

# **Printed Documentation**

---



## Table of Contents

K7AntiVirus Plus Help .....	1
Feature Summary .....	2
Online Help Conventions.....	3
Getting Started .....	5
Activating Your Product.....	5
Un-Installing K7AntiVirus Plus .....	7
Opening the Main Console .....	7
Overview of the Main Console.....	8
Viewing the Current Status of Your Protection.....	9
Enabling K7AntiVirus Plus .....	9
Disabling K7AntiVirus Plus .....	10
Updating Your Product.....	15
Updating Your Product.....	15
Automatically Checking for Updates.....	15
Manually Checking for Updates .....	16
Disabling Automatic Updates .....	17
Protecting Against Viruses .....	19
Managing the Virus Protection.....	19
Configuring the AntiMalware.....	20
Configuring the Real-Time Scanner .....	20
Configuring the Real-Time Scanner .....	20

## Printed Documentation

Enabling Real-Time Scan .....	21
Disabling Real-Time Scan .....	22
Configuring the Types of Threats to Scan .....	23
Managing Exclusions.....	24
Configuring the Email Scanner.....	25
Configuring the Email Scanner.....	25
Enabling the Email Scan.....	26
Disabling the Email Scanner.....	27
Configuring Email Server Settings .....	28
Scanning for Malicious Attachments.....	29
Configuring the Worm Blocking Settings .....	30
Configuring the System Monitor .....	30
Configuring the System Monitor .....	31
Enabling the System Monitor .....	32
Disabling the System Monitor .....	32
Configuring the System Check Points .....	33
Viewing System Monitor Events .....	34
Managing Quarantined Files.....	34
Managing Quarantined Files.....	34
Adding Files to the Quarantine Folder.....	35
Restoring Quarantined Files .....	35
Deleting Quarantined Files .....	36
Configuring Additional Scan Options .....	36

Configuring Additional Scan Options ..... 36

Configuring Messenger Scanning..... 37

Configuring Script Scanning..... 38

Configuring Office Plugin Scanning ..... 38

Configuring the Scan Settings ..... 38

    Configuring the Scan Settings ..... 39

    Selecting the Types of Files to Scan..... 40

    Adding File Extensions for the Scan ..... 41

Managing Scanner Tasks ..... 41

    Configuring Scan Tasks..... 41

    Configuring the QuickScan..... 42

    Creating Custom Scan Tasks ..... 43

    Customizing a Scan Task..... 44

    Scheduling Scan Tasks ..... 45

    Changing the Schedule for a Scan Task ..... 46

    Manually Running a Scan Task ..... 47

    Deleting Scan Tasks..... 47

Scanning Your Computer ..... 47

    Running QuickScan ..... 47

    Running Rootkits Scanner ..... 48

    Running Tracking Cookies Scanner ..... 48

    Scanning Your Entire Computer..... 49

    Scanning a Folder ..... 50

## Printed Documentation

Scanning a File.....	50
Scanning Multiple Locations .....	51
Configuring the General Scan Settings.....	52
Configuring the Log Options .....	52
Viewing Virus Information on the Web .....	53
MISC.....	63
Activation Reminder.....	63
Privacy Service ActiveX Alert.....	63
Adding an Exclude Entry .....	64
AppInit DLL Value.....	64
Boot Execute Value .....	65
Browser Settings .....	65
Context Menu Handler.....	66
Control Panel Listings.....	66
Customizing a Scan Task.....	67
Configuring Rules.....	68
Email Virus Alerts .....	70
Host File.....	71
IE Browser Helper .....	71
IE Extensions .....	72
IE Search Hooks .....	72
IE Security Settings.....	73
IE Toolbars.....	73

IE Trusted Site ..... 74

IE URL Settings ..... 74

IE Zone Settings..... 75

Privacy Service Java Applet Alert ..... 75

NT Load and Run Values ..... 76

Configuring the Scan Settings ..... 76

ScreenSaver Value ..... 78

Script Alerts ..... 78

Shared Task Scheduler..... 79

Shell Execute Hooks ..... 80

Shell Object Delay Load..... 80

Shell Open Command ..... 81

Accessing the Context Menu ..... 82

Start Up Folders ..... 82

System Check Points..... 83

System Monitor Alerts ..... 84

System Monitor Blocked Entries ..... 84

System Tray Icon ..... 85

System Monitor Alert ..... 85

Update Prompt ..... 86

User Init Value ..... 86

User Shell Folders..... 87

Win.Ini ..... 88

## Printed Documentation

WinLogon Values .....	88
Windows Security Settings .....	89
Windows Services.....	89
Windows Shell .....	90
Worm Block Alert.....	90
Glossary .....	91
Index .....	95

## K7AntiVirus Plus Help

Welcome to K7AntiVirus Plus.

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 Plus** is a powerful but easy-to-use comprehensive solution that offers protection against viruses.

K7AntiVirus Plus helps you to safeguard your computer from virus threats through the network, email or Internet. It protects your computer from Viruses, Trojan, 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 Plus 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.

### More Information

[Features of K7AntiVirus Plus](#)

[Overview of the Main Console](#)

---

## Feature Summary

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

The features in K7AntiVirus Plus include:

- **Auto-protection** - loads into memory when Windows starts and provides continuous protection while you work; and monitors your system for unusual symptoms that may indicate an active threat
- **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
- **Carnivore Drive-by-download blocking** - Detects and blocks many zero day browser exploits that include automatic downloading of malicious software
- **Carnivore Zero day threat blocking** - Carnivore, a new pro-active defense mechanism allows the product to detect and block zero day attacks from PDF based exploits
- **System security setting protection** - prevents unauthorized changes to the system security settings
- **Device Blocking** - Allows you to set read/write/execute access to external devices such as USB sticks, CD/DVD, Floppy disks
- **AutoScan USB** - Scans USB disks as soon as they are plugged in
- **AutoRun Protection** - AutoRun Protection disables the autorun feature for all removable drives on your computer
- **USB Vaccination** - This feature ensures that once a USB drive is 'vaccinated', it cannot automatically infect any pc on which it is used using autorun mechanism
- **USB Password Protection** - Allows you to set password protection on the system on which the product is installed before accessing the device type

- **Spyware and adware protection** - detects and removes spyware, adware, keyloggers and other Internet threats that get installed secretly while downloading programs from the Internet
  - **Vulnerability Scanner** - Detects and informs the users about vulnerable application modules that can be used by attackers to compromise the system
  - **Vulnerability Patches** - Identifies vulnerabilities and provides steps to patch the system against vulnerabilities
  - **K7 Boot CD** - The K7 product cd can now be used as a bootable rescue disc to scan your system and remove viruses when your system does not boot in the normal mode due to malware infection
  - **Desktop Update Manager** - This feature allows you to download updates in one system and push the updates to other systems using the Desktop Update Manager
  - **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
  - **RootKits Scanner** - Deep scan for rootkits can be used to scan the system generically for rootkits.
  - **Tracking cookies** -bits of information stored on a computer by a browser which enable a website to uniquely identify a user .
  - **Unwanted Registry entries** - Scans the windows registry for registry entries left behind by malicious or unwanted programs.
  - **Scan unwanted files** - Scans for the residual files left behind by malicious or unwanted programs.
  - **Password Protection** - Users now have the option to set a password for changing the settings, disabling features and uninstalling the product
  - **Tools** - The product comes with many useful tools like Windows Temp file cleaner, Internet Explorer History cleaner, Virtual Keyboard etc.
- 

## 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 **Security Center** tab, select **AntiVirus Protection** choose **Real Time File Scanner** and click the **Configure** button next to it.

Important notes are shown like this:

**Note:**

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

## Printed Documentation

Warnings about important steps to take are shown like this:



It is recommended that you *do not* disable K7AntiVirus Plus, as it could lead to your system getting infected.

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, Trojans, and harmful scripts.

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

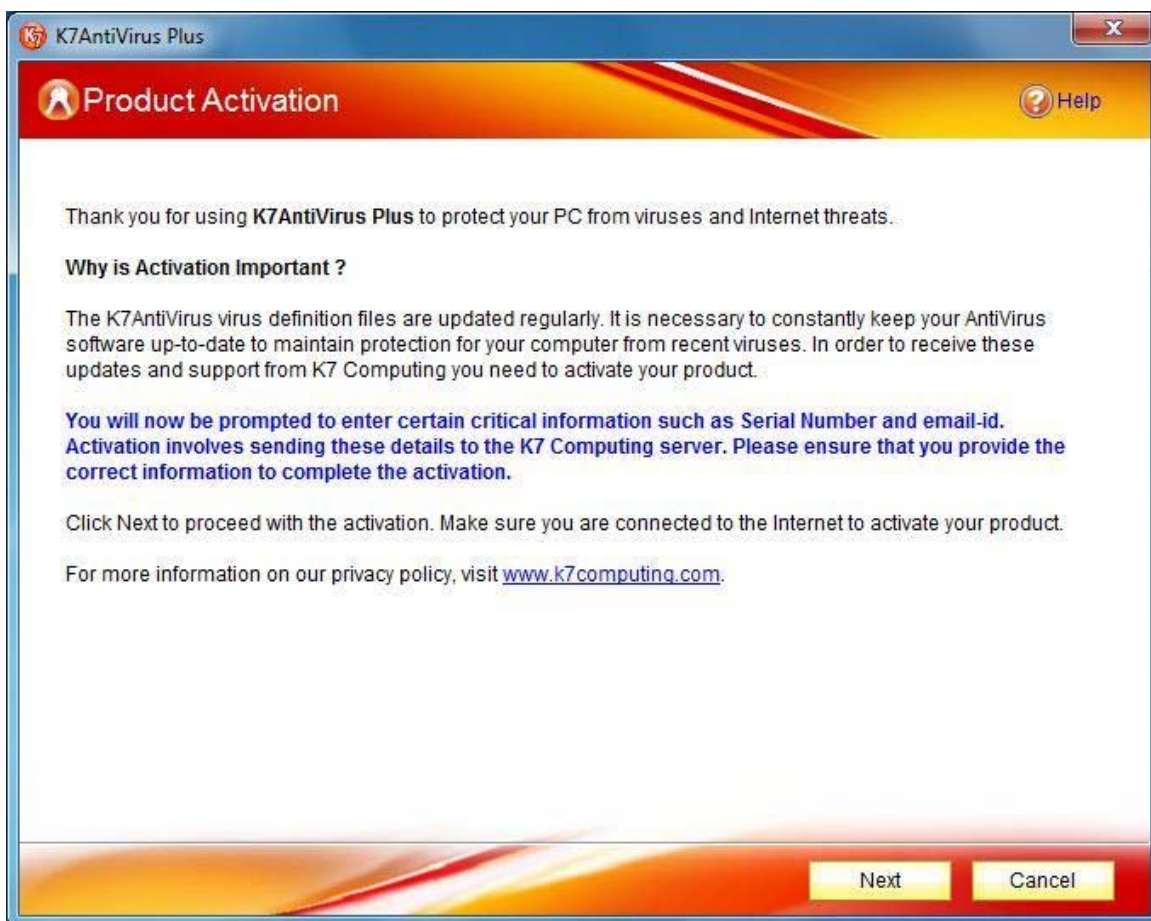
---

# Getting Started

## Activating Your Product

Activation is essential keep your product up-to-date so as to protect your computer from newly discovered threats. The K7AntiVirus Plus 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 when you are first prompted, you will receive an alert every day till you activate the product.



