

# **K7AntiVirus 7.0 User Manual**

---



**K7 Computing Private Limited,  
Chennai, India  
[www.k7computing.com](http://www.k7computing.com)**

## Table of Contents

1.	Feature Summary.....	4
2.	Online Help Conventions.....	5
3.	Activating Your Product .....	6
4.	Removing K7AntiVirus .....	7
5.	Opening the Main Console .....	7
6.	Overview of the Main Console .....	8
7.	Viewing the Current Status of Your Protection.....	9
8.	Updating Your Product.....	9
9.	Managing the Virus Protection.....	12
10.	Configuring the AntiVirus .....	13
11.	Configuring Spyware Protection.....	19
12.	Managing Exclusions .....	19
13.	Configuring the Email Scanner .....	20
14.	Enabling the Email Scan .....	22
15.	Disabling the Email Scanner.....	22
16.	Starting Email Scan Automatically.....	23
17.	Configuring Email Server Settings.....	23
18.	Scanning for Malicious Attachments.....	24
19.	Configuring the Worm Blocking Settings .....	24
20.	Managing Quarantined Files .....	25
21.	Configuring Additional Scan Options .....	27
22.	Configuring Messenger Scanning .....	28
23.	Configuring Script Scanning .....	28
24.	Configuring Office Plugin Scanning .....	29
25.	Configuring the Scan Settings .....	29
26.	Selecting the Types of Files to Scan.....	31
27.	Adding File Extensions for the Scan .....	31
28.	Configuring Scan Tasks.....	32
29.	Configuring the QuickScan .....	32
30.	Creating Custom Scan Tasks .....	33
31.	Customizing a Scan Task .....	34
32.	Scheduling Scan Tasks .....	36
33.	Changing the Schedule for a Scan Task .....	36
34.	Manually Running a Scan Task.....	37
35.	Deleting Scan Tasks .....	37
36.	Running QuickScan.....	38
37.	Scanning Your Entire Computer.....	38
38.	Scanning a Folder.....	38
39.	Scanning a File.....	39
40.	Scanning Multiple Locations .....	39
41.	Configuring the General Scan Settings .....	40
42.	Configuring the Log Options.....	41
43.	Viewing Virus Information on the Web.....	42
44.	Viewing News .....	42
45.	Using the Report Viewer .....	42
46.	Logging AntiVirus Activities .....	43
47.	Viewing the AntiVirus Log .....	45
	Glossary of Terms .....	46

## **K7AntiVirus**

Welcome to K7AntiVirus Help.

A virus is simply a computer program designed in such a way that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or a document containing a macro virus is opened, the attached virus program is activated and attaches itself to yet other programs and documents. In addition to replicating, viruses are generally programmed to deliver a payload. Most viruses simply display a message on a particular trigger date.

While the Internet gives you access to a large quantity of information and business opportunity, it also exposes your computer to a multitude of security threats that most of us are not aware of. **K7AntiVirus** is a powerful but easy-to-use comprehensive solution that offers protection against viruses.

K7AntiVirus helps you to safeguard your computer from virus threats through the network, email or Internet. It protects your computer from **viruses**, **Trojans**, **Internet worms** and harmful scripts. It scans all files that can be opened, executed or saved on your computer and all connected disk drives, and automatically detects and removes known viruses. K7AntiVirus detects viruses and potential threats in email messages and instant messenger attachments. It monitors the critical areas of your system for changes and warns you of the consequences.

## 1. Feature Summary

K7AntiVirus continuously monitors your system and protects it from known and unknown viruses.

The features in K7AntiVirus include:

- **Auto-protection** - loads into memory when Windows starts and provides continuous protection while you work;
- **Full on-access protection** - provides maximum protection by scanning every file opened, executed or saved; and prevents the opening or executing of infected files
- **Full online email protection** - checks all incoming and outgoing email, providing full protection from email-borne threats
- **Instant messenger protection** - scans and detects viruses in email and instant messenger attachments
- **Trojan protection** - detects the activity of Trojan programs and recovers system files modified by Trojans
- **Automatic threat handling** - automatically repairs or removes infected files and other threats such as trojans, worms and spyware
- **Automatic update** - updates and installs copies of the virus and spam definition files automatically

## 2. Online Help Conventions

Window and dialog names are shown in plain type, capitalized as the names appear on-screen in the title bars:

When you are finished, close the Email Settings dialog.

Menu names, commands, buttons, and data entry fields are shown in bold text, capitalized as they appear on-screen:

In the AntiVirus console, click the **Settings** option and then select the **Sentry** tab.

Important notes are shown like this:

**Note:** It is recommended that you select this option so that your computer is continually monitored.

Warnings about important steps to take are shown like this:

It is recommended that you *do not* disable K7AntiVirus, as it could make your system vulnerable to viruses.

Literal text that you type, or references to directories and file names is formatted in a monospaced courier typeface:

Type `program.exe` and press the **Enter** key.

Explanation for certain terms are displayed as pop-ups as shown below. Click on the term to view the information in a pop-up. Click outside the pop-up to close it.

K7AntiVirus protects your computer from viruses and **Trojans**.

Prompts and alerts that may appear on your screen are indicated as shown below. Click on the word "message" to view an image of the message. Click on the word "message" again to hide the image.

A confirmation **message** appears.

References to other sections of the Online Help are formatted as such:

**[See Updating Your Product](#)** for more information



### 3. Activating Your Product

Activating your product helps keep it up-to-date so as to protect your computer from newly discovered threats. The K7AntiVirus software must be updated frequently to handle new viruses and threats. In order to receive updates and support from K7 Computing it is important that you activate your product.

When you first install your software you are prompted to activate your product. If you do not activate it when you are first prompted, you will receive an **alert** every day till you register the product.


To register the product later, click the **Remind Later** button. If you do not want the alert to appear again, select the **Do not show this warning again** check box.

You can activate your product from the alert or from the K7AntiVirus main console.

#### ***To activate your product from the alert:***

1. Click the **Activate Now** button on the alert. The Product Activation screen appears.
2. Click **Next**.
3. Enter the registration details, your **Email address** and **Password**.
4. Enter the **Serial Number** of your product and click **Next**.
5. Re-enter your **Email Address** and **Password** for confirmation.
6. Make sure you are connected to the Internet and click **Next**.
7. On successful registration, you will receive your account information and License validity details.

#### ***To activate your product later:***

1. Double-click the  icon in the System Tray. The K7AntiVirus console opens.
2. If your product is not activated, it is indicated in the **License Information** panel. Click the **activate now** option. The Product Activation screen appears.
3. Follow the instructions detailed in steps 2 to 7 above to activate your product.

Once you have activated your product, the License information appears on the K7AntiVirus console.

## 4. Removing K7AntiVirus

Before you remove K7AntiVirus restore the files you have quarantined to a safe location such as a marked floppy disk or CD.



### *To remove K7AntiVirus:*

1. Click **Start->Settings->Control Panel**.
2. In the Control Panel, double-click the **Add or Remove Programs** option.
3. Select **K7AntiVirus** in the **Currently installed programs** list and click **Remove**.
4. Follow the instructions on your screen to remove the software.
5. Click **Finish** to restart Windows.

The above procedure will remove K7AntiVirus from your computer.

## 5. Opening the Main Console

You can start K7AntiVirus in any of the following ways:

- Click **Start->Programs->K7AntiVirus->K7AntiVirus 7.0**
- Double-click the  icon in the System Tray
- Right-click the  icon in the System Tray and then click the **Open K7AntiVirus** option

