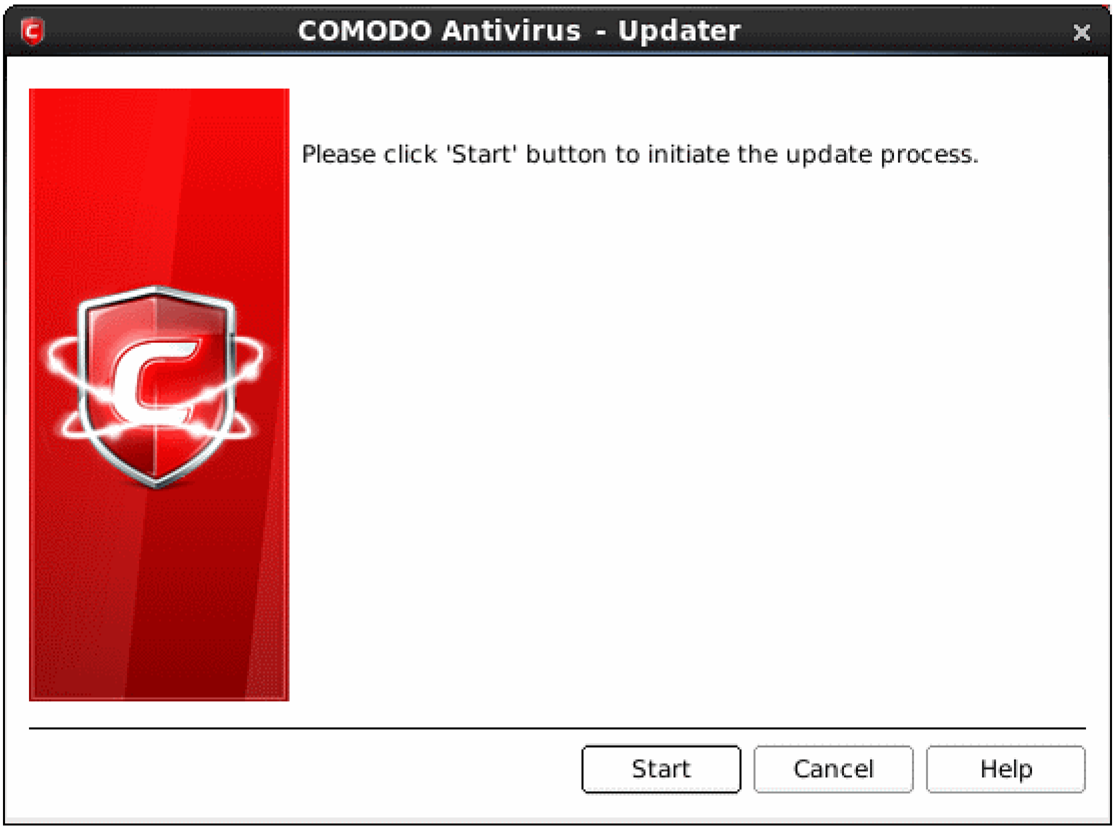


COMODO Antivirus

Please run "sudo /opt/COMODO/cavupdater" command in console, or run "su -" command to switch to root user and then run "/opt/COMODO/cavupdater" command.

- Enter the command as root user in the terminal and press 'Enter'.