To activate the product later, click the **Cancel** button.

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

***To activate your product with a serial number from the alert:***

1. Click the **Next** button on the Product activation screen.
2. If you have purchased the subscription click on the radio option **I have purchased the subscription and have a valid serial number.**

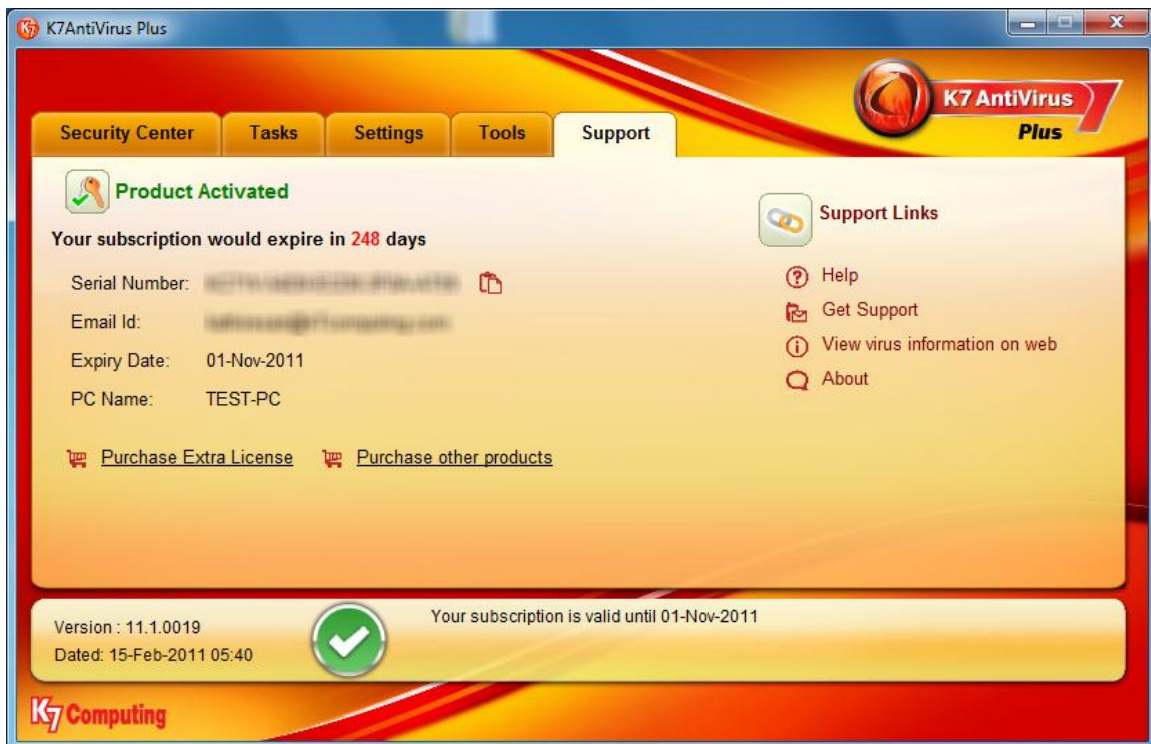
## Printed Documentation

3. Enter the Activation details, your **Name, Email address**.
4. Enter the **Serial Number** of your product and click **Next**.
5. In the confirmation screen if you want to change any details click the **Back** button.
6. Make sure you are connected to the Internet .Select **Next** button to proceed activation.
7. On successful Activation, you will receive your account information and License validity details.

### *To activate your product as Evaluation product:*

1. Click the **Next** button on the Product activation screen.
2. Click on the radio option **I want to evaluate the product before purchasing it**.
3. Enter the Activation details, your **Name, Email address**.
4. In the confirmation screen if you want to change any details click the **Back** button.
5. Make sure you are connected to the Internet .Select **Next** button to proceed activation.
6. On successful Activation, you will receive your account information and License validity details.

Once you have activated your product, your Licence information is displayed on the K7AntiVirus Plus main console.



## Un-Installing K7AntiVirus Plus

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

**Note:**

To un-install K7AntiVirus Plus you must be logged on as an Administrator. Also, you will need to restart your computer after removing the software.



**To remove K7AntiVirus Plus:**

1. Click **Start->Settings->Control Panel**.
2. In the Control Panel, double-click the **Add or Remove Programs** option.
3. Select **K7AntiVirus Plus** 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.

---

## Opening the Main Console

You can start K7AntiVirus Plus in any of the following ways:

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

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

*See* Overview of the Main Console

---

## Overview of the Main Console

The layout of the K7AntiVirus Plus main console is explained in the following figure.



The main console has two distinct areas - one is the **Tabs section** and the other is the **Info Bar**.

The **Info Bar** is the area which provides the status information of the product like Version number, Expiry status, Protection Status etc.

Also it provides a short help on each of the options as you move the mouse over them.

The Tabs sections contains several tabs - **Security Center**, **Tasks**, **Settings**, **Tools** and **Support**

The **Security Center Tab** provides the overall status of the product components and allows you to enable disable or configure the components

The **Tasks Tab** provides you with several options that include scanning the system, updating the product, managing Quarantined files, Vulnerability scan etc.

Configuration settings for all the components can be accessed either from the **Security Center Tab** or exclusively from the **Settings** tab.

Several useful tools like USB Vaccination, Virtual keyboard etc can be accessed from the **Tools Tab**

Users can purchase additional licenses, activate the product, view Help topics and access support using the **Support Tab**

---

## Viewing the Current Status of Your Protection

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

*To view the current status:*

1. Open the K7AntiVirus Plus main console.
2. Click the **Security Center** tab in the main section which is the default tab.
3. The **Security Status** panel indicates which of the components of your product are enabled or disabled.



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

4. The silver **Information bar** displays the product version and the virus definition version.
- 

## Enabling K7AntiVirus Plus

K7AntiVirus Plus is enabled by default. If you disable it for any reason, you can enable it again.



It is recommended that you enable K7AntiVirus Plus so that your computer is protected from viruses and threats continuously.

*To enable K7AntiVirus Plus:*

1. Right-click the  icon in the System Tray.
2. Select **Enable Product Protection**.


## Disabling K7AntiVirus Plus

K7AntiVirus Plus is enabled by default. You can disable the product.



It is recommended that you *do not* disable K7AntiVirus Plus, as it could lead to your system getting infected.

### To disable K7AntiVirus Plus:

1. Right-click the  icon in the System Tray.
2. Click the **Disable Product Protection** option.
3. A confirmation message appears.



4. If you are sure you want to disable K7AntiVirus Plus, click **Yes**.
5. If you want to turn off K7AntiVirus Plus for a short period of time enter the time in minutes.
6. Click **No** to leave K7AntiVirus Plus enabled.

**Note:**

If K7AntiVirus Plus is disabled, the K7 icon in the System Tray appears as such .









# Updating Your Product

## Updating Your Product

In order to protect your computer from newly discovered viruses and threats you must keep the K7AntiVirus Plus product installed on your computer up-to-date. Your computer's security depends directly on updating the threat signatures and program modules regularly. 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 **Activated** before you update it.

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

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

You can choose to


- Automatically check for updates
  - Manually check for updates
  - Disable automatic checking for updates
- 

## 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 Plus main console and click the **Tasks** tab. Click **Check for recent updates**.

Alternatively, right-click the  icon in the System Tray and select the **Run Update** option. The Update Manager dialog appears.

2. Click **Click here to change settings** on the bottom of the Update Manager dialog. The Options dialog opens.
3. Select the **Automatically check for updates** check box.
4. You can choose the sequence in which the update is checked:

- **Use Internet Only** - this will download the update directly from the K7Computing web site.
  - **Use Internet, if Internet is not present use K7Local Update Server** - the update files is checked directly from the web site, if the web site is unable to be connected then it checks for the update from the Local update server specified. You can specify the address of this Local update server and the port in the space provided below.
  - **Use the Local update Server only** - this will take the update from the specified local update server. Systems that are not connected directly to the Internet can get the updates from the Local Update server.
  - **Use K7Local Update Server, if not present use the Internet to download the updates** - the local sever is checked for latest updates. If unable to connect to the Local update server then the K7Computing server is checked for updates.
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. If you need to specify the Local Update server then specify the **Local K7Update server address** and the **port number** in the space provided.
  6. Click **OK** to close the Options dialog.
  7. Make sure you are connected to the Internet and click **Click here to update now**. 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.

---

## 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 Plus main console and click the **Tasks** tab. Click **Check for recent updates**.  
Alternatively, right-click the  icon in the System Tray and select the **Run Update** option. The Update Manager dialog appears.
2. Make sure you are connected to the Internet and click **Click here to check for new updates**. 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.
- 

## Disabling Automatic Updates

For maximum protection, it is recommended that you configure K7AntiVirus Plus 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 Plus main console and click the **Tasks** tab. Click **Check for recent updates**.  
Alternatively, right-click the  icon in the System Tray and select the **Run Update** option. The Update Manager dialog appears.
2. Click **Click here to change settings** on the bottom 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** check box to prevent K7AntiVirus Plus 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.

---




# Protecting Against Viruses

## Managing the Virus Protection

K7AntiVirus Plus 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 Plus main console opens.
  2. On the **Security Center** tab, the Status of the protection appears below the **AntiVirus Protection** bar. The product indicates if the Real-Time Scanner, Advanced Behavioral Monitor, Advanced Exploit Protection, Advanced System Monitor and Malicious site filter are enabled (indicated by a green check mark in front of the option).
  3. The date and time of the Virus Definition files that were last downloaded is displayed on the Info Bar on the lower portion of the console. To update the virus definition, click the **Task tab** and then click the **Click here to check for newer updates** option. The Update Manager dialog appears. *See* Manually Updating Your Product for more information
  4. The **Tasks** panel of the console has options to do the following:
    - Run Scan for Rootkits
    - Run Scan for Tracking cookies
    - Run quick scan
    - View System Monitor Events
    - Manage Quarantined Files
  7. To configure the AntiVirus Protection settings, point the mouse on the required option and click the **Configure** button. The **Configure AntiVirus** dialog opens. *See* Configuring the AntiMalware for more information
  8. If you want to scan multiple locations on your computer, click the **Tasks** tab in the in the main console and choose **Scan a specific folder**  
*See* Scanning Multiple Locations for more information
  9. To configure and schedule scan tasks, click the **Tasks** tab and click on **Manage all Tasks** under Schedule a Task to run Automatically  
*See* Configuring Scan Tasks for more information
-

## Configuring the AntiMalware

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

### *To configure the AntiVirus:*

1. Open the K7AntiVirus Plus main console.
  2. To configure the AntiVirus Protection settings, point the mouse on the required option and click the **Configure** button. 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 the System Monitor
    - Configure Script and Instant Messenger Protection
    - Configure the Scan Settings
    - Configure Device Access
    - Configure Carnivore
    - Configure the General Scan Settings
- 

## Configuring the Real-Time Scanner

### 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 AntiMalware protection attempts to clean or remove the infection.