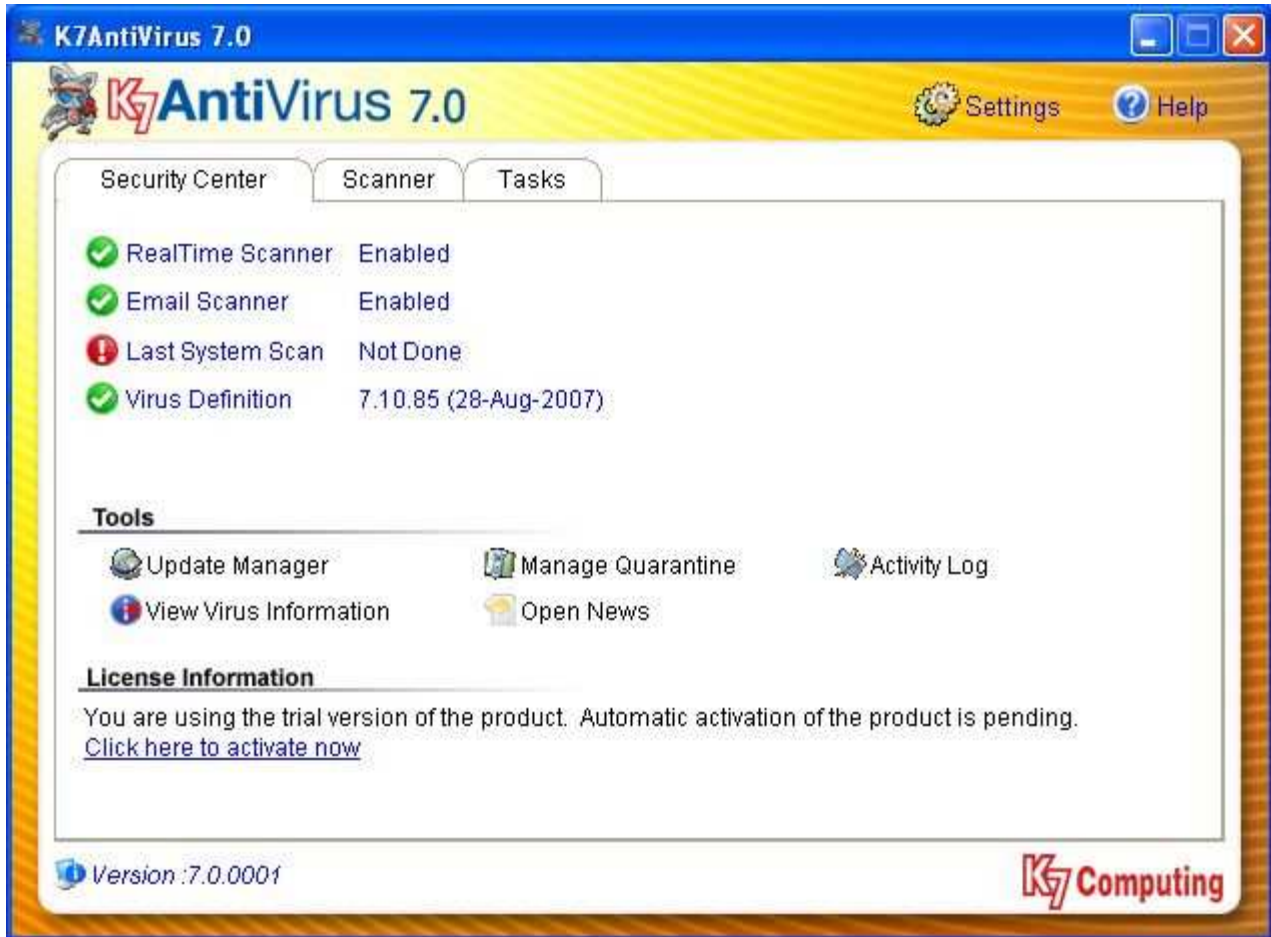
[\*\*\*See System Tray Icon\*\*\*](#)

The main console of K7AntiVirus opens and displays the current status of your product.

[\*\*\*See Overview of the Main Console\*\*\*](#)

## 6. Overview of the Main Console

The layout of the K7AntiVirus main console is as shown in the following figure.



The Top panel has options to configure the **Settings** of the AntiVirus.

The Main panel displays the Security status and License Information.

The **Tools** panel has options to manage updates and quarantined files; and view the activity log, news and virus information.

## 7. Viewing the Current Status of Your Protection

The K7AntiVirus main console shows the current status of the protection of your computer.

### *To view the current status:*

1. Open the K7AntiVirus console.
2. The **Security Center** tab indicates which of the components of your product are enabled or disabled. It also displays the date on which you last updated your product.

If you have not updated your product in the last month, please update it immediately.  
[See Updating Your Product](#) for details

3. The License Information panel displays the serial number and validity of your product.

## 8. Updating Your Product

In order to protect your computer from newly discovered viruses and threats you must keep the K7AntiVirus product installed on your computer up-to-date. Product updates are improvements on your installed product. Updates can be obtained from the K7 Computing web site for the duration of your license. When your license is due to expire, you will be prompted to renew it. Select **Renew Now** and follow the instructions to renew your license. Once the license is renewed, the product automatically checks for updates.

Your product must be registered before you update it.

K7AntiVirus is automatically configured to check for updates when you are connected to the Internet, and then notify you with alerts. You can configure K7AntiVirus to notify you before downloading and installing updates.

**Note:** You must be connected to the Internet for K7AntiVirus to check for available updates.



You can choose to

- [Automatically check for updates](#)
- [Manually check for updates](#)
- [Disable automatic checking for updates](#)

## 8.1. Automatically Checking for Updates

You can configure your product to check for protection updates automatically. New updates are posted on the K7 Computing web site. If you configure your product to check for updates automatically, it will obtain the new updates from the K7 Computing web site without intervention from you provided your Internet connection is available. The product will check for updates every five minutes, and after a successful update it will connect to the K7 Computing site again to check for updates after three hours.

### *To configure your product to automatically check for updates:*



1. Open the K7AntiVirus console and click the  **Update Manager** option on the **Tools** panel. Alternatively, right-click the  icon in the System Tray and select the **Updates** option. The Update Manager dialog appears.
2. Click **Options** on the top of the Update Manager dialog. The Options dialog opens.
3. Select the **Enable Automatic Update of the Product when the System Starts** check box and then select one of the following options:
  - **Automatically update the product, notify on completion** - automatically downloads and installs the update; and notifies you when the update is installed
  - **Download the updates, prompt before copying files** - notifies you before copying the update files to your computer
  - **Prompt before downloading the updates** - notifies you before downloading any update
4. If your Internet connection is through a proxy server, select the Access Internet through a Proxy Server check box and enter the details of the proxy server in the fields provided.
5. Click Close to close the Options dialog.
6. Make sure you are connected to the Internet and click Start. Your product connects to the K7 Computing web site and downloads the updates. A message indicating the status of the update is displayed.

Your product must have a valid license to update your product. If your license period has lapsed, you are warned.
7. Once the product has been updated you will need to close all open applications and reboot your computer.

## 8.2. Manually Checking for Updates

Perform a manual update of your product anytime to ensure that you are using the latest protection updates. In addition, it is recommended that you perform a manual update whenever there is a threat outbreak, or if you suspect that your computer is infected, and a scan did not detect any threats.

### *To manually check for updates:*

1. Open the K7AntiVirus console and click the  **Update Manager** option on the **Tools** panel. Alternatively, right-click the  icon in the System Tray and select the **Updates** option. The Update Manager dialog appears.
2. Make sure you are connected to the Internet and click **Start**. Your product connects to the K7 Computing web site and downloads the updates. A message indicating the status of the update is displayed.



Your product must have a valid license to update your product. If your license period has lapsed, you are warned.

3. Once the product has been updated you will need to close all open applications and reboot your computer for the update to take effect.

## 8.3. Disabling Automatic Updates

For maximum protection, it is recommended that you configure K7AntiVirus to automatically download and install updates. However, if you want to manually update your product, you can disable the automatic updating feature.

### *To disable automatic updating:*

1. Open the K7AntiVirus console and click the  **Update Manager** option on the **Tools** panel. Alternatively, right-click the  icon in the System Tray and select the **Updates** option. The Update Manager dialog appears.
2. Click **Options** on the top of the Update Manager dialog. The Options dialog opens.
3. By default, the system is configured to automatically download and install updates. Clear the **Enable Automatic Update of the Product when the System Starts** check box to prevent K7AntiVirus from automatically checking for updates.
4. Click **Close**.


### **Note:**

If you disable the automatic update, you must manually check for updates *at least* once a week to ensure that your computer is protected with the latest security updates.

## 9. Managing the Virus Protection

K7AntiVirus provides a reliable and up-to-date virus protection. It continuously scans your system in the background and prevents virus infection from files coming in through email attachments, instant messenger, Internet downloads and through vulnerability exploits. It also scans for certain non-virus threats like spyware, adware, and other attack tools.

### *To manage the virus protection:*

1. Double click the  icon in the System Tray. The K7AntiVirus console opens.
2. The status of the protection appears on the main panel of the console. The system indicates if the Real-Time Scanner and Email Scanner are enabled (indicated by a green tick).
3. The date on which the system was last scanned is displayed. If you want to scan your system, click the **Last System Scan** option and then click the **Not Done** option that appears. If the scanning is done, click on the status displayed.
4. The date on which the Virus Definition files were last downloaded is displayed. To update the virus definition, click the **Virus Definition** option and then click the **Open Update Program** option. The Update Manager dialog appears. [See Manually Updating Your Product](#) for more information
5. The **Tools** panel of the console has options to do the following:
  - [Open Update Manager](#)
  - [Manage Quarantined Files](#)
  - [View Virus Information on the Web](#)
  - [View the Activity Log](#)
  - [View News on viruses](#)
6. To configure the AntiVirus settings, click the Settings option on the top panel of the console. The Configure AntiVirus dialog opens. See [Configuring the AntiVirus](#) for more information
7. If you want to scan multiple locations on your computer, click the Scanner tab.