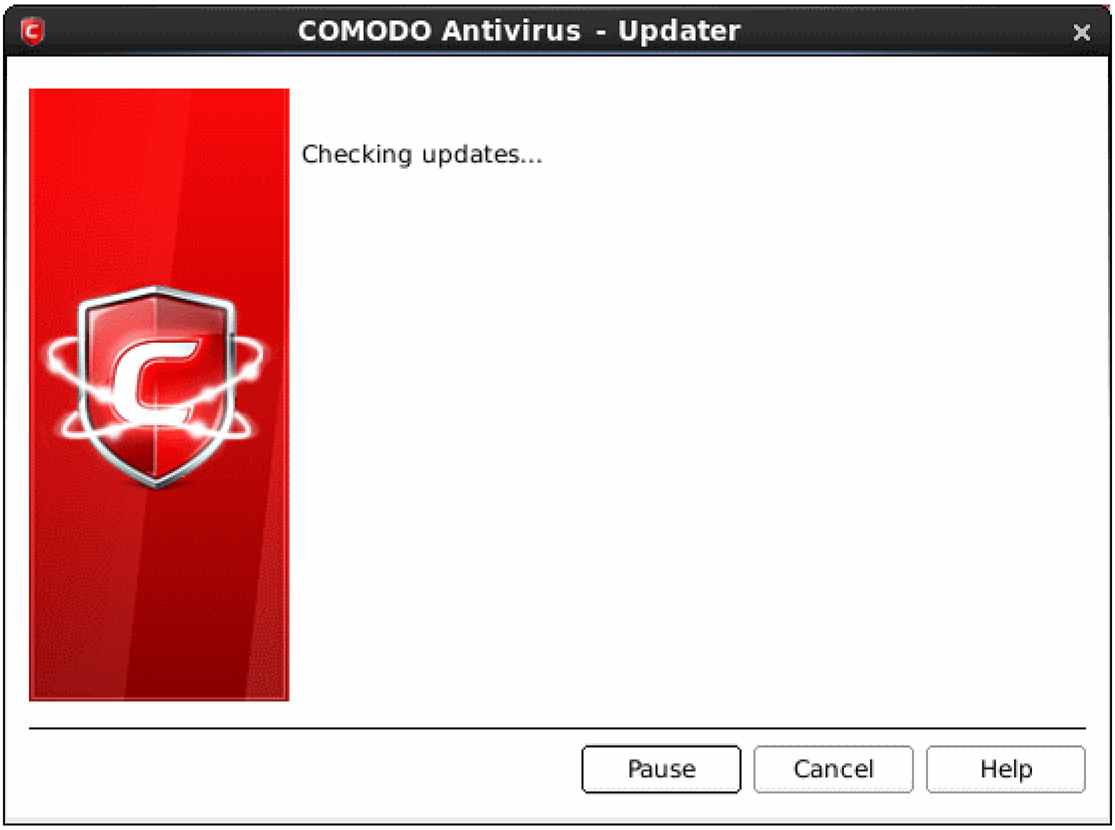
The 'Updater' screen will be displayed.



Please click 'Start' button to initiate the update process.