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

1. Open the K7AntiVirus Plus main console.
2. In the **Security Center** tab, click on **Real Time File Scanning** and click **Configure**.
3. Under **What to Scan**, select the types of files you want to scan. The options are described in the following table.

Option	Description
All Files	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> . <i>See</i> Selecting the Types of Files to Scan 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> . <i>See</i> Adding File Extensions for Scan 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. <i>See</i> Defining Types of Threats to Scan for details

7. 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 or Remove the infected files</b>	Clean files that are infected or Remove the Malware file without any interaction from you. An alert is displayed with the details of the detection and the action taken.
<b>Deny access</b>	Restricts access to the infected file

8. 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
9. Once you have configured the Sentry, click **Apply** to save the changes.

## 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:*

1. Open the K7AntiVirus Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, the status of the real-time protection is indicated by a red cross mark if the option is disabled.

When Real Time protection is enabled, the status is indicated by a green check mark.

3. If the real-time protection is currently disabled, the **Enable** option is indicated in blue. Click this option to enable the real-time scan.
  5. A message appears indicating that the protection has been enabled.
- 

### Disabling Real-Time Scan

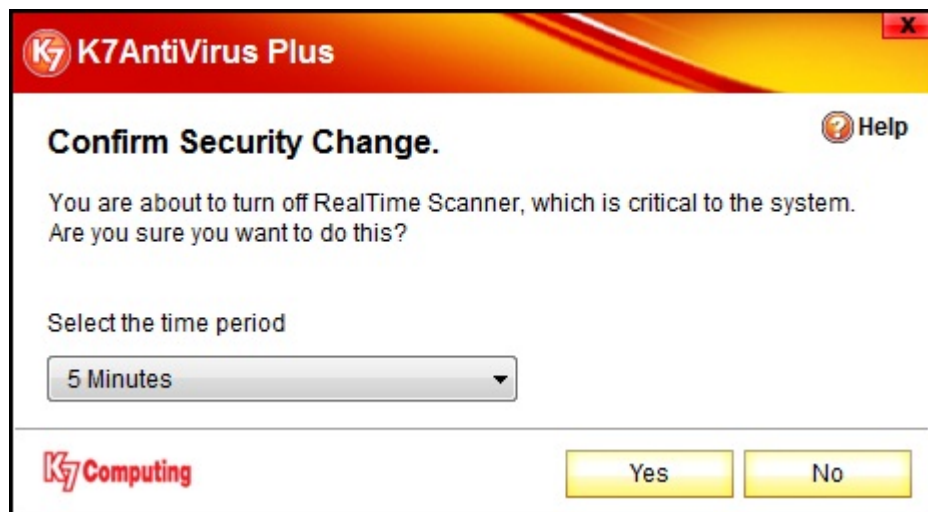
The real-time scan is enabled by default. You can disable the real-time scan.



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 Plus main console.
2. In the **Security Center** tab below the **AntiVirus Protection** bar, the status of the real-time protection is indicated by a red cross mark if the option is disabled. When Real Time protection is enabled, the status is indicated by a green check mark.
3. If the real-time protection is currently enabled, the **Disable** option is indicated in blue. Click this option to disable the real-time scan.
5. A confirmation message appears.



6. If you are sure you want to disable the real-time scan, click **Yes**.

7. If you want to turn off the real-time protection for a short period of time, choose a time option in the drop down box.
8. In order to disable it permanently choose the **Permanently** option in the drop down box.
9. In order to disable only until restart choose the **Until System restarts** option in the drop down box.
10. 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



## 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 Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar click on the **Configure** button next to **RealTime Scanning** and select the **Sentry** tab or the **Email** tab. Alternatively, click on the **Settings** tab in the main console and choose **Real Time Protection**
3. Select the **Detect Spyware and adwares** check box and click the **customize** option. The Types of Threats to Scan dialog opens.
4. 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, Trojans and Internet worms. 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>Clean or Remove the infected file</b>	Clean or remove the infected file from your computer
<b>Deny access</b>	Deny access

7. Click **OK** to save the settings.
- 

## Managing Exclusions

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

### *To manage exclusions:*

1. Open the K7AntiVirus Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar click on the **Configure** button next to **RealTime Scanning**. Alternatively, click on the **Settings** tab in the main console and choose **Real Time Protection**
3. In the **Sentry** tab, click the **Click Here to 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. To delete all the excluded entries you added from the scan result window click on the link **Click here to clear Malware trace exclusion**
  8. Select the following options:
    - **Ignore from RealTime Scanner** - to exclude the selected file or folder from the real-time scan
    - **Ignore from Offline Scanner** - to exclude the selected file or folder from the offline scan
    - **Include Subfolders** - to exclude subfolders under the selected folder from the scan. This option is not available when a file is selected for exclusion.
  8. Click **OK** to save the new entry and return to the Exclude List dialog.
  9. To remove a file or folder from the Exclude list, select the entry in the list and click **Remove**.
  10. Click **OK** to save the exclusion settings.
- 

## Configuring the Email Scanner

### 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 Plus main console.
2. Click **Configure** on **Real Time Email Scanning**
3. Select the **Enable email protection**.
4. 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.

7. 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. <b>See</b> Defining Types of Threats to Scan 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. <b>See</b> Configuring Worm Blocking 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. <b>See</b> Scanning for Malicious Attachments for details

8. 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

9. K7AntiMalware 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
10. Once you have configured the Email Scanner, click **Apply** to save the changes.

## 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 Plus main console.
  2. In the **Security Center** tab, below the **AntiVirus Protection** bar, the status of **Real Time Email Scanning** is indicated by a red cross mark if the option is disabled. When **Real Time Email Scanning** is enabled, the status is indicated by a green check mark.
  3. If **Real Time Email Scanning** is currently disabled, the **Enable** option is indicated in blue. Click this option to enable **Real Time Email Scanning**.
  5. A message appears indicating that the email protection has been enabled.
- 

**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 Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, the status of **Real Time Email Scanning** is indicated by a red cross mark if the option is disabled. When **Real Time Email Scanning** is enabled, the status is indicated by a green check mark.
3. If **Real Time Email Scanning** is currently enabled, the **Disable** option is indicated in blue. Click this option to disable **Real Time Email Scanning**.
5. A confirmation message appears.



6. If you want to turn off the Email Scanner protection for a short period of time, choose a **time** option in the drop down box.
  7. In order to disable it permanently choose the **Permanently** option in the drop down box.
  8. In order to disable only until restart choose the **Until System restarts** option in the drop down box.
  9. If you are sure you want to disable the Email Scanner, click **Yes**.
  10. If you want to disable the Email Scanner for a short period of time, choose a time option in the drop down box
  11. Click **No** to leave the Email Scanner on.
- 


## Configuring Email Server Settings

K7AntiMalware 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 Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, click on the **Configure** button next to **Real Time Email Scanning**. Alternatively, click on the **Settings** tab in the main console and choose **Email Scanning**.
3. Click the **Email Settings** button. The Email Processing Settings dialog opens.
4. Select the required **Options**. The options are:
  - **Send Keep Alive Signals** - 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.

- **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.
6. Click **OK** to save the settings and close the dialog.
- 

### 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 Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, click on the **Configure** button next to **Real Time Email Scanning**. Alternatively, click on the **Settings** tab in the main console and choose **Email Scanning**.
3. Select the **Protect against malicious attachments** 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.

## 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 Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, click on the **Configure** button next to **Real Time Email Scanning**. Alternatively, click on the **Settings** tab in the main console and choose **Email Scanning**.
3. Select the **Enable Worm blocking** check box and click the **Customize** option next to it. The Worm Blocking Settings dialog opens.
4. 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


5. Select the **Show Alert** check box if you want an alert to appear when a worm is identified.
  6. 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.
  7. Click **OK** to save the worm blocking settings.
- 

## Configuring the System Monitor

## Configuring the System Monitor

The System Monitor continuously monitors the critical areas of your computer and warns you of the consequences of any changes made to your system. It helps in the early detection of viruses, and protects your computer from hidden threats before they run.

### *To configure the System Monitor:*

1. Double-click the  icon in the System Tray. The K7AntiVirus Plus main console opens.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar click on the **Configure** button next to **Advanced System Monitor**. Alternatively, click on the **Settings** tab in the main console and choose **System Monitor**
3. Select the **Level of Protection** you want the System Monitor to use when checking for spyware. The levels are detailed in the following table.

Level of Protection	Description
<b>High</b>	Monitors all check points for spyware
<b>Medium</b>	Monitors most check points except non-critical points
<b>Low</b>	Monitors only the most critical check points
<b>User Defined</b>	Allows you to select the check points you want the System Monitor to check based on your requirement <a href="#">See</a> Configuring the System Check Points for details

6. To set additional **Options**, select the required check boxes. The options are described in the following table.

Option	Description
<b>Automatically allow all files that are digitally signed</b>	Allows all files that are digitally signed
<b>Automatically allow all files that System Monitor recognises</b>	Allows all files that the System Monitor recognises
<b>Always prompt if changes are found when a new software is installed</b>	Prompts if the changes detected indicate that a new software is being installed. Clear the check box if you want the product to ignore such changes.

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

## Enabling the System Monitor

The System Monitor is enabled by default. If you disable it for any reason, you can enable it again.

**Note:** It is recommended that you enable the System Monitor so that the critical areas of your computer are monitored continuously.