[See Scanning Multiple Locations](#) for more information

8. To configure and schedule scan tasks, click the Tasks tab.

[See Configuring Scan Tasks](#) for more information

## 10. Configuring the AntiVirus

You can configure K7AntiVirus to manage real-time viruses and infected emails. It also provides script and instant messenger protection.

### *To configure the antivirus:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option in the top panel of the console. The Configure AntiVirus dialog opens.
3. Using the options provided in this dialog, you can do the following:
  - [Configure the RealTime Scanner](#)
  - [Configure the Email Scanner](#)
  - [Configure Script and Instant Messenger Protection](#)
  - [Configure the Scan Settings](#)
  - [Configure the General Scan Settings](#)

### 10.1. Configuring the Real-Time Scanner

By default the virus protection (real-time scanning) is enabled. It constantly monitors your system for virus activity. The Sentry scans files each time you or your computer accesses them. When a virus is detected, the AntiVirus protection attempts to clean or remove the infection.

#### ***To configure the Real-Time Scanner:***

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
3. Click the **Sentry** tab.
4. Select the **Load K7Sentry automatically when the System starts** check box if you want the Sentry to start when your computer starts.

**Note:** It is recommended that you select this option so that your computer is continuously monitored.

5. Under What to Scan, select the types of files you want to scan. The options are described in the following table.

Option	Description
<b>All Files</b>	Scans all files
<b>Automatic Identification</b>	Scans all executable files, Microsoft documents and script files. To select the required options, click the <b>customize</b> option. The Types of Files to Scan dialog appears. Select the <b>Type of Files to Scan</b> and click <b>OK</b> . <a href="#">See Selecting the Types of Files to Scan</a> for details
<b>Specific Extensions</b>	Scans files with the specified extensions. In addition to the default list of file extensions that K7AntiVirus is configured to scan, you can add other extensions. To do so, click the <b>customize</b> option. The Types of File Extensions to Scan dialog appears. Add the <b>Extensions</b> and click <b>OK</b> . <a href="#">See Adding File Extensions for Scan</a> for details
<b>Detect Spywares and adwares</b>	Select the check box if you want the Sentry to scan the files for threats such as spyware, adware, etc. Click <b>customize</b> to select the types of threats to scan and the action to take when a selected threat is identified. <a href="#">See Defining Types of Threats to Scan</a> for details

- Under Action to Take When a Virus is Found, select an action to be taken if a file is found to be infected. The actions are described in the following table.

Action	Description
<b>Clean automatically, deny access if unable to clean</b>	Cleans the file without any interaction from you. If cleaning is not possible, access is denied to the infected file. An alert is displayed with the details of the detection and the action taken.
<b>Clean automatically, quarantine if cleaning is not possible</b>	Repairs the file. Moves the file to the Quarantine folder if cleaning is not possible. An alert is displayed with the details of the detection and the action taken.
<b>Deny access</b>	Restricts access to the infected file

- You can exclude files or folders from being monitored. If you want to exclude files or folders, click the Manage Exclusions option on the Sentry tab. See Managing Exclusions for details.
- Once you have configured the Sentry, click Apply to save the changes.


## 10.2. Enabling Real-Time Scan

The real-time scan is enabled by default. If you disable it for any reason, you can enable it again.

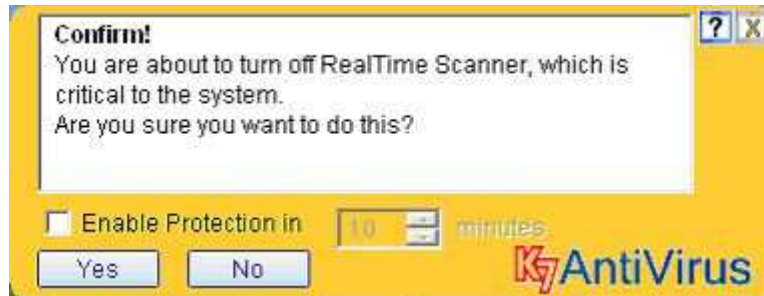
It is recommended that you have the real-time protection enabled all the time so that your computer is protected from viruses and threats continuously.

### ***To enable the Real-Time scan:***

- Open the K7AntiVirus console.
- The status of the RealTime Scanner is displayed in the main panel.
- If the real-time protection is currently disabled, click the status (**Disabled**). You are prompted to enable the real-time scan.

**Note:** To quickly turn on the real-time protection, right-click the  icon in the System Tray and click **Enable RealTime Scan**.

- A message appears indicating that the protection has been enabled.




### 10.3. Disabling Real-Time Scan

The real-time scan is enabled by default. You can disable the real-time scan.


It is recommended that you *do not* disable the real-time protection, as your computer could get infected with viruses.

#### ***To disable the Real-Time scan:***

1. Open the K7AntiVirus main console.
2. The status of the RealTime Scanner is displayed in the main panel.
3. If the real-time protection is currently enabled, click the status (**Enabled**). You are prompted to disable the real-time scan.

**Note:** To quickly turn off the real-time protection, right-click the  icon in the System Tray and click **Disable RealTime Scan**.

4. A confirmation message appears.
5. If you are sure you want to disable the real-time scan, click Yes.
6. If you want to turn off the real-time protection for a short period of time, check the Enable Protection in check box and enter the time in minutes.
7. Click No to leave the real-time protection on.

**Note:** If the real-time scanner is disabled, the K7 icon in the System Tray appears as such .

## 10.4. Automatically Starting Real-Time Scan

### *To start the Real-time scan automatically:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option and then select the **Sentry** tab in the Configure AntiVirus dialog.
3. Select the **Load K7Sentry automatically when the System starts** check box.  
Clear the check box if you do not want the real-time scan to start automatically when the system starts.
4. Click **Apply** to save the settings.
5. Click **Close** to close the Configure AntiVirus dialog.

## 10.5. Configuring the Types of Threats to Scan

You can define the additional threats you want K7AntiVirus to identify during the manual, real-time and email scan.

### *To define additional threats:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option. The Configure AntiVirus dialog opens.
3. Select the **Sentry** tab or the **Email** tab.
4. Select the **Detect Spyware and adwares** check box and click the **customize** option. The Types of Threats to Scan dialog opens.
5. Select the appropriate check boxes to define the types of **threats to identify**. The types of threats that K7AntiVirus can identify are described below.

Threat	Description
<b>Viruses, Worms and Trojans</b>	Viruses, <b>Trojans</b> and <b>Internet worms</b> . These are scanned by default.
<b>Security Risks</b>	Known programs that may or may not be a risk to your computer, but have worm properties
<b>Spywares</b>	Stand-alone programs that monitor your system activity in the background and can detect and send confidential information such as passwords out of your computer
<b>Adwares</b>	Stand-alone programs in which advertising banners are displayed while the program runs. These programs usually include code that tracks a user's personal information and passes it on to third parties.
<b>Dialers</b>	Programs that dial out without your knowledge to other prone or ftp sites basically to make charges

<b>Joke Programs</b>	Programs that change the normal behaviour of your system like making sticky keys or changing the function keys
<b>Network Access</b>	Programs that allow others to access your computer through the Internet to gather information or attack your computer
<b>Hacker tools</b>	Programs or tools used by hackers to gain unauthorized access to your computers. These could be simply Keyboard loggers that capture keystrokes and send the information to the hacker.

6. Select an option to specify what Action needs to be taken when the selected threats are identified. The actions that can be taken are detailed below.

<b>Action</b>	<b>Description</b>
<b>Quarantine the file</b>	Moves the file containing the threat to the Quarantine folder
<b>Delete the file</b>	Deletes the file containing the threat
<b>Do not take any action</b>	Takes no action when a threat is identified
<b>Prompt for an action</b>	Prompts you for the action to be taken when a threat is identified

7. To customize how K7AntiVirus detects spywares, click the customize Spyware detection option. The Spyware Management dialog opens. See Configuring Spyware Protection for details
8. Click OK to save the settings.

## 11. Configuring Spyware Protection

Spywares are programs that collect personal information about users without their consent. Adwares are programs in which advertising banners are displayed while the program runs. These programs usually include code that tracks a user's personal information and passes it on to third parties. Personal information is secretly recorded using techniques such as logging keystrokes, recording Internet web browsing history, etc.