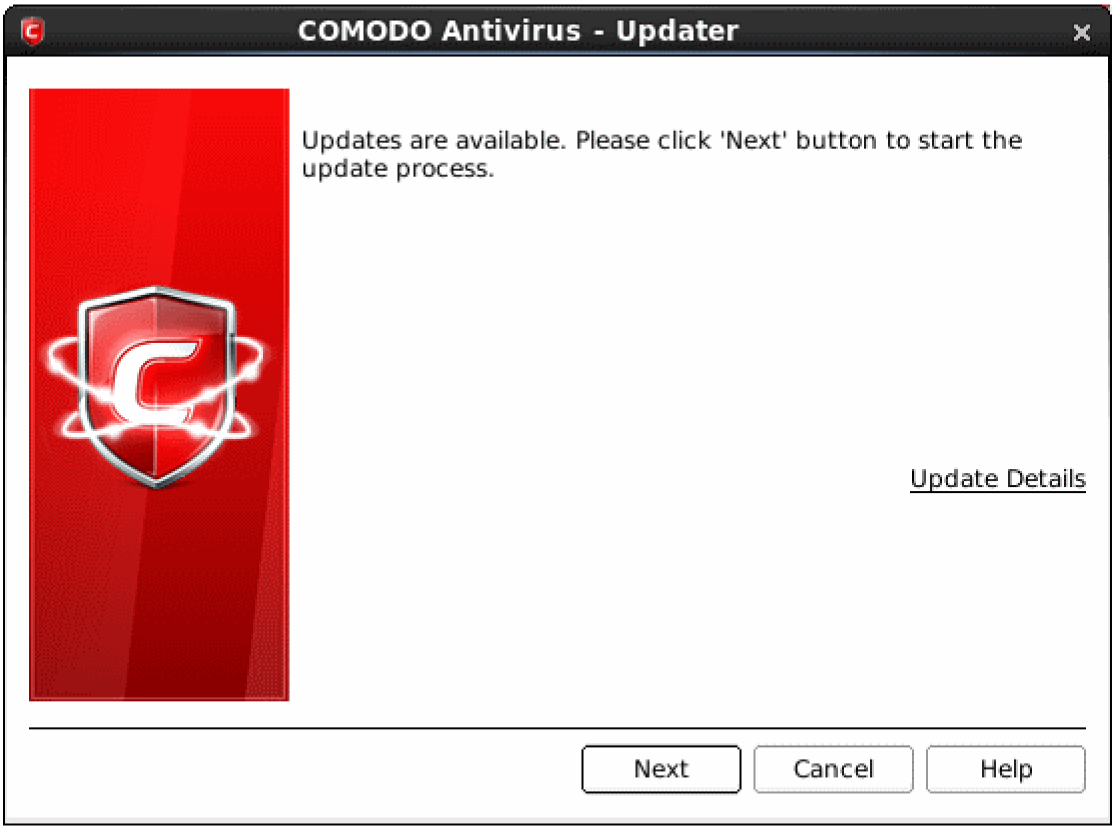
To check for availability of updates

- Click 'Start'.



Checking updates...

On completion of checking, the screen shows the availability of updates.



COMODO Antivirus - Updater

Updates are available. Please click 'Next' button to start the update process.

The 'Update Details' link will lead you to the web page that provides release notes for the latest version of the application.

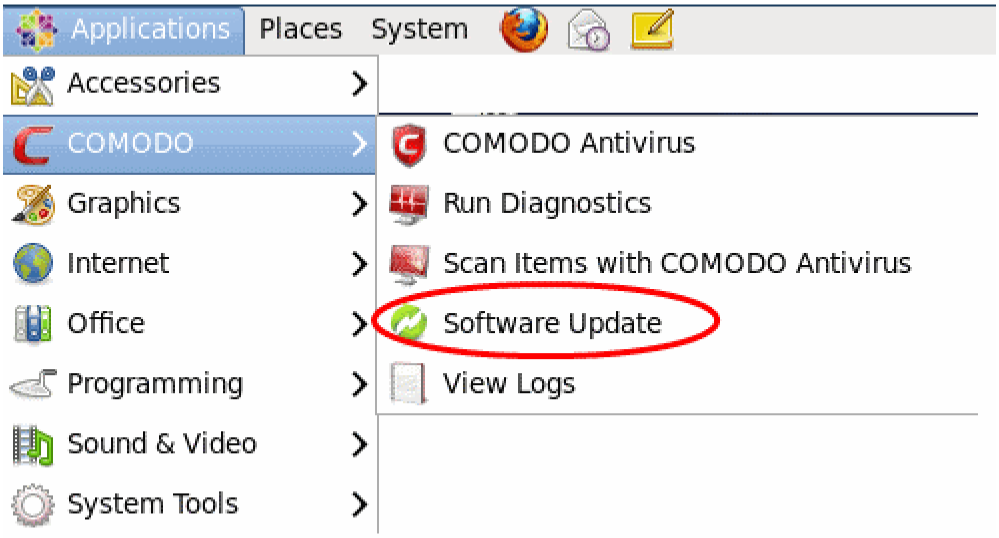
To initiate the update process

- Click the 'Next' button in the panel.

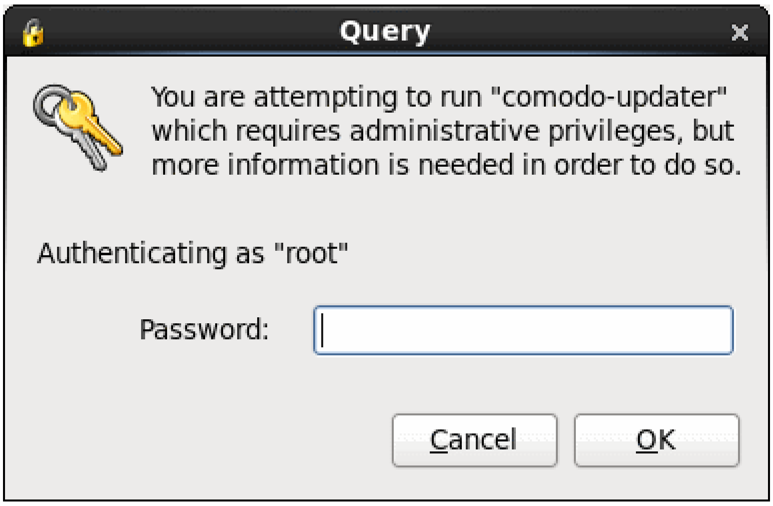
Note: If you want to download and install the updates later, click the 'Cancel' button.