### *To enable the System Monitor:*

1. Open the K7AntiVirus Plus main console.
  2. In the **Security Center** tab, below the **AntiVirus Protection** bar, the status of System Monitor protection is indicated by a red cross mark if the option is disabled. When System Monitor is enabled, the status is indicated by a green check mark.
  3. If the System Monitor is currently disabled, the **Enable** option is indicated in blue. Click this option to enable the System Monitor.
  5. The System Monitor is enabled and a message appears.
  6. Click **Yes**.
- 

## Disabling the System Monitor

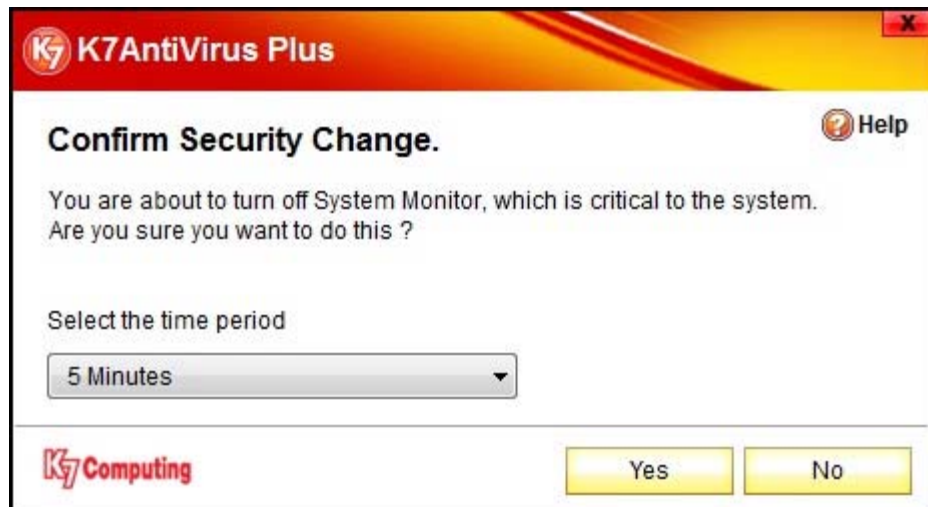
The System Monitor is enabled by default. You can disable the System Monitor.



It is recommended that you *do not* disable the System Monitor, as your computer could be affected by hidden threats.

### *To disable the System Monitor:*

1. Open the K7AntiVirus Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, the status of System Monitor protection is indicated by a red cross mark if the option is disabled. When System Monitor is enabled, the status is indicated by a green check mark.
3. If the System Monitor is currently enabled, the **Disable** option is indicated in blue. Click this option to disable the System Monitor.
5. A confirmation message appears.



6. In order to disable it permanently choose the **Permanently** option in the drop down box.
  7. In order to disable only until restart choose the **Until System restarts** option in the drop down box.
  8. If you are sure you want to disable the System Monitor, click **Yes**.
  9. If you want to turn off the real-time protection for a short period of time, choose a time option in the drop down box
  10. Click **No** to leave the System Monitor enabled.
- 

### Configuring the System Check Points

*To configure the system check points that System Monitor should monitor:*

1. Open the K7AntiVirus Plus main console.
2. In the **Security Center** tab, below the **AntiVirus Protection** bar, click on the **Configure** button next to **Advanced System Monitor**. Alternatively, click on the **Settings** tab in the main console and choose **System Monitor**
3. Under **Select Level of Protection**, select the **User Defined** option and click the **customize** option that appears below it. The System Monitor Check Points dialog opens.
4. By default all the options are selected. Select or clear the required system check points.  
*See* System Monitor Check Points for details
5. The System Monitor will monitor only the selected check points for any changes.
6. Click **OK** to save the settings.

## Viewing System Monitor Events

The System Monitor helps protect your computer, privacy and personal information from hidden threats before they run, stopping most spyware threats before they install.

When the System Monitor is enabled, it continuously monitors your computer and warns you when any changes have taken place or when any suspicious program is trying to enter your computer. When the warning appears, you can either allow the changes to take place or block the changes. The changes that have been allowed or blocked are tracked. You can view and undo the action taken when the warning appeared.

### *To view and undo the changes:*


1. Open the K7AntiVirus Plus main console.
  2. Select the **Tasks** tab.
  3. Choose **Manage System Monitor Events** option under Administrative Task. The System Monitor - Blocked Entries dialog appears.
  4. The list of **Blocked Events** is displayed.
  5. Select an event from the list and its **Details** appears on the dialog.
  6. To view more information on the event, click the **More about this entry** option.
  7. If you want to undo the change made by the program, select the event in the list and click the **UnBlock** option.
  8. Click **Close** to close the dialog.
- 


## Managing Quarantined Files

### 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. Double-click the  icon in the System Tray. The K7AntiVirus Plus main console opens.
2. Click on the **Tasks** tab.

3. Click the **Manage Quarantined Files** option under **Administrative Task** section. The **Quarantine Manager** console opens.
  4. 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.
  5. 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
  6. For more information on a file that is quarantined and its current status, select it in the list and click **Properties**.
  7. Click the  to close the Quarantine Manager console.
- 


### 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. Open the K7AntiVirus Plus main console.
2. Click on the **Tasks** tab.
3. Click the **Manage Quarantined Files** option under **Administrative Task** section. The **Quarantine Manager** console opens.
4. Click **Add**. The Add Files to Quarantine dialog opens.
5. Browse to select the file you want to add to the Quarantine folder and click **Open**.

**Note:** To remove the file from this location select the **Remove the file from this location** check box in the Add Files to Quarantine dialog.

6. The file is added to the Quarantine folder and listed in the dialog.
  7. You can take action on the file at a later point in time.
  8. Click the  button to close the Quarantine Manager console.
- 

### 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


## Printed Documentation

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 Plus main console.
  2. Click on the **Tasks** tab.
  3. Click the **Manage Quarantined Files** option under **Administrative Task** section. The **Quarantine Manager** console opens.
  4. Select the file you want to restore and click **Restore**.
  5. A warning message appears informing you that a quarantined file is being restored.
  6. Click **Yes** if you want to restore the file. The file is returned to its original location.
  7. Click the  button to close the Quarantine Manager console.
- 

## 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 Plus main console.
  2. Click on the **Tasks** tab.
  3. Click the **Manage Quarantined Files** option under **Administrative Task** section. The **Quarantine Manager** console opens.
  4. Select the file in the quarantined list and click **Delete**.
  5. A message confirming the deletion appears.
  6. Click **OK** to permanently delete the file.
  7. Click the  button to close the Quarantine Manager console.
- 

## Configuring Additional Scan Options

### 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. Double-click the  icon in the System Tray. The K7AntiVirus Plus main console opens.
  2. Click on the **Settings** tab in the main console and choose **Messenger and Office Plug-ins** option.
  3. You can configure the scanning of
    - Scripts, *see* Configuring Script Scanning
    - Instant Messenger programs, *see* Configure Messenger Scanning
    - Office files, *see* Configuring Office Plugin Scanning
  6. Click **Apply** to save the settings.
  7. Click **Close** to close the Configure AntiMalware dialog.
- 

**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 Plus main console.
2. Click on the **Settings** tab in the main console and choose **Messenger and Office Plug-ins** option.
3. Select the messenger program you want to include in the protection. Currently, Windows/MSN, AOL and Yahoo messengers are supported.
4. 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.
- 

### 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 Plus main console.
2. Click on the **Settings** tab in the main console and choose **Messenger and Office Plug-ins** option.
3. 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

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

### Configuring Office Plugin Scanning

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

#### *To configure Office Plugin scanning:*


1. Open the K7AntiVirus Plus main console.
  2. Click on the **Settings** tab in the main console and choose **Messenger and Office Plug-ins** option.
  3. To scan all Word and Excel files opened by MSOffice, select the **Enable Office Plugin** check box.
  4. Click **Apply** to save the settings.
- 

### Configuring the Scan Settings

## 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:

1. Double-click the  icon in the System Tray. The K7AntiVirus Plus main console opens.
2. Click on the **Settings** tab in the main console and choose **On Demand Scanner** option.
3. 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 executable (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. <i>See</i> Selecting the Types of Files to Scan 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. <i>See</i> Selecting the Types of File Extensions to Scan 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. <i>See</i> Configuring the Types of Threats to Scan for details

5. 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.

Option	Description
<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 partition table of the hard disk
<b>Scan for critical system settings</b>	There are a few system settings that are critical for normal functionality of the system. This option scans for such registry modification done by the virus.

<b>Scan suspicious AutoRun.inf files</b>	Scans for suspicious entries in Autorun.inf files on all user drives..
<b>Scan tracking cookies</b>	Scans for the presence of tracking cookies for currently logged-in user.
<b>Scan unwanted Registry entries</b>	Scans the windows registry for registry entries left behind by malicious or unwanted programs.
<b>Scan unwanted files</b>	Scans for the residual files left behind by malicious or unwanted programs.

6. 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 or Remove the infected files</b>	Clean files that are infected or Remove the Malware file without any interaction from you. An alert is displayed with the details of the detection and the action taken.
<b>Report only</b>	Reports the infection in the file but does not take any action

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

### Selecting the Types of Files to Scan

K7AntiVirus Plus 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 Plus main console.
2. Click on the **Settings** tab in the main console and choose **On Demand Scanner** option.
3. 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.
4. Select the required options. The options are described in the table below.

<b>Option</b>	<b>Description</b>
<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.
- 

## Adding File Extensions for the Scan

K7AntiVirus Plus 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 Plus main console.
  2. Click on the **Settings** tab in the main console and choose **On Demand Scanner** option.
  3. 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.
  4. The list of file extensions configured is displayed.
  5. 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.
  6. To select *only* the default file extensions and discard all added extensions, click the **Default** button.
  7. If you want to remove a file extension, select it in the list and click **Delete**.
  8. Click **OK** to save the settings.
- 

## Managing Scanner Tasks


### 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 Plus main console opens.
  2. Click on the **Tasks** tab
  3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
  4. 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
- 

### 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 from the **Status Window** 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 Plus main console.
2. Click the **Tasks** tab.
3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
4. Select the **QuickScan** task and click **Change**.
5. In the **Scan Settings** tab, **Only Action to take on virus found** option can be configured others are fixed. *See* Configuring Scan Settings for details

Option	Description
<b>Clean or Remove the infected files</b>	Clean files that are infected or Remove the Malware file without any interaction from you. An alert is displayed with the details of the detection and the action taken.
<b>Report only.Do not take any action</b>	Reports the infection in the file but does not take any action

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.
- 

## 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 Plus main console. Click the **Tasks** tab.
2. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined 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 partition table, boot sector, 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> .

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

## 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 Plus main console.
2. Click on the **Tasks** tab
3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
4. Select the scan task and click the **Change** button. The Configure Scan Tasks dialog opens.
5. Select the **How to Scan** tab.
6. 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

7. 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

8. 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

9. 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

10. Click **Apply** to save the scan options.

## 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. Open the K7AntiVirus Plus main console.
2. Click on the **Tasks** tab
3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
4. Select the scan task and click the **Change** button. The Configure Scan Tasks dialog opens.
5. Click the **Schedule** tab.
6. Select the **Enable Scheduling of this task** check box to ensure the task runs.