### *To customize how K7AntiVirus handles spyware and adware:*

1. Open the K7AntiVirus console.
2. Click the Settings option on the top panel of the console. The Configure AntiVirus console opens.
3. Open the Sentry tab or Email tab (to protect emails) and select the Detect Spywares and adwares check box.
4. Click the customize link. The Types of Threats to Scan dialog opens.
5. Click the customize Spyware detection option at the bottom of the dialog. The Spyware Management dialog opens.
6. The list of spywares that K7AntiVirus can detect is displayed in the Spyware List.
7. To exclude any spyware from detection, select it in the Spyware List and click the Add Entry button. The selected spyware is moved to the Spyware Excluded list and will not be detected by the manual, real-time or email scan.
8. To ensure a spyware is detected in the scan, select it in the Spyware Excluded list and click Remove. The selected spyware is added to the Spyware List and will be detected during the scan.
9. Click OK to save the spyware settings.

## 12. Managing Exclusions

You can exclude certain files and areas such as folders or programs from the scan.

### *To manage exclusions:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option in the top panel. The Configure AntiVirus console opens.
3. Open the **Sentry** tab and then click the **Manage Exclusions** option. The Exclude List dialog opens.
4. The list of folders and files excluded from protection is displayed.
5. To add the folders or files you want to exclude from protection, click **Add Entry**.
6. In the Add New Exclude Entry dialog that appears, enter the path of the folder or file. If you are not sure of the path, click **Add Folder** or **Add File** to select the folders or files respectively.
7. Select the following options:
8. **Ignore from RealTime Scanner** - to exclude the selected file or folder from the real-time scan
9. **Ignore from Offline Scanner** - to exclude the selected file or folder from the offline scan

10. **Include Subfolders** - to exclude subfolders under the selected folder from the scan. This option is not available when a file is selected for exclusion.
11. Click **OK** to save the new entry and return to the Exclude List dialog.
12. To remove a file or folder from the Exclude list, select the entry in the list and click **Remove**.
13. Click **OK** to save the exclusion settings.

### 13. Configuring the Email Scanner

By default the email protection is enabled. The Email Scanner checks incoming and outgoing emails and ensures that no infected email reaches your mailbox. If an email contains a virus, the Email Scanner deletes or quarantines the infected attachments.

#### *To configure the Email Scanner:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
3. Click the **Email** tab.
4. Select the **Enable email protection on Windows startup** check box if you want the Email Scanner to start when your computer starts.
5. Select the required check boxes to scan **incoming** and **outgoing** emails. It is recommended that you select both these options so that all your emails are continuously monitored.

**Note:** If you select to scan incoming and outgoing emails without enabling the email protection, the emails are not scanned.

6. Under Advanced Protections, select the options you want to include in the scan. The options are described in the following table.

Option	Description
<b>Detect Spywares and Adwares</b>	Scans all email attachments for additional threats like Spyware, Adware, dialers, etc. Click on <b>customize</b> next to this option to select the type of threats to scan for and the action to take when such threats are found. <a href="#">See Defining Types of Threats to Scan</a> for details
<b>Enable Worm blocking</b>	Prevents any new mass-mailing virus that has entered your system from spreading and warns you of its presence. Click <b>customize</b> to define how to protect the system in case of a mass-mailing threat. <a href="#">See Configuring Worm Blocking</a> for details

<b>Protect against malicious attachments</b>	Treats binary attachments as malicious attachments. Click on <b>customize</b> to configure the action to take when such malicious attachments are found. <a href="#">See Scanning for Malicious Attachments</a> for details
--	--

7. Under Action to Take When a Virus is Found, select an action to be taken if an email is found to be infected with a virus. The actions are described in the following table.

Action	Description
<b>Clean automatically, prompt if cleaning is not possible</b>	Cleans the email without any interaction with you. If cleaning is not possible, you are prompted to define the action to be taken.
<b>Clean automatically, quarantine if cleaning is not possible</b>	Cleans the email without any interaction with you. If cleaning is not possible, moves the file to the Quarantine folder.
<b>Clean automatically, delete if cleaning is not possible</b>	Cleans the email without any interaction with you. If cleaning is not possible, the files are deleted.
<b>Prompt for action</b>	Prompts you to take action whenever an infected email arrives
<b>Do not take any action</b>	Reports the infection but does not take any action. This is not a recommended option unless you are an advanced user.
<b>Show alert</b>	Select the check box if you want an alert to be displayed when a virus is found

8. K7AntiVirus uses an in-built proxy server to process the emails. To configure the server settings, click the Email Settings button. See Configuring Email Server Settings for details
9. Once you have configured the Email Scanner, click Apply to save the changes.


## 14. Enabling the Email Scan

The Email Scan is enabled by default. If you have disabled it for any reason you can re-enable it.

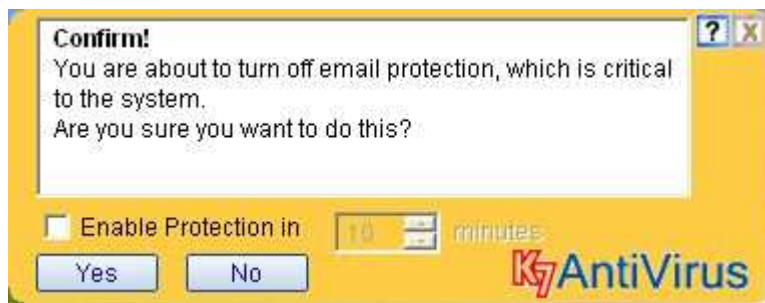
**Note:** It is recommended that you enable the Email Scan so that all incoming and outgoing mails are continuously monitored for viruses.

### To enable the Email Scan:

1. Open the K7AntiVirus main console.
2. The status of the Email Scanner is displayed in the main panel.
3. If the Email Scanner is currently disabled, click the status (**Disabled**). You are prompted to enable the email scan.

**Note:** To quickly turn on the email protection, right-click the  icon in the System Tray and click **Enable Email Scan**.

4. A message appears indicating that the email protection has been enabled.




## 15. Disabling the Email Scanner

The Email Scan is enabled by default. You can disable the Email Scan.

It is recommended that you *do not* disable the email scan, as your computer could get infected with viruses from emails.

### To disable the Email Scan:

1. Open the K7AntiVirus main console.
2. The status of the Email Scanner is displayed in the main panel.
3. If the Email Scanner is currently enabled, click the status (**Enabled**). You are prompted to disable the email scan.

**Note:** To quickly turn off the email protection, right-click the  icon in the System Tray, point to **K7Antivirus** and click **Disable Email Scan**.

4. A confirmation message appears.
5. If you are sure you want to disable the Email Scanner, click Yes.

6. If you want to disable the Email Scanner for a short period of time, check the Enable Protection in check box and enter the time in minutes.
7. Click No to leave the Email Scanner on.

## 16. Starting Email Scan Automatically


### *To start the email scan automatically:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus console opens.
3. Select the **Email** tab.
4. Select the **Enable email protection on Windows startup** check box.
5. Clear the check box if you do not want the email scan to start automatically when the system starts.
6. Select the **Scan incoming mails** and **Scan outgoing mails** check boxes to ensure that both incoming and outgoing mails are scanned always.
7. Click **Apply** to save the settings.
8. Click **Close** to close the Configure AntiVirus dialog.

## 17. Configuring Email Server Settings

K7AntiVirus uses an in-built proxy server to process the emails. Emails are scanned for viruses and spam before they are sent to your email client.

### *To configure the server settings:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
3. Select the **Email** tab and then click the **Email Settings** button. The Email Processing Settings dialog opens.
4. Select the required **Options**. The options are:
5. **Send Time Outs** - sends time outs to the mail server. Mails are scanned when they are received. In cases where the email scan takes more time than that required for the mail to be received, a time out is sent to the mail server to ensure that the session does not expire. This is a requirement for any mail server.
6. **Show separate icon when processing mails** - displays an icon () in the System Tray when the server processes the emails.  
If you want the icon to be displayed all the time, select the **Always** check box. If you want the icon to appear only when mails are being processed, select the **Only when processing emails** check box.
7. Click **OK** to save the settings and close the dialog.

## 18. Scanning for Malicious Attachments

Email viruses usually spread as binary attachments. The virus disguises itself as a non-program file. This option allows you detect a binary file arriving as an email attachment and take appropriate action on it.

### *To customize how K7AntiVirus handles malicious attachments:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus console opens.
3. In the **Email** tab, select the **Protect against malicious attachment** check box and click the **customize** option next to it. The Email Scan for Malicious Attachments dialog opens.
4. Select an option to specify what **Action** needs to be taken when a suspicious attachment is received. The actions that can be taken are detailed below.