After the installation process is completed, Click 'Finish'. Uncheck the 'Restart the system' checkbox to restart the system at a later time.

The update checker also can be run using the Applications menu in the panel.



The update checker can be run only by the root user (Admin user). If you are not a root user, then a dialog will appear to enter root password.



Query

You are attempting to run "comodo-updater" which requires administrative privileges, but more information is needed in order to do so.

Authenticating as "root"

Password:

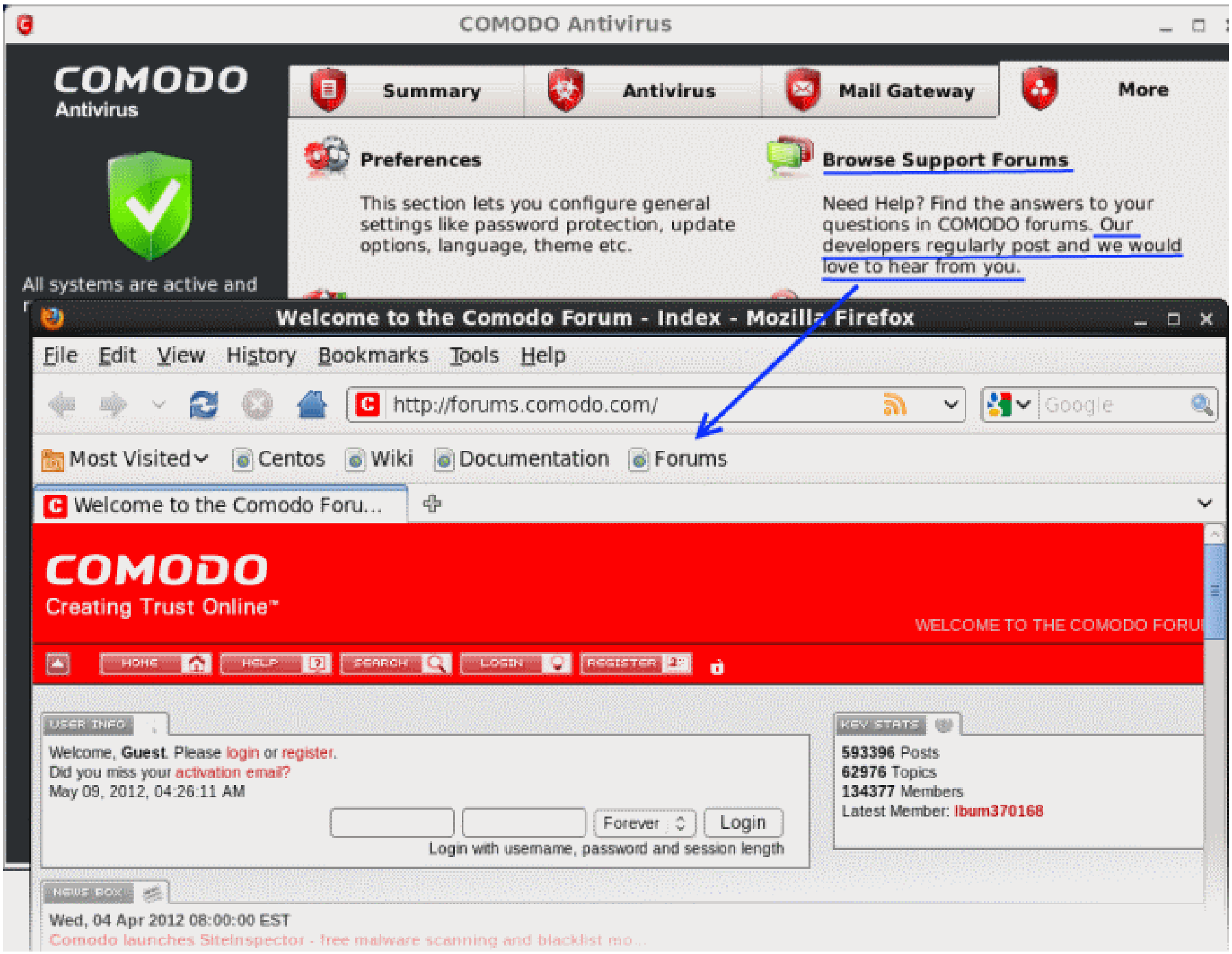
Enter the root password and click 'OK'

The process of update checking will begin as explained above.