7. 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.
  8. Use the **Start Time** controls to set the time of the day when you want the task to run.
  9. 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:
    10. **Daily** - specify the number of days between scans in the **Schedule Task Daily** panel
    11. **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
    12. **Monthly** - specify the day of the month on which you want the scan to run in the **Schedule Task Monthly** panel
  6. Click the **Apply** button to save the schedule.
  7. Click **Close** to close the Configure Scan Tasks dialog.
  - 8.
- 

### 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 Plus main console.
2. Click on the **Tasks** tab
3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
4. Select the scan task and click the **Change** button. The Configure Scan Tasks dialog opens.
5. To customize how the scan must run, select the required options in the **How to Scan** tab.  
*See* Customising a Scan Task for details
6. To set the schedule for the scan task, select the required options in the **Schedule** tab.  
*See* Scheduling Scan Tasks for details

7. Click **Apply** to save the changes.
  8. Click **Close** to close the Configure Scan Tasks dialog.
- 

## 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 Plus main console.
  2. Click on the **Tasks** tab
  3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined scheduled tasks are displayed.
  4. Select a scan task in the list and click **Run Now**. The scan task is executed and the results displayed.
- 

## 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 Plus main console.
  2. Click on the **Tasks** tab
  3. Under **Schedule a Task to run Automatically**, choose **Manage all Tasks**. The pre-defined custom and scheduled tasks are displayed.
  4. Select the custom scan task you want to delete and click the **Delete** button.
  5. The selected scan task is deleted after a confirmation.
  6. If you try to delete a pre-defined scan task, you are warned.
- 

## Scanning Your Computer


### Running QuickScan

## Printed Documentation

The Quick Scan 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.

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

1. Open the K7AntiVirus Plus main console.
2. Click on the **Tasks** tab.
3. Choose **Do a Quick Scan** option under **Scan my computer for viruses and spyware**.

**Note:** To quickly Run the quick scan, Right-click the  icon in the System Tray and select the **Status Window** option. Click **Run Quick Scan**

4. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
  5. The folders that are configured are scanned and the result of the scan is displayed in the K7AntiVirus Scanner dialog.
- 

## Running Rootkits Scanner

The deep scan for rootkits can be used to scan the system generically for rootkits..

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

1. Open the K7AntiVirus Plus main console.
  2. Click on the **Tasks** tab.
  3. Choose **Scan for Hidden Rootkits** option under **Scan my computer for viruses and spyware**.
  4. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
  5. The Rootkit scanner scans for hidden registry entries, hidden processes and hidden file system entries. The results of the scan are displayed in the K7Antivirus scanner dialog.
- 

## Running Tracking Cookies Scanner


Tracking cookies are bits of information stored on a computer by a browser which enable a website to uniquely identify a user. The scan for Tracking cookies scans for tracking cookies present for the currently logged-in user.

### *To run a tracking cookies scan of your entire computer:*

1. Open the K7AntiVirus Plus main console.
  2. Click on the **Tasks** tab.
  3. Click on **Scan my system for tracking cookies** option under **System Health Scan**
  4. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
  5. Once the scan for tracking cookies has completed the results of the scan are displayed in the k7AntiVirus scanner dialog.
- 

### Scanning Your Entire Computer

*To manually scan your entire computer:*

1. Double-click the  icon in the System Tray. The K7AntiVirus Plus main console opens.
  2. Click on the **Tasks** tab.
  3. Click on **Do a complete scan** under the section **Scan my computer for viruses and spyware**.
  4. The K7AntiVirus Scanner dialog opens and displays the progress of the scan.
  5. 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
  6. If there are viruses in any of the drives or folders, the details appear in the dialog.
  7. To exclude a file that has been detected as infected from being treated and from future scans, select it in the list and click **Exclude**.
  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 the selected folder(s), a message appears.
  12. Click the **Save Result** button to save the K7AntiVirus Scanner Result.
  13. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.
  14. Click the **Exit** button to close the K7AntiVirus Scanner dialog.
-

## 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 Select **Scan with K7AntiVirus**.
  3. Alternatively, click on the **Tasks** tab in the K7AntiVirus Plus main console and choose **Scan a specific folder**. *See* **Scanning Multiple Folders**
  4. 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.
  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 folder(s), 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**.
- 

## 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 Select **Scan with K7AntiVirus**.
3. Alternatively, click on the **Tasks** tab in the K7AntiVirus Plus main console and choose **Scan specific files**.
4. 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.
5. To clean the infected file, select it in the list and click **Clean**.
6. If you want to delete the file containing the virus, select the 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 file, 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**.
- 

### 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 Plus main console.
  2. click on the **Tasks** tab in the K7AntiVirus Plus main console and choose **Scan a specific folder**.
  3. 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.
  4. Select the check box(es) corresponding to the folders you want to scan and click **Start Scan**. The K7AntiMalware Scanner dialog opens and displays the progress of the scan.
  5. The selected folder(s) are scanned and the results of the scan are displayed in the K7AntiMalware Scanner dialog. If there are viruses in the selected folders, the details appear in the dialog.
  6. To clean an infected file, select it in the list and click **Clean**.
  7. If you want to delete the file containing the virus, select the infected file and click **Delete**.
  8. To quarantine an infected file, select it in the list and click **Quarantine**.
  9. If there is no virus in the selected folder(s), a message appears.
  10. Click the **Stop** option on the top of the dialog to stop the scan. Once the scan is complete, the option toggles to **Exit**.
  11. To configure the settings for the scan, click the **Settings** button. The Configure AntiMalware dialog appears.
  12. Select the options for the scan and click **Close**. *See* Configuring Scan Settings for details
  13. If you want to reset the scan settings, click the **Reset** button.
  14. Click the **Exit** button to close the K7AntiMalware Scanner dialog.
-

## Configuring the General Scan Settings

K7AntiVirus allows you to configure some general scan settings.

*To configure the general scan settings:*

1. Open the K7AntiVirus Plus main console.
2. Click on the **Settings** tab in the main console and choose **General Options**.
3. 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>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>Take Automatic action on infected archives</b>	<p><b>Delete the archives:</b> If the Archive contains one or more infected file(s), the archive is Deleted</p> <p><b>Quarantine the archives:</b> If the Archive contains one or more infected file(s), the archive is Quarantine</p>
<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.

## Configuring the Log Options

K7AntiMalware allows you to record the various activities of the product.

*To configure the log options:*

1. Open the K7AntiVirus Plus main console.
2. Click on the **Settings** tab in the main console and choose **General Options**.

3. To set the **Log Options**, select the **Enable Logging** check box.
4. Select the log options. 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 'r;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

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

## 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 Plus main console.
  2. Click on the **Support** tab.
  3. Click the **View Virus Information on the Web** under **Support Links** section. 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.
  4. Use the links on the web page to access the virus information you want to view.
  5. When you finish viewing the virus information close your browser window.
-



















# MISC

## Activation Reminder

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



To activate your product from the alert, click the link **Click here to activate now**. The Activation screen appears.

**See** Activation Your Product for more information

To activate the product later, click the link **Click here to remind after some time**.

If you do not want the alert to appear again, Click the link **Click here to remind after 12 hours**.

---

## Privacy Service ActiveX Alert

Privacy Settings helps prevent other web sites from learning the about your browsing habits, the web sites last visited and other browser specific information. These information are collected using Cookies, Active-X controls and Java applets. You can specify how privacy should behave when these are encountered. You can configure the actions by using the Browser Settings options for the user.

**See** Creating User Profiles for more information

The ActiveX alert appears If you have configured the browser to prompt for action when ActiveX controls are encountered. You can select one of the following options:

Option	Description
--------	-------------

<b>Allow</b>	Allows the ActiveX control to be loaded on your computer
<b>Block</b>	Blocks the ActiveX control from being loaded on your computer
<b>Always apply this action to this website</b>	Applies the selected action (allow or block) whenever an ActiveX control is encountered from this web site

Click the  button to close the alert.

---

## Adding an Exclude Entry

*To add a file or folder to the Exclude list:*

1. Enter the path of the folder or file.
  2. If you are not sure of the path, click **Add Folder** or **Add File** to select the folders or files respectively.
  3. Select the following options:
    - **Ignore from RealTime Scanner** - to exclude the selected file or folder from the real-time scan
    - **Ignore from Offline Scanner** - to exclude the selected file or folder from the offline scan
    - **Include Subfolders** - to exclude subfolders under the selected folder from the scan. This option is not available when a file is selected for exclusion.
  4. Click **OK** to save the new entry.
- 

## AppInit DLL Value

**What is a AppInit\_Dlls Value?**

The AppInit\_Dlls value is found in the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows
```

All the DLLs that are specified in this value are loaded by each Microsoft Windows-based application that is running in the current log on session. All the programs that link to the User32.dll will load the App\_Init DLLs also.

**Advice:**

Whenever you receive a AppInit\_Dll value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Boot Execute Value

**What is Boot Execute Value?**

Any file added in this entry will get loaded every time the system starts.

**Advice:**

Whenever you receive a Boot Execute Value alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Browser Settings

To specify the options for the user when he accesses web sites, click the **Browser Settings** tab and select the required options. The browser properties are described in the following table.

Property	Option	Description
Action on Cookies	Allow all cookies	Allows cookies
	Block all cookies	Blocks cookies
	Prompt for action	Prompts for action each time a cookie is encountered
Action on Active-X Controls	Allow all ActiveX	Allows Active-X controls
	Block all ActiveX	Blocks Active-X controls
	Prompt for action	Prompts for action each time an ActiveX control is encountered
Action on Java applets	Allow all JavaApplets	Allows Java applets

	<b>Block all JavaApplets</b>	Blocks Java applets
	<b>Prompt for action</b>	Prompts for action each time a Java applet is encountered
<b>Ad Blocking</b>	<b>Block Advertisements</b>	Select the check box if you want to block advertisements from appearing when you access web sites

---

## Context Menu Handler

### What is a context menu handler?

A context menu handler is a shell extension handler that allows an application to add its commands to the existing context (right-click) menu of specific file class. By implementing and registering a handler, an application can add items to an object's context menu.

The context menu handler registry values monitored by K7SystemMonitor are:

```
HKCR\*\shellex\ContextMenuHandlers
HKCR\Folder\shellex\ContextMenuHandlers
HKCR\Directory\shellex\ContextMenuHandlers
```

### Advice:

Whenever you receive a context menu handler registry value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Control Panel Listings

### What is a Control Panel Listings?

It is possible to disable controls in Control Panel by adding an entry to the C:\windows\control.ini file. In control.ini, you can specify which control panels can be viewed. If inetcpl.cpl=no, your settings may have been changed by a software or by your system administrator.

### Advice:

Whenever you receive a Control Panel listings alert from K7SystemMonitor, click on the **Details**

button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## 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. Select the **How to Scan** tab.
2. 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

3. 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

4. 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

- 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

- Click **Apply** to save the scan options.

## Configuring Rules

You can define rules for exceptions.

### *To define rules:*

- To add a rule, click the **Add** option. The Rule Definition dialog opens.
- Enter a **Short Description** for the rule.
- Select a **Rule Tag** and configure its properties in the lower panel. The options appearing in the lower panel depend on the tag selected.
- The following table describes the options available for each Rule tag.

Rule Tag	What to configure	Option	Description
<b>When Direction is</b>	Direction	<b>Incoming</b>	Rule applies to incoming connections from other computers to your computer

		<b>Outgoing</b>	Rule applies to outgoing connections to other computers from your computer
		<b>Both</b>	Rule applies to both incoming and outgoing connections
<b>When Protocol is</b>	Protocol	<b>Any Protocol</b>	Rule applies to any communication
		<b>TCP</b>	Rule applies to TCP (Transmission Control Protocol) communication
		<b>UDP</b>	Rule applies to UDP (User Datagram Protocol) communication
		<b>TCP or UDP</b>	Rule applies to both TCP and UDP communications
		<b>Specific Protocol</b>	Rule applies to the protocol you specify here
<b>When Local Port is</b>	Source Port	<b>Any port Address</b>	Rule applies to communication using any port originating from the local computer
		<b>Specific port Address</b>	Rule applies to communication originating from the local computer using the port you specify here
		<b>Port Address Range</b>	Rule applies to communication originating from the local computer using the range of ports you specify here
<b>When Remote Port is</b>	Remote Port	<b>Any port Address</b>	Rule applies to communication using any port originating from another computer
		<b>Specific port Address</b>	Rule applies to communication originating from another computer using the port you specify here
		<b>Port Address Range</b>	Rule applies to communication originating from another computer using the range of ports you specify here
<b>When Local IP is</b>	Source IP Address	<b>Any IP Address</b>	Rule applies to communication originating from any local IP address
		<b>Specific IP Address</b>	Rule applies to communication originating from the local IP address you specify here
		<b>IP Address Range</b>	Rule applies to communication originating from the local IP, which falls under the specified IP range
		<b>Network Address</b>	Rule applies to communication originating from the local IP, which falls under the specified network
<b>When Remote IP is</b>	Remote IP Address	<b>Any IP Address</b>	Rule applies to communication to any IP address

<b>IP is</b>	Address	<b>Specific IP Address</b>	Rule applies to communication to the remote IP address you specify here
		<b>IP Address Range</b>	Rule applies to communication to the remote IP, which falls under the specified IP range
		<b>Network Address</b>	Rule applies to communication to the remote IP, which falls under the specified network
<b>Action</b>	Action to take on the rule	<b>Allow the Packet</b>	Allows the communication that matches with the configured rule
		<b>Block the Packet</b>	Blocks the communication that matches with the configured rule
		<b>Show an alert</b>	Displays an alert when a communication matches this rule
		<b>Create Log Entry</b>	Creates an entry in the log when a communication matches this rule



6. When you select an option to configure the rule, click the **update** option to save the changes to the rule.
7. Click **Ok** to close the Rule Definition dialog.

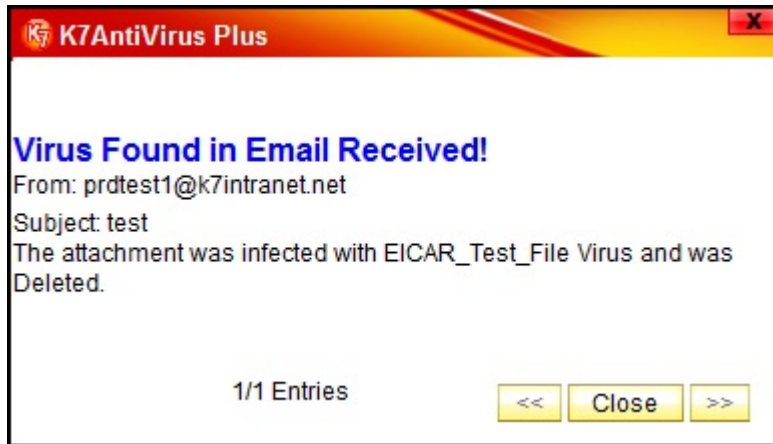
## Email Virus Alerts

K7AntiVirus can be configured to check 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.

**See** [Configuring the Email Scanner](#) for more information

If you enable email protection, you can select to clean the files automatically.

- When you configure the Email Scanner to clean the files automatically and to quarantine or delete the attachment if it cannot be cleaned and you select the **Show Alerts** option, the system displays such an alert. Use the  and  options to view the other alerts. Click **Close** to close the alert.



---

## Host File

### What is Host file?

Windows uses the host file for translating Domain names into IP addresses for web sites. This is also known as Host file Redirection. For instance, the entry