Action	Description
<b>Prompt for action</b>	Prompts for action when a suspicious attachment is received
<b>Do not take any action</b>	Takes no action when a suspicious attachment is received
<b>Delete the attachment</b>	Deletes the suspicious attachment when it is received
<b>Quarantine the attachment</b>	Moves the suspicious attachment to the Quarantine folder

5. Select the Show Alert check box if you want an alert to appear when a malicious attachment is identified.
6. Click OK to save the settings.

## 19. Configuring the Worm Blocking Settings

Worms are similar to viruses in design, but spread from computer to computer unaided. The biggest danger of a worm is that it can replicate itself on your computer, and instead of your computer sending out a single worm, it could send out hundreds or thousands of copies of itself. An example would be a worm copying itself to every address in your Address book and sending itself out to everyone in your address book.

### *To configure how K7AntiVirus blocks worms:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus console opens.
3. Select the **Email** tab.

4. Select the Enable Worm blocking check box and click the customize option next to it. The Worm Blocking Settings dialog opens.
5. Select the If outgoing mails contain suspicious attachments check box and select an option to specify what Action needs to be taken when a worm is identified. The actions that can be taken are detailed below.


Action	Description
<b>Prompt for action</b>	Prompts the user for action when a worm is identified. This option is selected by default and is the recommended option.
<b>Do not take any action</b>	Takes no action when a worm is identified
<b>Delete the attachment</b>	Deletes the attachment containing the worm
<b>Quarantine the file</b>	Moves the attachment containing the worm to the Quarantine folder

6. Select the Show Alert check box if you want an alert to appear when a worm is identified.
7. If you want to be alerted when mails are sent continuously from your computer, select the Alert me if more than 'x' mails are sent continuously check box and enter the number in the space provided.
8. Click OK to save the worm blocking settings.

## 20. Managing Quarantined Files

The Quarantine feature temporarily isolates infected and suspicious files to a **quarantine folder** until appropriate action can be taken. Files that have been moved to the quarantine folder may contain a virus or maybe a malicious program. Update your K7AntiVirus and clean your computer before you restore a quarantined file to its original location.


### *To manage quarantined files:*

1. Open the K7AntiVirus console.
2. Click the **Manage Quarantine** option in the **Tools** panel. The Quarantine Manager console opens.
3. The list of **Quarantined Items** are displayed in the console. For each file, details such as the Filename, Original Location, Quarantined date, Problem Description and Status are displayed.
4. You can choose to do any of the following:
  - [Add files to the Quarantine folder](#)
  - [Delete quarantined files](#)
  - [Restore quarantined files to their original locations](#)
5. For more information on a file that is quarantined and its current status, select it in the list and click Properties.
6. Click the  to close the Quarantine Manager console.

## 20.1. Adding Files to the Quarantine Folder

If you suspect a file is infected, you can manually add the file to the Quarantine folder.

### *To add files to the Quarantine folder:*

1. Click the **Manage Quarantine** option in the **Tools** panel. The Quarantine Manager console opens.
2. Click **Add**. The Add Files to Quarantine dialog opens.
3. Browse to select the file you want to add to the Quarantine folder and click **Open**.
4. The file is added to the Quarantine folder and listed in the dialog.
5. You can take action on the file at a later point in time.
6. Click the  button to close the dialog.


## 20.2. Restoring Quarantined Files

You can restore quarantined files to their original folder. If you suspected a system file and moved it to the Quarantine folder, the associated program may not work properly. In such a case, you will need to move the file back to its original location for the required program to work properly.

### **Important:**

Before you restore a quarantined file, download product updates from the K7 Computing web site, run the scan and clean the file.


### *To restore quarantined files:*

1. Open the K7AntiVirus console.
2. Click the **Manage Quarantine** option in the **Tools** panel. The Quarantine Manager dialog opens.
3. Select the file you want to restore and click **Restore**.
4. A warning message appears informing you that a quarantined file is being restored.
5. Click **Yes** if you want to restore the file. The file is returned to its original location.
6. Click the  button to close the dialog.

### 20.3. Deleting Quarantined Files

If a file moved to the Quarantine folder contains a malicious program such as a Trojan or worm that cannot be cleaned, it is recommended that you delete it.

***To delete files from the Quarantine folder:***

1. Open the K7AntiVirus console.
2. Click the **Manage Quarantine** option in the **Tools** panel. The Quarantine Manager console opens.
3. Select the file in the quarantined list and click **Delete**.
4. A message confirming the deletion appears.
5. Click **OK** to permanently delete the file.
6. Click the  button to close the Quarantine Manager console.

## 21. Configuring Additional Scan Options

The Additional scan options allow you to protect your computer by scanning Messenger attachments, Office documents and Script viruses.

***To configure the additional scan options:***

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
3. Click the **Add Ons** tab.
4. You can configure the scanning of
5. Scripts, [see Configuring Script Scanning](#)
6. Instant Messenger programs, [see Configure Messenger Scanning](#)
7. Office files, [see Configuring Office Plugin Scanning](#)
8. Click **Apply** to save the settings.
9. Click **Close** to close the Configure AntiVirus dialog.

## 22. Configuring Messenger Scanning

Instant messenger scanning detects threats in inbound attachments that come via popular Instant Messenger programs.

### *To configure Messenger scanning:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
3. Click the **Add Ons** tab.
4. Select the messenger program you want to include in the protection. Currently, only Windows/MSN and Yahoo messenger are supported.
5. Select the type of **Action** that needs to be taken if an inbound attachment on the messenger program contains a threat. The actions are described in the following table.

Action	Description
<b>Prompt for action</b>	Prompts you for action when a threat is identified in an attachment
<b>Clean automatically, quarantine if unable to clean</b>	Cleans the attachment; quarantines the attachment if it is not able to clean it
<b>Clean automatically, delete if unable to clean</b>	Cleans the attachment; deletes the attachment if it is not able to clean it

6. Select the Always notify on scanning check box if you want the scanner to alert you when it scans attachments on a messenger program.
7. Click Apply to save the settings.

## 23. Configuring Script Scanning

Scripts can create, copy or delete files. They can also open your Windows registry. Script scanning automatically blocks harmful scripts from running on your computer.

### *To configure the script scanning:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
3. Click the **Add Ons** tab.
4. To enable script scanning, select the **Enable Script Protection** check box and then select the type of **action** to be taken if a malicious script is identified. The actions are described in the following table.

Action	Description
<b>Prompt when a malicious script is executed</b>	Prompts you for action when a malicious script is executed
<b>Deny access and notify about the activity</b>	Denies access to the script and alerts you when a malicious script is identified

- Click **Apply** to save the settings.

## 24. Configuring Office Plugin Scanning

You can configure the real-time scanner to scan all MSOffice files.

### *To configure Office Plugin scanning:*

- Open the K7AntiVirus console.
- Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
- Click the **Add Ons** tab.
- To scan all Word and Excel files opened by MSOffice, select the **Enable Office Plugin** check box.
- Click **Apply** to save the settings.

## 25. Configuring the Scan Settings

Before you perform a manual or scheduled scan, you need to specify the types of files to scan, the system areas to scan and the action to be taken in case a virus or threat is found.

### *To configure the scan settings:*

- Open the K7AntiVirus console.
- Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
- Select the **Scanner** tab.
- Select the types of files you want to scan in the **What to Scan** panel. The options are described in the following table.

Option	Description
<b>All Files</b>	Scans all the files in the system irrespective of the extension or type
<b>Automatic Identification</b>	Scans all <b>executable</b> (program) files, Microsoft Document files and Script files whether or not the extensions are specified or listed. Click <b>customize</b> next to this option to select which of these types of files you want to scan. <b>See <a href="#">Selecting the Types of Files to Scan</a></b> for details

<b>Specific Extensions</b>	Scans files with the specified file extensions. To specify the extension, click on the <b>customize</b> option that appears next to it. You can view, add or remove the extension you want to scan. <a href="#">See <u>Selecting the Types of File Extensions to Scan</u></a> for details
<b>Scan within compressed files</b>	Scans files within compressed files for viruses and threats
<b>Detect Spywares and adwares</b>	Scans the selected files for additional threats like Spyware, Adware, dialers, etc. Select the check box and then click on the <b>customize</b> option that appears next to it to configure the type of threats to scan and the action to take when a threat is found. <a href="#">See <u>Configuring the Types of Threats to Scan</u></a> for details

- In the System Areas to Scan panel, select the system areas you want to include in the scan. The options are detailed in the table below.