4.5. Browse Support Forums

The fastest way to get further assistance on Comodo Antivirus is by posting your question on Comodo Forums, a message board exclusively created for our users to discuss anything related to our products.

- Click the **Browse Support Forums** link to be taken straight to the website at **http://forums.comodo.com/**. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.



COMODO Antivirus

Preferences

This section lets you configure general settings like password protection, update options, language, theme etc.

Browse Support Forums

Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.

All systems are active and

Welcome to the Comodo Forum - Index - Mozilla Firefox

http://forums.comodo.com/

WELCOME TO THE COMODO FORU

Welcome, **Guest**. Please login or register.
Did you miss your activation email?
May 09, 2012, 04:26:11 AM

Login with username, password and session length

593396 Posts
62976 Topics
134377 Members
Latest Member: **lbum370168**

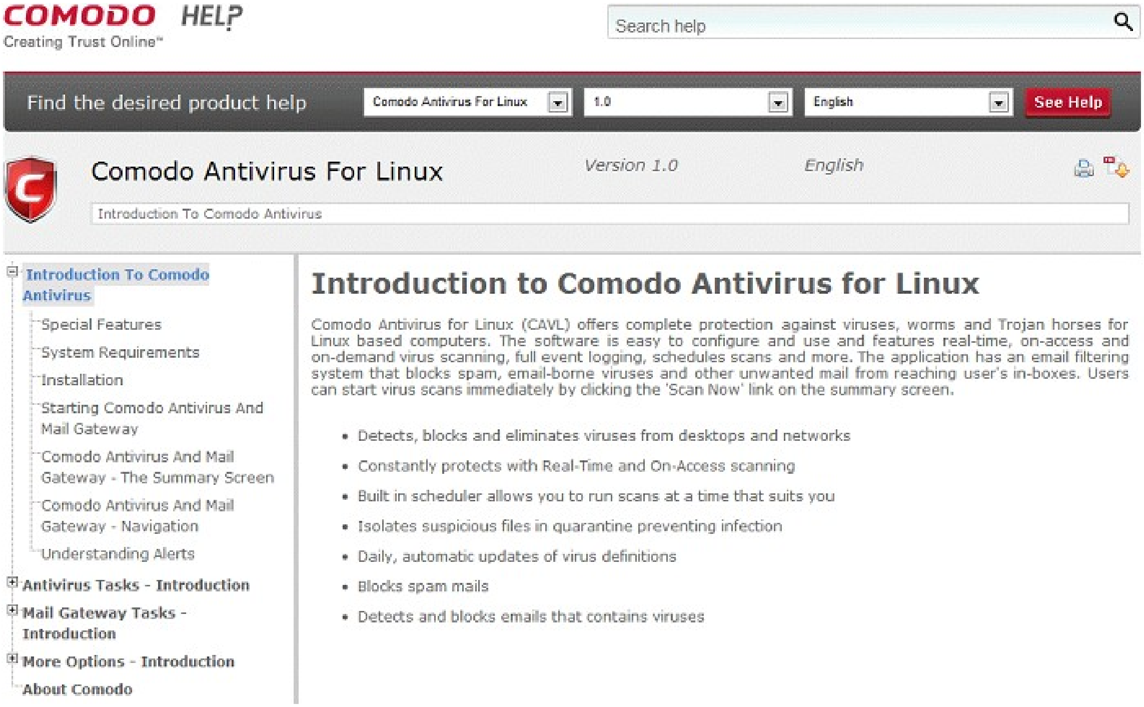
Wed, 04 Apr 2012 08:00:00 EST
Comodo launches SiteInspector - free malware scanning and blacklist mo...