```
202.54.63.218 www.k7computing.com
```

in the Host file will redirect the browser to the specified IP address when connecting to www.k7computing.com

Threats like spyware and adware may use this facility to either:

- Redirect genuine domain names to unwanted IP addresses
- Restrict access to certain web sites
- Generally, any genuine application software does not modify the Host file.

### Advice:

Whenever you receive a Host file change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Browser Helper

### What is an IE Browser Helper Object?

A browser helper object (BHO) is an application that acts as a plug-in to Internet Explorer and helps developers to provide useful functionality. BHOs can be used to:

## Printed Documentation

- Monitor Internet browsing and suggest related links during search operations
- Track and control downloads

As a result, legitimate search sites often use this technique.

However, spyware also use BHOs to watch the user's activities over the internet and to display banners or advertisements. These unwanted BHOs are often installed on the victim machine without the user's consent or knowledge. K7SystemMonitor watches for the installation of BHOs on the system and warns the user whenever such an action occurs.

### Advice:

Whenever you receive a IE Browser Helper Object alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Extensions

### What is Internet Explorer Extensions?

The Internet Explorer extensions control icons on the main Internet Explorer toolbar or items in the Internet Explorer Tools menu that are not part of the default installation. Any program that gets attached as an extension will get loaded whenever Internet Explorer loads.

### Advice:

Whenever you receive an IE Extensions value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Search Hooks

### What are IE Search Hooks?

An Internet Explorer search hook is used by the browser to translate the address of an unknown URL protocol. This is used when the user types a URL (like [www.k7computing.com](http://www.k7computing.com)) in the address bar of the browser without specifying the protocol (like `http://` or `https://`). In such cases, Internet Explorer will try to find out the proper protocol by itself based on the address entered. If this is not possible, it will then use the IE search hook to find the address entered.

### Advice:

Whenever you receive an IE Search Hooks value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Security Settings

### What are IE Security Settings?

Internet Explorer security settings can be used to safeguard user data from malicious web sites. Viruses and other malware may try to change these browser security settings to a lower level in order to perform operations like:

- Switch between secure and non-secure browsing modes
- Visit web sites with an invalid site certificate
- Transmit data over an open or unsecured connection
- Redirect data submitted by user in a web-based form to a site other than the one currently being viewed

These kinds of changes are not generally made by any genuine application and hence indicates a virus infection. K7SystemMonitor watches for changes made to these settings to help protect the system.

#### Advice:

Whenever you receive a IE security settings change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Toolbars

### What is Internet Explorer Toolbars?

The Internet Explorer tool bars are the toolbars that are below the navigation bar and menu in the Internet Explorer browser. Any program that gets attached as a toolbar will get loaded whenever Internet Explorer loads.

#### Advice:

Whenever you receive an IE Toolbar value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been

made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Trusted Site

### What is IE Trusted Site List?

Internet Explorer classifies all web content into four different zones. It is possible to assign different security setting to each of these zones, thereby restricting the actions the sites under each zone will be allowed to perform.

The Trusted Site list in one of these four zones and contains all the sites that are trusted by the user not to cause any damage to or loss of user data. This zone has a low security setting by default and hence the sites under this zone will be allowed by the browser to run potentially harmful scripts and download files onto the user's system without prompting.

The sites under this zone can be viewed and edited by the user by opening Internet Explorer and navigating to **Tools->Internet Options->Security Tab** and selecting **Trusted sites** and then clicking on the **Sites** button.

Owing to the various actions that can be performed when a site is added to this zone, spyware often add sites to this zone. This enables them to download and install their updates and also other malware on the victim machine as well as run various dangerous scripts.

### Advice:

Whenever you receive an IE Trusted Site List change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE URL Settings

### What are IE URL Settings?

When your Web browser is redirected, attempts to view some Web sites, such as common search engines or popular Web directory sites, are automatically redirected to a alternative Web site without your knowledge or consent. A browser re-director can also disallow access to certain Web pages, for example an AntiMalware site. These programs can also disable AntiMalware and anti-spyware software.

The Internet Explorer URLs Agent monitors changes to Internet Explorer URLs to help prevent browser redirecting.

**Advice:**

Whenever you receive a IE URL settings change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## IE Zone Settings

**What are IE zone settings?**

Internet Explorer allows the classification of various types of web content into four major zones, namely:

- **Local Intranet zone** - comprises all the web content within a company's intranet or local network
- **Trusted zone** - comprises all the web content that can be trusted not to damage and/or abuse user data
- **Restricted zone** - comprises all the web content that are likely to cause damage to the system or user data
- **Internet zone** - comprises all the web content that have not been classified under any of the above 3 zones

Each of these zones can be assigned High, Medium, Medium-low or Low settings, which will restrict the operations allowed to them. The settings can be assigned in the **Security** tab of **Internet Options**.

K7SystemMonitor monitors these zone settings in order to ensure no unauthorized changes are made which might breach the system's security.

**Advice:**

Whenever you receive a IE zone settings change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Privacy Service Java Applet Alert

Privacy Settings helps prevent other web sites from learning the about your browsing habits, the web sites last visited and other browser specific information. These information are collected using Cookies, Active-X controls and Java applets. You can specify how privacy should behave

## Printed Documentation

when these are encountered. You can configure the actions by using the Browser Settings options for the user.

**See** [Creating User Profiles](#) for more information

The Privacy Service Java Applet alert appears if you have configured the browser to prompt for action when Java Applets are encountered. Select one of the following options:

Option	Description
<b>Allow</b>	Allows the Java applet to be loaded on your computer
<b>Block</b>	Blocks the Java applet from being loaded on your computer
<b>Always apply this action to this website</b>	Applies the selected action (allow or block) whenever a Java applet is encountered from this web site

Click the  button to close the alert.

---

## NT Load and Run Values

### What is NT Load and Run Values?

Any file added in this entry will get loaded every time the system starts.

#### Advice:

Whenever you receive a NT Load and Run Values alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Configuring the Scan Settings

*To configure the scan settings:*

1. 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 executable (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 three types you want to scan. <b>See</b> Selecting the Types of Files to Scan for details
<b>Specific Extensions</b>	Scans files with the specific file extension. 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 be scanned here. <b>See</b> Selecting the Types of File Extensions to Scan 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. Click on the <b>customize</b> option that appears next to it to select the type of threats to scan for and the action to take when a threat is found. <b>See</b> Configuring the Types of Threats to Scan for details

2. 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.

Option	Description
<b>Memory</b>	Checks the memory of your computer for the presence of virus
<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 partition table of the hard disk
<b>Scan for critical system settings</b>	There are a few system settings that are critical for normal functionality of the system. This option scans for such registry modification done by the virus.
<b>Scan suspicious AutoRun.inf</b>	Its scans for Autorun.inf file in all the drives.
<b>Scan tracking cookies</b>	Scans for tracking cookies for the current user.
<b>Scan unwanted Registry entries</b>	Scans the registry for unwanted registry traces left out by the malware after the malware is removed.
<b>Scan unwanted files</b>	Scans for the unwanted files that left out by the malware after the malware is removed.

3. Select the **Action** to be taken if a virus is found. The actions are described in the following table.

Action	Description
<b>Clean or Remove the infected files</b>	Clean files that are infected or Remove the Malware file without any interaction from you. An alert is displayed with the details of the detection and the action taken.

**Report only**

Reports the infection in the file but does not take any action

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

## ScreenSaver Value

### What is ScrenSaver value?

Windows has a default screen saver which is shown over the login screen even when no screen saver has been selected. These settings allow you to configure the default login screen saver.

On Windows NT based machines, this can be done by changing the value of `Scrnsave.exe` under the key `HKEY_CURRENT_USER\ControlPanel\Desktop` to the required filename.

Certain viruses use this technique to run themselves at an early stage of Windows startup, even before the user logs on to the machine.

### Advice:

Whenever you receive a Screensaver value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. This change generally happens when you have changed /installed a new Screen Saver. You can allow this change if you have done this or recognize the program or publisher.

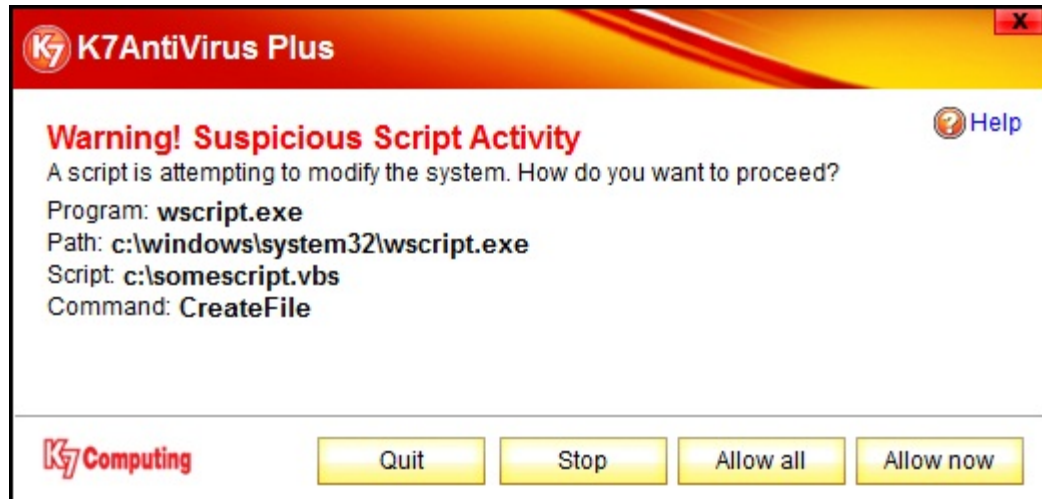
---

## Script Alerts

K7AntiVirus can be configured to automatically block harmful scripts from running on your computer. Scripts can create, copy or delete files. They can also open your Windows registry. **See** [Configuring Script Scanning](#) for more information



If you enable script protection, you can select to be prompted when a malicious script is executed or select to deny access to the script and be notified of such a script.

- When you select to be prompted for action when a script is executed the systems displays an alert. You can select one of the following options:



Option	Description
Quit	Close the prompt.
Stop	Stops the execution of the script. Select this if you suspect the script to be malicious.
Allow all	Allows the execution of all such scripts always. Select this option if it is a harmless script.
Allow onetime	Allows the execution of the script only this time. Select this option if you want the script to be executed only this time.

Click the  button to close the alert.

- When you select to deny access to the script and be notified when the script is executed the systems displays an alert. Use the  and  options to view the other script prompts. Click **Close** to close the alert.

## Shared Task Scheduler

### What is Shared Task Scheduler?

Windows executes instructions in the Windows Task Scheduler. The files listed in Shared Task Scheduler will be run automatically when you start Windows

#### Advice:

Whenever you receive a Shared Task Scheduler alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

## Shell Execute Hooks

### What are Shell Execute Hooks?

Shell execute hooks are programs that load themselves directly into `Explorer.exe` - the shell of the Windows operating system. Once a program does this, the shell execute hook program will receive all the execute commands that are run on a computer.

This type of program can control the operating system's acceptance or rejection of a command to start specific programs. In other words, every action the user performs through the shell of the Windows operating system is caught up by a shell execute hook program.

Viruses and other malware may try to use this technique to hide their active presence on the victim machine or prevent other security related processes from starting. These programs are notified of the programs the user launches and they can perform any additional task before the program is actually run.

K7SystemMonitor watches for the addition of such programs and alerts the users accordingly.

### Advice:

Whenever you receive a Shell Execute Hooks alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Shell Object Delay Load

### What is Shell Object Delay Load?

`Explorer.exe` is the shell of the Windows operating system. Hence it will automatically load the files listed under the `ShellServiceObjectDelayLoad` when Windows starts. These files are loaded early in the system boot process even before there is any user interaction. This technique may be used by viruses and other malware to load themselves whenever Windows starts.

The files listed under the `ShellServiceObjectDelayLoad` are treated similar to those listed under the `Run` key in the Windows registry. However, the main difference between the two is that, the values under the `Run` key point to the actual file itself whereas the values listed under `ShellServiceObjectDelayLoad` points to the `CLSID InProcServer` that has the information about the particular `.dll` file that is being used.

K7SystemMonitor watches for any values added under:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKCU\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
```

**Advice:**

Whenever you receive a Shell Object Delay Load value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Shell Open Command

### What is a shell open command?

Windows uses the shell open command registry values to associate file extensions with specific applications. For instance, the default value "%1" %\* under the registry key `HKKEY_CLASSES_ROOT\exefile\shell\open\command` instructs the operating system how to execute a file with a .exe extension. If this value is changed to "Virus.exe %1\" %\*", then Windows will execute the file `Virus.exe` whenever any EXE file is run.

This technique may be used by viruses to:

- Execute themselves on the user machine
- Restrict access to system tools like registry editor

These kinds of changes are not generally made by any genuine application and may hence indicate a virus infection. Some of the critical shell open command registry values monitored by K7SystemMonitor are:


- `exefile\shell\open\command`
- `scrfile\shell\open\command`
- `comfile\shell\open\command`
- `piffile\shell\open\command`

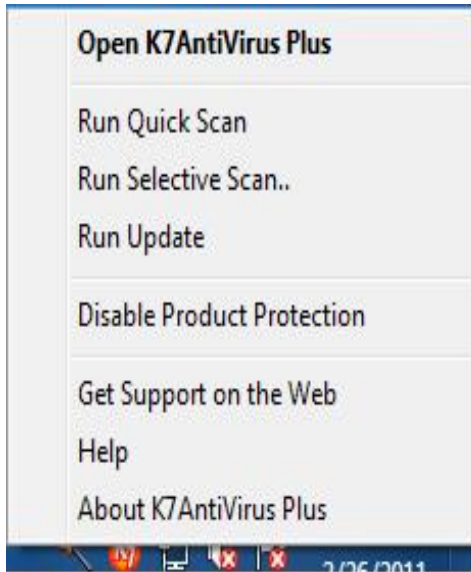
**Advice:**

Whenever you receive a shell open command registry value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Accessing the Context Menu

The K7 taskbar icon is available in your System Tray when your system starts. You can access the functions of K7AntiVirus Plus from the context menu that appears when you right-click your mouse on the  icon in the System Tray.



You can use the options in the above menu to access the features of K7AntiVirus Plus. Click on the required option in the shortcut menu to access the features.

To enable or disable features of the AntiMalware, Firewall, Privacy and AntiSpam components from the above menu; focus your mouse on the option and select the required option from the submenu that appears.

---

## Start Up Folders

### What are Startup folders?

Applications that are listed in the startup folders are loaded automatically when Windows starts. For example, if you place a Microsoft Word document in the Start Up folder, Word will run and automatically open that document; if you place a .wav file there, your audio software will play the music; and if you put a Web-page Favorites there, Internet Explorer (or your own choice of a browser) will run and open that Web page. The examples cited here could just be shortcuts to a .wav file or a Word document, and so on

If a new startup program is added to your user or all users startup folder, the agent alerts you. If the program added is known to be safe, the agent will allow it. If it is known to be spyware, the agent blocks it and warns you.

Any files or shortcut files placed in this folder are used for programs that should be automatically started for all users who will log on to this computer. This folder applies to all Windows NT, 2000, XP and 2003 versions. Possible folder paths are:

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup
C:\WINNT\Profiles\All Users\Start Menu\Programs\Startup
C:\Documents and Settings\All Users\Start Menu\Programs\Startup
```

**Advice:**

Whenever you receive a startup folder alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## System Check Points

There are several check points that need to be monitored in real-time so that spywares and viruses are identified and removed before they are installed in your system. The System Monitor monitors the following System Check Points:

- Startup Registry Values
- Shared Task Scheduler
- Shell Execute Hooks
- Shell Service Object Delay load
- NT Load and Run Values
- Boot Execute Value
- AppInit\_Dlls Value
- UserInit Program
- Windows Shell
- ScrnSave.Exe
- Context Menu Handlers
- Windows Services
- Logon Notification Handlers
- Shell Open Command
- Control Panel Listings
- User Shell Folders
- Windows Security Settings
- IE Browser Helper Objects

## Printed Documentation

- IE ToolBars
  - IE Extensions
  - IE URL Search Hooks
  - IE URL Settings
  - IE Security Settings
  - IE Zone Settings
  - IE Trusted Site List
  - Win.Ini
  - System.Ini
  - Host File
  - Startup Folders
- 

## System Monitor Alerts

The System Monitor continuously monitors the critical areas of your computer and warns you of the consequences of any changes made to your system. It helps in the early detection of viruses, and protects your computer from hidden threats before they run.

**See** [Configuring the System Monitor for more information](#)

If any system file or file association is modified or a new program is added to the Windows start-up, the System Monitor alert appears. You can select one of the following options:

Option	Description
<b>Details</b>	Displays the details of the change taken place
<b>Allow</b>	Allows the change that has occurred
<b>Block</b>	Blocks the change that has occurred
<b>Block Always</b>	Blocks such changes whenever they occur

Click the  button to close the alert.

---

## System Monitor Blocked Entries

The System Monitor Blocked entries are those suspicious changes that are detected and blocked by the System Monitor.


Select the entry in the **Blocked Events** list and its **Details** appear in the lower panel of the dialog.




Click the **UnBlock** option to allow the change.

To view more information about the entry, click the **More about this entry** option.


Click the  button to close the alert.

## System Tray Icon

Once you install K7AntiVirus Plus, its icon () appears in the System Tray. The icon reflects the protection status and provides direct access to a number of basic functions performed by the program. The status of the product is indicated by the appearance of the icon as described in the following table.

Icon	Status
	K7AntiVirus Plus is enabled and your computer is being protected
	K7AntiVirus Plus is disabled and your computer is <i>not</i> being protected
	The Real-time scan or Firewall is disabled

The icon also provides access to the basic functions of the application through a context menu. [See](#) [Accessing the Context Menu](#)

To open the context menu, right-click the  icon.

To open K7AntiVirus Plus main console to the default first screen, double-click the  icon.

## System Monitor Alert

The System Monitor warns you of any changes made to your system that are similar to those that occur when a new program is installed on your computer. If you have installed a trusted software you can accept the change. If you have not installed a program, then it is recommended you select to be prompted to see each of the changes before you accept them.

You can select one of the following options:

Option	Description
Details	Displays the details of the change taken place
Accept	Accepts the change made to your system
Prompt	Displays each change so that you can accept only the required changes

Click the  button to close the alert.

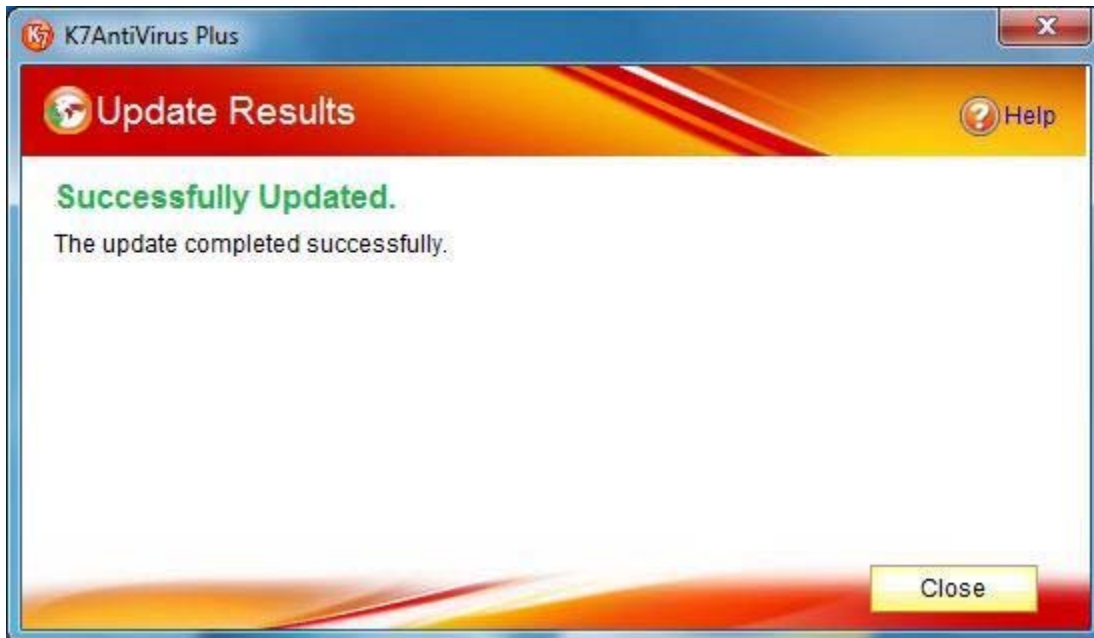
## Update Prompt

If updates are available for your product or you have selected to be prompted when updates are being downloaded or copied to your computer, alerts will be displayed.

The options on the alert are described below:

Option	Description
<a href="#">Click here to update now</a>	Updates your product
<a href="#">Click here to remind you after some time</a>	Reminds you to update your product after some time
<a href="#">Click here to remind you after 12 hours</a>	Reminds you to update your product after 12 hours

Once the product is updated, a message appears.



---

## User Init Value

### What is a UserInit Value?

The Userinit value specifies the programs that will be started when the user logs on to Windows. By default, Winlogon runs `Userinit.exe`, which takes care of operations like re-establishing

network connections, starting `Explorer.exe`, which is the shell for the Windows operating system, and running logon scripts.

The Windows registry can be modified to add programs to this list. This entry can also be used for making applications to start even before `Explorer.exe` runs. To do so, substitute `Userinit.exe` with the name of the program and then include instructions to start `Userinit.exe` in that program.

K7SystemMonitor watches for changes to this value under the following key:

```
HKLM\SW\MS\WinNT\CV\WinLogon
```

**Advice:**

Whenever you receive a UserInit value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## User Shell Folders

### What are User Shell folders?

Windows makes use of User Shell folders to indicate the default location for specific types of settings and data. These folders are usually common system folders like My Documents, Program Files and other standard Windows folders.

By default, the user shell folders location is in `%UserProfile%` that is `C:\Documents and Settings\user`. Some of the main user shell folders are:

- AppData
- Cookies
- Desktop
- Favorites
- History
- Local Settings
- NetHood
- Personal
- Programs
- Recent
- SendTo
- Start Menu
- Startup

## Printed Documentation

These values are stored under the key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Us  
er Shell Folders
```

Viruses and malware may use these settings to auto start themselves whenever Windows starts. For example, by changing the value of the Startup under the above-mentioned key to C:\Virus, all files present in this folder will be executed when Windows starts.

### Advice:

Whenever you receive a User Shell folder change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Win.Ini

### What is Win.Ini?

The `win.ini` file is the Windows initialization file that is located in the Windows folder. This has the various settings that is used when Windows starts. Any program that is listed after the `run=` or `Load=` will be executed when Windows Starts. Potentially harmful viruses also make entries here to get loaded when Windows starts.

### Advice:

Whenever you receive a `win.ini` value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## WinLogon Values

### What are WinLogon values?

The Winlogon Userinit entry specifies the programs that are run when you logon. This entry is generally changed by programs that would like to run before Windows Explorer user interface starts. This can be done by appending the required filename to the value of Userinit under the

key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon
```

The files specified in the Winlogon Shell will load automatically when the user logs on. This value is found under the following keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

The Shell by default points to Explorer.exe.

**Advice:**

Whenever you receive a WinLogon value change alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If you have not installed any such software that needs to run before Windows Explorer, this could possibly indicate a threat.

---

## Windows Security Settings

### What is Windows Security Settings?

Alerts when the Windows security settings are modified.

**Advice:**

Whenever you receive a Windows Security Settings alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Windows Services

### What is Windows Services?

Notifies whenever there is a change in the Services that get installed in the system.

**Advice:**

Whenever you receive a Windows Services alert from K7SystemMonitor, click on the **Details**

## Printed Documentation

button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Windows Shell

### What is Windows Shell?

Any file added in this entry will get loaded every time the system starts.

#### Advice:

Whenever you receive a Windows Shell alert from K7SystemMonitor, click on the **Details** button to view the changes that have taken place. If the changes specified have been made by you or by any software you had installed, select the **Backup** option; otherwise, select the **Restore** option.

---

## Worm Block Alert

The Worm alert appears if you have configured K7AntiVirus to prompt for action when suspicious mail activity is identified or when mails are sent continuously from your computer.

**See** [Configuring the Worm Blocking Settings](#) for more information

You can select one of the following options:

Option	Description
Disconnect	Stops the activity
Ignore	Ignores the activity

Click the  button to close the alert.

---

# Glossary

## 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.

**Autorun.inf:** Autorun.inf files are text files present in the root directory of a drive that contains information about the respective drive. This information includes any executable that must be automatically run when drive is accessed, the icon displayed for the drive and any other menu commands applicable to the drive.

## 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. BackdoorTrojans 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 harddisk.

**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 K7AntiVirus Plus moves uncleanable 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 improve antivirus management efficiency.

**Spyware:** Spyware refers to a 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 key strokes, 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.

**Tracking cookies:** Tracking cookies are bits of information stored on the computer by a browser which enable a website to uniquely identify a user.

**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.

# Index

<b>A</b>		files.....	24
activation your product .....	5	folders .....	24
reminder .....	63	Exclude list, adding files.....	64
alerts		<b>F</b>	
email virus.....	70	features .....	2
script.....	78	file extensions types.....	41
System Monitor.....	83	file types.....	40
Antivirus, configure .....	20	<b>G</b>	
automatically		general settings	
updating your product.....	15	scan .....	51
<b>C</b>		<b>H</b>	
current status		help conventions .....	3
quick view of.....	10	<b>K</b>	
viewing.....	10	K7AntiVirus Plus	
<b>E</b>		about.....	1
email scanning		disabling.....	11
configuring.....	25	enabling.....	10
disabling.....	27	<b>L</b>	
enabling.....	26	Licence Information.....	5
malicious attachments.....	29	<b>M</b>	
email server settings.....	28	main console	
exclude from protection		opening.....	8

## Printed Documentation

overview of .....	8	scan tasks	
malicious attachments .....	29	changing schedule of.....	46
messenger scanning .....	37	configuring.....	41
<b>O</b>		creating custom .....	43
Office files scanning .....	38	customizing .....	43
<b>Q</b>		deleting.....	47
Quarantine.....	34	manually running .....	47
adding files.....	35	scheduling .....	45
deleting files.....	36	scanning	
managing.....	34	entire computer .....	49
restoring files .....	35	file .....	50
QuickScan		floppy disk .....	49
configuring.....	42	folder .....	49
running .....	47	full system.....	49
<b>R</b>		hard drive .....	49
real-time scanning		multiple folders .....	51
configuring.....	20	removable drive .....	49
disabling.....	22	script scanning .....	38
enabling.....	21	shortcut menu.....	81
Root kits scan		system check points .....	82
running .....	48	configuring.....	33
<b>S</b>		System Monitor	
scan settings .....	39	configuring.....	31

disabling .....	32	automatically checking for.....	15
enabling.....	32	disabling automatic .....	17
events, viewing .....	34	manually checking for.....	16
system tray icon .....	84	updating your product.....	15
<b>T</b>		<b>V</b>	
threats, types of .....	23	virus information.....	53
Tracking cookies scan		virus protection, managing.....	19
running .....	48	<b>W</b>	
<b>U</b>		Word files, scanning .....	37
uninstalling your product .....	7	Worm Blocking settings .....	30
updates			