<b>Option</b>	<b>Description</b>
<b>Memory</b>	Checks the memory of your computer for the presence of viruses
<b>Boot Sectors</b>	Checks for boot viruses in the <b>Boot sectors</b> of the hard disk drive or Floppy you are scanning
<b>Partition Tables</b>	Checks for viruses in the <b>partition table</b> of the hard disk

- Select the Action to take if a virus is found. The actions are described in the following table.

<b>Action</b>	<b>Description</b>
<b>Clean Automatically, Quarantine if cleaning is not possible</b>	Cleans the file without any interaction with you and moves the file to the Quarantine folder if cleaning is not possible
<b>Clean Automatically, skip if unable to clean</b>	Cleans the file; if unable to clean the file does not take any action
<b>Report only</b>	Reports the infection in the file but does not take any action

- Click Apply to save the scan settings.

## 26. Selecting the Types of Files to Scan

K7AntiVirus can be configured to scan program files, Microsoft Office files and script-based files.

### *To select the types of files to scan:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
3. Select the **Scanner** tab.
4. Select the **Automatic Identification** option in the **What to Scan** panel and then click the **customize** option that appears next to it. The Types of Files to Scan dialog opens.
5. Select the required options. The options are described in the table below.

Option	Description
<b>All Program Files</b>	Scans all executable program files (.exe) in the system
<b>All files which contain macros</b>	Scans all files that contain macros whether or not the extensions are specified or listed
<b>Text or Script based files</b>	Scans all script files whether or not the extensions are specified or listed

6. Click OK to save the settings.

## 27. Adding File Extensions for the Scan

K7AntiVirus is configured to scan a default list of file types. You can add a file type to this list by providing the file extension such as .doc, .xls, etc.


### *To add file extensions for the scan:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel of the console. The Configure AntiVirus dialog opens.
3. Select the **Scanner** tab.
4. Select the **Specific Extensions** option in the **What to Scan** panel and then click the **customize** option that appears next to it. The Types of File Extensions to Scan dialog opens.
5. The list of file extensions configured is displayed.
6. Enter the file extension in the text box provided and click the **Add** button. If the file extension is not present in the list, it is added. If the new extension already exists in the list, a message appears.
7. To select *only* the default file extensions and discard all added extensions, click the **Default** button.
8. If you want to remove a file extension, select it in the list and click **Delete**.
9. Click **OK** to save the settings.


## 28. Configuring Scan Tasks

K7AntiVirus scans all files that are accessed by you or your computer. You can also schedule the automatic scanning of your computer so as to check for viruses and potential threats at specific intervals. Some scan tasks come pre-installed with your product and you need to assign schedules for them. You can create and schedule custom tasks, and schedule the pre-defined tasks to automatically run at a specific time.

### *To configure scan tasks:*

1. Double-click the  icon in the System Tray. The K7AntiVirus console opens.
2. Click the **Tasks** tab. The pre-defined scheduled tasks are displayed.
3. You can choose to do any of the following:
  - [Create custom scan tasks](#)
  - [Change the schedule of scan tasks](#)
  - [Delete scan tasks](#)
  - [Manually run a scan task](#)

## 29. Configuring the QuickScan

You can configure the predefined scan task "QuickScan" to scan important folders and files on your computer. The QuickScan can be run using the **Scan critical areas** option on the context menu that appears when you right-click the  icon in the System Tray.

### *To configure the QuickScan:*

1. Open the K7AntiVirus console.
2. Click the **Tasks** tab. The pre-defined scheduled tasks are displayed.
3. Select the **Quick Scan** task and click **Change**.
4. Specify a description for the scan task and select a scan option in the **What to Scan** tab. The options are described in the following table.

Option	Description
<b>Task Description</b>	Name of the scan task
<b>Scan all Harddisk drives</b>	Scans the <b>partition table</b> , <b>boot sector</b> , and all the files in all the hard disk drives present in your computer
<b>Scan the following drives/folders/files</b>	Scans the drives, folders and files specified. To add the folders, click the <b>Add Folders</b> button and browse to select the folder. To add files, click the <b>Add Files</b> button and browse to locate the files you want to scan. To delete any of the selected folders or files, select it in the list and click <b>Delete Entry</b> .

5. In the Scan Settings tab, select how you want to scan the selected files and folders. See Configuring Scan Settings for details

6. To configure how you want the scan task to run, select the options in the How to Scan tab.  
See Customising a Scan task for details
7. Click the Schedule tab and schedule the time at which you want the scan to run.  
See Scheduling a Scan task for details
8. Click Apply to save the settings for the custom scan task.
9. Click the Close button to close the Configure Scan Tasks dialog.

## 30. Creating Custom Scan Tasks

K7AntiVirus allows you to create custom scan tasks and schedule them to run at a specific time.

### *To create a custom scan task:*

1. Open the K7AntiVirus console.
2. Click the **Tasks** tab. The predefined scheduled tasks are displayed.
3. Click the **Add** button. The Configure Scan Tasks dialog opens.
4. Specify a description for the scan task and select a scan option in the **What to Scan** tab. The options are described in the following table.

Option	Description
<b>Task Description</b>	Name of the scan task
<b>Scan all Harddisk drives</b>	Scans the <b>partition table</b> , <b>boot sector</b> , and all the files in all the hard disk drives present in your computer
<b>Scan the following drives/folders/files</b>	Scans the drives, folders and files specified. To add the folders, click the <b>Add Folders</b> button and browse to select the folder. To add files, click the <b>Add Files</b> button and browse to locate the files you want to scan. To delete any of the selected folders or files, select it in the list and click <b>Delete Entry</b> .

5. In the Scan Settings tab, select how you want to scan the selected files and folders.  
See Configuring Scan Settings for details
6. To configure how you want the scan task to run, select the options in the How to Scan tab.  
See Customising a Scan task for details
7. Click the Schedule tab and schedule the time at which you want the scan to run.  
See Scheduling a Scan task for details
8. Click Apply to save the settings for the custom scan task.
9. Click the Close button to close the Configure Scan Tasks dialog.

## 31. Customizing a Scan Task

You can customize a scan task to run in the background or to be interactive.

### *To select how you want a scan task to run:*

1. Open the K7AntiVirus console.
2. Click the **Tasks** tab.
3. Select the scan task and click the **Change** button. The Configure Scan Tasks dialog opens.
4. Select the **How to Scan** tab.
5. To configure when you want to enable the scan task, use the options in the **When to Enable the Scan Task** panel. The options are described in the following table.

Option	Description
<b>Enable Task only when one or more users are logged on</b>	Enables the scan task <i>only</i> when one or more users are logged onto the computer
<b>Enable Task only whether the user is logged on or not</b>	Enables the scan task all the time, even if the user has not logged onto the computer

6. To configure how you want the scanner to run, use the options in the How to Start the Scanner panel. The options are described in the following table.

Option	Description
<b>Scan silently in the background</b>	Runs the scan task in the background without interfering with your work
<b>Run as minimized window</b>	Runs the scan task with the task window minimized so that you can open it whenever you want to view the status of the scan
<b>Run as normal window</b>	Runs the scan task with the window displayed while the scan is in progress

7. To configure what actions a user can take on a scan task, use the options in the How User can Control the Scanning panel. The options are described in the following table.

Option	Description
<b>Non Admin user can take action on reported files</b>	Select this option if you want to allow a user who does not have Administrator rights to take action on files that are reported to have viruses or are potential threats
<b>Non Admin user can stop the scan</b>	Select this option if you want to allow a user who does not have Administrator rights to be able to stop the scan while it is in progress

8. To select how you want the scan completion to be handled, select an option in the How to Finish Scanning panel. The options are described in the table below.

Option	Description
<b>Show completion of scan always</b>	Displays the Scan Summary window once the scan task is completed, whether a virus is detected or not
<b>Show completion of scan only when virus is found</b>	Displays the Scan Summary window on completion of the scan task and a virus is detected. If no virus is found, the scan task is not reported.
<b>Do not show the Scan Completion Report</b>	Select this option if you do not want to view the Scan Completion Report

9. Click Apply to save the scan options.

## 32. Scheduling Scan Tasks

Scanning selected areas of your computer for malicious objects is one of the key steps in protecting your computer. You can configure K7AntiVirus to automatically run the custom or pre-defined scan tasks at a specified time interval. This ensures that the scanning takes place without intervention from you.