Online Knowledge Base

We also have an online knowledge base and support ticketing system at **http://support.comodo.com/**. Registration is free.

4.6. Help

Clicking the Help link in the More section opens this online help guide. Each area has its own dedicated page containing detailed descriptions of the application's functionality.



COMODO HELP
Creating Trust Online
Search help
Find the desired product help
Comodo Antivirus For Linux
1.0
English
See Help
Comodo Antivirus For Linux
Version 1.0
English
Introduction To Comodo Antivirus
Introduction To Comodo Antivirus
Special Features
System Requirements
Installation
Starting Comodo Antivirus And Mail Gateway
Comodo Antivirus And Mail Gateway - The Summary Screen
Comodo Antivirus And Mail Gateway - Navigation
Understanding Alerts
Antivirus Tasks - Introduction
Mail Gateway Tasks - Introduction
More Options - Introduction
About Comodo

Introduction to Comodo Antivirus for Linux

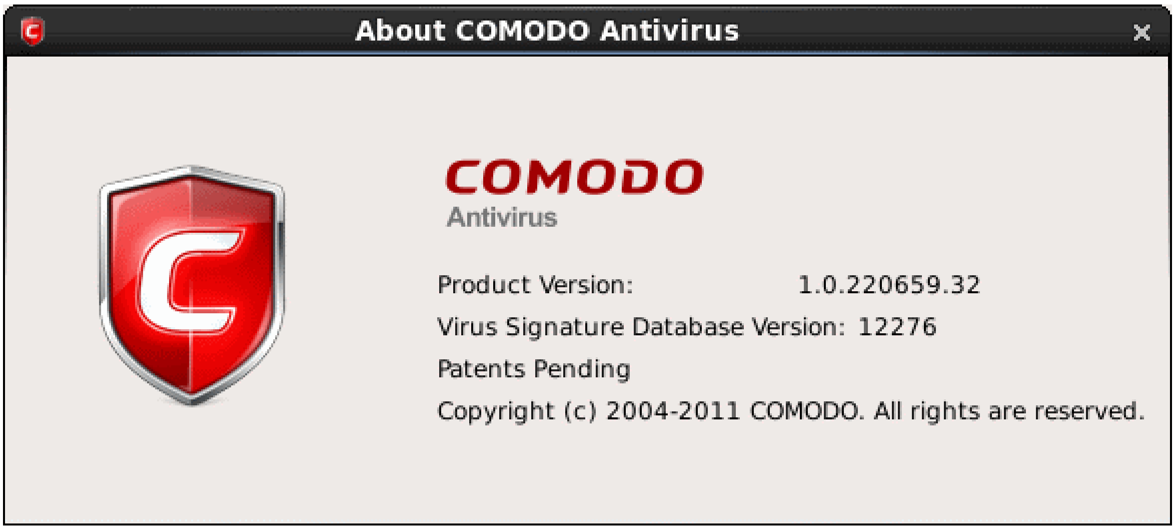
Comodo Antivirus for Linux (CAVL) offers complete protection against viruses, worms and Trojan horses for Linux based computers. The software is easy to configure and use and features real-time, on-access and on-demand virus scanning, full event logging, schedules scans and more. The application has an email filtering system that blocks spam, email-borne viruses and other unwanted mail from reaching user's in-boxes. Users can start virus scans immediately by clicking the 'Scan Now' link on the summary screen.

- Detects, blocks and eliminates viruses from desktops and networks
- Constantly protects with Real-Time and On-Access scanning
- Built in scheduler allows you to run scans at a time that suits you
- Isolates suspicious files in quarantine preventing infection
- Daily, automatic updates of virus definitions
- Blocks spam mails
- Detects and blocks emails that contains viruses

You can also print or download the help guide in pdf format from the webpage.

4.7. About

Click the 'About' option in the 'More' Screen to view the 'About' information dialog.



Product Version: 1.0.220659.32
Virus Signature Database Version: 12276
Patents Pending
Copyright (c) 2004-2011 COMODO. All rights are reserved.

The 'About' dialog displays the copyright information and the information on the version numbers of Comodo Antivirus and the Virus Signature Database installed on your computer. The serial number is used to identify your installation and is necessary for support purposes.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

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