### *To schedule a scan task:*

1. Click the **Schedule** tab.
2. Select the **Enable Scheduling of this task** check box to ensure the task runs.
3. Select the frequency at which you want the task to run in the **Schedule Task** drop-down. You can schedule the task to run everyday, on certain days of the week or on any one day in a month. The options in the panel below appear according to the frequency selected.
4. Use the **Start Time** controls to set the time of the day when you want the task to run.
5. Select how often you want the scan to run in the **Schedule Task** panel, and select additional options that appear in the panel based on your choice. The options that appear based on your choice are:
  6. **Daily** - specify the number of days between scans in the **Schedule Task Daily** panel
  7. **Weekly** - specify the number of weeks between scans, and the day(s) of the week when you want the scan task to run in the **Schedule Task Weekly** panel
  8. **Monthly** - specify the day of the month on which you want the scan to run in the **Schedule Task Monthly** panel
9. Click the **Apply** button to save the schedule.
10. Click **Close** to close the Configure Scan Tasks dialog.

## 33. Changing the Schedule for a Scan Task

Some scan tasks come pre-installed with the product. You will need to assign the schedule for these scan tasks. In addition to the pre-defined tasks you can create custom scan tasks. You can change the schedule for a custom or pre-defined scan task.

### *To change the schedule for a scan task:*

1. Open the K7AntiVirus console.
2. Click the **Tasks** tab. The predefined and custom scan tasks are displayed.
3. Select the scan task for which you want to change the schedule and click the **Change** button. The Configure Scan Tasks dialog opens.
4. To customize how the scan must run, select the required options in the **How to Scan** tab.  
[See Customising a Scan Task](#) for details
5. To set the schedule for the scan task, select the required options in the **Schedule** tab.  
[See Scheduling Scan Tasks](#) for details
6. Click **Apply** to save the changes.
7. Click **Close** to close the Configure Scan Tasks dialog.

## 34. Manually Running a Scan Task

In addition to scheduling the automatic scanning of your computer so as to check for viruses and potential threats at specific intervals, you can manually run a scan task at any time.

### *To manually run a scan task:*

1. Open the K7AntiVirus console.
2. Click the **Tasks** tab. The scheduled tasks are displayed.
3. Select a scan task in the list and click **Run Now**. The scan task is executed and the results displayed.

## 35. Deleting Scan Tasks

You can delete custom scan tasks.

**Note:** You are not allowed to delete the pre-defined scan tasks.

### *To delete a scan task:*


1. Open the K7AntiVirus console.
2. Click the **Tasks** tab. The predefined and custom scan tasks are displayed.
3. Select the custom scan task you want to delete and click the **Delete** button.
4. The selected scan task is deleted after a confirmation.
5. If you try to delete a pre-defined scan task, you are warned.

## 36. Running QuickScan

The Quick Scan can be configured to scan important drives and folders (that is, the c: drive, **Windows** and **Program Files** folders) on your computer for viruses and other potential threats.

[See Configuring the QuickScan](#) for more information

### *To run a quick scan of your entire computer:*

1. Right-click the  icon in the System Tray and select the **Scan Critical Areas** option. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
2. The folders that are configured are scanned and the result of the scan is displayed in the K7AntiVirus Scanner dialog.

## 37. Scanning Your Entire Computer

### *To manually scan your entire computer:*

1. Open the K7AntiVirus console.
2. Do one of the following:
3. Click the **Last System Scan** option and then click the **Not Done** or status option that appears adjacent to it
4. Click the **Scanner** tab, select the check box corresponding to 'My Computer' and click **Start Scan**
5. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
6. All the drives and folders in your computer are scanned and the result of the scan is displayed in the K7AntiVirus Scanner dialog. The scanning is carried out based on the settings configured.  
[See Configuring Scan Settings](#) for details
7. If there are viruses in any of the drives or folders, the details appear in the dialog.
8. To clean an infected file, select it in the list and click **Clean**.
9. If you want to delete the file containing the virus, select the infected file and click **Delete**.
10. To quarantine an infected file, select it in the list and click **Quarantine**.
11. If there is no virus in your computer, a message appears.
12. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.
13. Click the **Exit** button to close the K7AntiVirus Scanner dialog.

## 38. Scanning a Folder

You can scan the entire contents of a removable drive, floppy disk, folder (including sub-folders) or any of your computer's drives. When you manually scan a drive or folder, K7AntiVirus scans all the file types in the selected drive or folder and executes the necessary actions according to the Scan settings. [See Configuring the Scan Settings](#)

***To scan a folder:***

1. Open Windows Explorer.
2. Right-click on the folder you want to scan and click **K7AntiVirus**.
3. All the files in the selected folder are scanned and the results of the scan displayed in the K7AntiVirus Scanner dialog. If there are viruses in the selected folder, the details appear in the dialog.
4. To clean an infected file, select it in the list and click **Clean**.
5. If you want to delete the file containing the virus, select the infected file and click **Delete**.
6. To quarantine an infected file, select it in the list and click **Quarantine**.
7. If there is no virus in the selected folder(s), a message appears.
8. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.

**39. Scanning a File**

You can manually scan a single file. K7AntiVirus scans the file and executes the necessary actions according to the Scan settings. [See Configuring the Scan Settings](#)

***To scan a file:***

1. Open Windows Explorer.
2. Right-click on the file you want to scan and click **K7AntiVirus**.
3. The selected file is scanned and the results of the scan displayed in the K7AntiVirus Scanner dialog. If the selected file contains a virus, the details appear in the dialog.
4. To clean the infected file, select it in the list and click **Clean**.
5. If you want to delete the file containing the virus, select the file and click **Delete**.
6. To quarantine an infected file, select it in the list and click **Quarantine**.
7. If there is no virus in the selected file, a message appears.
8. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.

**40. Scanning Multiple Locations**

When you want to manually scan multiple drives or folders on your computer (and not the entire computer) you can specify the folders you want to scan.

***To select multiple folders for scanning:***

1. Open the K7AntiVirus console.
2. Click the **Scanner** tab. The folders in your computer are displayed. To expand a folder, click the '+' icon next to the folder name. The icon toggles to '-'. Click the '-' icon to collapse the folder.
3. Select the check boxes corresponding to the folders you want to scan and click **Start Scan**. The

K7AntiVirus Scanner dialog opens and displays the progress of the scan.

4. The selected folders are scanned and the results of the scan are displayed in the K7AntiVirus Scanner dialog. If there are viruses in the selected folders, the details appear in the dialog.
5. To clean an infected file, select it in the list and click **Clean**.
6. If you want to delete the file containing the virus, select the infected file and click **Delete**.
7. To quarantine an infected file, select it in the list and click **Quarantine**.
8. If there is no virus in the selected folders, a message appears.
9. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.
10. To configure the settings for the scan, click the **Settings** button. The Configure AntiVirus dialog appears.
11. Select the options for the scan and click **Close**. *See [Configuring Scan Settings](#) for details*
12. If you want to reset the scan settings, click the **Reset** button.
13. Click the **Exit** button to close the K7AntiVirus Scanner dialog.

## 41. Configuring the General Scan Settings

K7AntiVirus allows you to configure some general scan settings.

### *To configure the general scan settings:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
3. Select the **General** tab.
4. Select the required **Options**. The options are described in the following table.

Option	Description
<b>Warn when Virus Database expires</b>	Displays an alert when the Virus definition is not updated for more than 5 days
<b>Create a backup file in quarantine before cleaning</b>	Creates a copy of the quarantined file in the same folder, when the clean option is selected
<b>Quarantine only unique files</b>	Checks if the file already exists in the Quarantine folder before moving it
<b>Delete files from Quarantine after 'x' days</b>	Automatically deletes the files present in the Quarantine folder after the specified 'x' days

<b>Enable Shortcut menu in Status Bar</b>	Displays the K7AntiVirus option in the shortcut menu that appears when you right-click on the K7 System Tray icon
<b>Automatically submit security risk or suspicious files</b>	Automatically uploads any malicious files received via email to the K7Computing server for analysis. Selecting this option enables your product to participate in such submissions.

5. To set the Log Options, see **Configuring the Log Options**.

6. Click **Apply** to save the scan settings.

## 42. Configuring the Log Options

K7AntiVirus allows you to record the various activities of the product.

*To configure the log options:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option on the top panel. The Configure AntiVirus dialog opens.
3. Select the **General** tab.
4. To set the **Log Options**, select the **Enable Logging** check box and then select the log options. The options are detailed in the following table.

<b>Option</b>	<b>Description</b>
<b>Purge Log files more than 'x' days</b>	Deletes the contents of the log when it has been in your computer for more than 'x' days
<b>Log Virus Detection</b>	Saves details of viruses detected through Sentry, Email Scanner, Manual scans, Tasks, Script Blocking and Worm Blocking to a file
<b>Scan Summary</b>	Saves details of every Scan completion such as total number of files scanned, total number of files infected, etc., to a file
<b>Log Protection Disable/Enable</b>	Logs details such as when the Sentry, System Monitor or Email Protection is disabled or enabled
<b>Completion of Tasks</b>	Saves details of the completion of scan tasks to a file

5. Click **Apply** to save the log settings.

### 43. Viewing Virus Information on the Web

The K7 Computing website ([www.k7computing.com](http://www.k7computing.com)) is updated with the latest information on new viruses and their threat levels everyday.

***To view virus information on the Web:***


1. Open the K7AntiVirus console.
2. Click the **View Virus Information** option in the **Tools** panel. The Virus Encyclopedia on [www.k7computing.com](http://www.k7computing.com) opens in your Internet browser. The page lists the virus names and their threat levels.
3. Use the links on the web page to access the virus information you want to view.
4. When you finish viewing the virus information close your browser window.



### 44. Viewing News

You can view the latest news on security threats and new viruses.

***To view the latest news:***

1. Open the K7AntiVirus console.
2. Click the  **Open News** option in the **Tools** panel. The latest news appears in a **message** box.
3. Click **x** to close the message.

### 45. Using the Report Viewer

K7AntiVirus maintains logs of all virus detections and activity it has monitored. You can review this information.


The Report viewer displays the history of activities of your product. Using the information in the Log Viewer, you can view detailed information recorded in each log by selecting the category in the left column and viewing the details in the right pane.

***To open the Report Viewer:***

1. Open the K7AntiVirus console.
2. Click the **Activity Log** option in the **Tools** panel. The K7AntiVirus Reports console opens.
3. Select K7AntiVirus in the left pane.

4. Click the (+) icon to expand the module to view the log options.
5. Click on a log option and its details appear on the right pane.
6. The following options are available in the Log Viewer menu:

Option	Description
<b>Save</b>	Saves the log details to a text file for later use. Enter the name and select the location in which you want to save the file.
<b>Refresh</b>	Refreshes the Log Viewer with the most recent logged details
<b>Clear</b>	Purges the contents of the Log file
<b>Help</b>	Opens this help

7. Click the  button to close the K7AntiVirus Reports console.

## 46. Logging AntiVirus Activities

K7AntiVirus allows you to specify whether you want to enable or disable logging of antivirus activities. Entries are created when a virus or other malicious program is detected. Virus log entries also contain the time the virus was detected, the type of scan that detected the virus, the location of the virus, the name of the file that contains the virus, the description of the problem, the status of the file, and the action taken.

### *To configure the log options:*

1. Open the K7AntiVirus console.
2. Click the **Settings** option in the top panel. The Configure AntiVirus dialog opens.
3. Select the **General** tab.
4. To set the **Log Options**, select the **Enable Logging** check box.  
If you do not want to log the AntiVirus activities, clear this check box.
5. Select the activities you want to log. The options are detailed in the following table.

Option	Description
<b>Purge Log files more than 'x' days</b>	Deletes the contents of the log when it has been in your computer for more than 'x' days
<b>Log Virus Detection</b>	Saves details of viruses detected through Sentry, Email Scanner, Manual scans, Tasks, Script Blocking and Worm Blocking to a file
<b>Scan Summary</b>	Saves details of every Scan completion such as total number of files scanned, total number of files infected, etc., to a file

<b>Log Protection Disable/Enable</b>	Logs details such as when the Sentry or Email Protection is disabled or enabled
<b>Completion of Tasks</b>	Saves details of the completion of scan tasks to a file

6. Click Apply to save the log settings.


## 47. Viewing the AntiVirus Log

You can check the AntiVirus activity log to see which tasks were performed and the results of those tasks.

### *To view the AntiVirus activity log:*

1. Open the K7AntiVirus console.
2. Click the **Activity Log** option on the **Tools** panel. The K7AntiVirus Reports console opens.
3. Select **K7AntiVirus** in the left pane. The K7AntiVirus Report appears in the right pane.
4. Click the (+) icon to expand the 'K7AntiVirus' module and view the log options. The options are described in the following table.

Option	Description
<b>Virus Found Events</b>	Displays events in which a virus was detected. The details such as Date & Time of detection, User name, Program that detected the virus, Location of infected file, Problem Description, current Status of infected file and Action taken are displayed.
<b>Scan Summary</b>	Displays the scan details - Date & Time of scan, User, Scan Type, Description (usually time of completion of scan, and Summary of the scan (number of files analyzed, number of files scanned and number of infected files))
<b>Other Events</b>	Displays event occurrences such as enabling, disabling and loading of the Email and Virus scan. The details displayed include Date & Time of occurrence, User name, Program that was loaded/enabled/disabled and Description of the event.

5. Click on the required option and the details appear in the right pane.
6. Click Refresh to refresh the event list.
7. To clear all the log entries, click the Clear button. The system will clear all the antivirus log entries after receiving a confirmation from you.
8. When you finish viewing the information, click the  button.

## Glossary of Terms

### A

**Adware:** Adware are programs designed to launch advertisements, often pop-up banners, on host machines and/or to re-direct search engine results to promotional web sites. Adware programs are often built into freeware or shareware programs, where the adware forms an indirect 'price' for using the free program.

### B

**Boot sector:** The boot sector is the area on a hard disk and floppy disks containing instructions that are executed during the boot process, i.e. when the PC starts. Among other things, the boot sector specifies the location of the operating system files. On a hard disk, the boot sector is the first sector(s) on the bootable partition, i.e. the partition containing the system files. On a floppy disk, the boot sector is the first sector on the disk: all floppy disks contain a boot sector, even if they are just data disks.

### D

**Dialers:** A type of online scam using unauthorized use of pay-per-use Internet services, which are commonly pornographic web sites. The dialers installed by hackers initiate modem connections from your computer to the number for the pay service. These phone numbers often have very high rates and the user is forced to pay enormous telephone bills.

### F

**Firewall:** A firewall provides a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic coming into and going out of your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer. The firewall protects against attacks malicious hackers commonly use including: Ping of Death, IP conflict, SYN flooding, and others.

### J

**Joke programs:** Joke programs are programs that alter or interrupt the normal behavior of your computer, creating a general distraction or nuisance.

### K

**Keylogger:** A keylogger can be used by a third-party to obtain confidential data (login details, passwords, credit card numbers, PINs, etc.) by intercepting key presses. Backdoor Trojans typically come with a built-in keylogger; and the confidential data is relayed to a remote hacker to be used to make money illegally or gain unauthorized access to a network or other company resource.

### M

**Malicious code:** Malicious code refers to any program that is deliberately created to perform an unauthorized, often harmful, action.

**Malware:** Malware (short for malicious software) refers to any program that is deliberately created to perform an unauthorized, often harmful, action.

## P

**Partition table:** A Partition table holds information on the number of partitions, their size and which one is 'active' (i.e. which one contains the operating system used to boot the machine). It is present in the MBR (Master Boot Record), which is the first sector on a hard disk.

**Phishing:** Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

**POP3:** Post Office Protocol 3 ( POP3 ) is an Internet standard protocol for receiving email from a remote server. The server receives mail on your behalf and stores it until you check your mailbox and download the messages. Nearly all subscribers to individual Internet service provider e-mail accounts access their e-mail with client software that uses POP3.

**Proxy server:** A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes, usually to view websites normally not allowed, such as game, sites pornography sites at work or school.

## Q

**Quarantine folder:** A Quarantine folder is a restricted access folder into which K7TotalSecurity moves un-cleanable files and malicious programs it detects during a real-time or manual scan.

## S

**Scan task:** A scan task is a quick and convenient way to perform a variety of virus scanning. Scan tasks automate routine antivirus maintenance procedures on your desktop and improves antivirus management efficiency.

**Spyware:** Spyware refers to software that is designed to gather data from a computer and forward it to a third party without the consent or knowledge of the computer's owner. This includes monitoring keystrokes, collecting confidential information (passwords, credit card numbers, PIN numbers, etc.), harvesting e-mail addresses or tracking browsing habits. There's a further by-product, of course: such activities inevitably affect network performance, slowing down the system and thereby affecting the whole business process.

## T

**TCP:** TCP, one of the main protocols in TCP/IP networks, enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**Trojan horse:** A Trojan horse is a program that contains malicious or harmful code inside an apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. A Trojan horse may be widely redistributed as part of a computer virus. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

## U

**UDP:** UDP, a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

## V

**Virus:** A computer virus attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Much like human viruses, computer viruses can range in severity: Some viruses cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

**Virus definition:** Virus definitions (or signatures) contain a unique sequence of bytes used by an anti-virus program to identify each piece of malicious code. Signature analysis is one of the key methods used to find and remove malicious code.

## W

**Worms:** Worms are generally considered to be a subset of viruses, but with key differences. A worm is a computer program that replicates, but does not infect other files: instead, it installs itself on a victim computer and then looks for a way to spread to other computers.