

# USER GUIDE

Guardian AntiVirus 2011

**Quick Heal Technologies (P) Ltd.**

<http://www.guardianav.co.in>

Copyright © 1993-2010 Quick Heal®

**All Rights Reserved.**

All rights are reserved by Quick Heal Technologies (P) Ltd.

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Quick Heal Technologies (P) Ltd, 603 Mayfair Towers II, Wakdevadi, Shivajinagar, Pune-411005, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies (P) Ltd. is liable to legal prosecution.

**Trademarks**

Quick Heal, Guardian and DNAScan are registered trademarks of Quick Heal Technologies (P) Ltd.

Microsoft, MSN, Windows and Windows Logo are trademarks of Microsoft Corporation. All brand names and product names used in this manual may be trademarks, registered trademarks or trade names of their respective companies.

# END USER LICENSE AGREEMENT

## IMPORTANT

PLEASE READ THIS USER LICENSE AGREEMENT CAREFULLY BEFORE USING THIS SOFTWARE.

BY USING THIS SOFTWARE OR BY CLICKING THE "I AGREE" BUTTON OR LOADING THE QUICK HEAL'S SOFTWARE, IN ANY WAY, YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS USER LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS BELOW, DO NOT USE THIS SOFTWARE IN ANY WAY AND PROMPTLY RETURN IT OR DELETE ALL THE COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

## Guardian License Agreement

This License is a legally enforceable contract between you as an individual (assuming you are above 18 years), or the Company or any legal entity that will be using the software (hereinafter referred to as 'you' or 'your' for the sake of brevity) referred to as the licensee, and Quick Heal Technologies Private Ltd (hereinafter referred as "Quick Heal" for the sake of brevity). In consideration of payment of the License Fee, which is a part of the price, evidenced by the Receipt, Quick Heal grants the Licensee, a non-exclusive and non-transferable right. Quick Heal reserves all rights not expressly granted, and retains title and ownership of the Software, including all subsequent copies in any media. This Software and the accompanying written materials are the property of Quick Heal and are copyrighted. Copying of the Software or the written material is expressly forbidden.

## DO'S & DON'TS

### You can:

- use one copy of the software on a single computer. In case of multi-user, use the software only on the said number of systems as mentioned on the packaging.
- make one copy of the software solely for backup purpose.
- install the software on a network, provided you have a licensed copy of the software for each computer that can access the software over that network.

### You cannot:

- sublicense, rent or lease any portion of the software.
- debug, decompile, disassemble, modify, translate, and reverse engineer the software.
- try making an attempt to reveal/discover the source code of the software.
- use for unlicensed and illegal purpose.

## MANDATORY ACTIVATION

Quick Heal warns you that in the process of installation of the software, the other security products/software installed on your computer may uninstall or disable if the same are not compatible with the software. The license rights granted under this Agreement are limited for the first twenty (20) days after you first install the Product unless you supply registration information required to activate your licensed copy as described in Activation Wizard of the Product. You can activate the Product through the Internet or telephone; toll charges may apply. You may also need to reactivate the Product if you happen to re-install the product due to some reasons. There are technological measures in this Product that is designed to prevent unlicensed or illegal use of the Product. You agree that we may use those measures. You agree that the software may use the measures that can control and prevent piracy of the software.

As the only warranty under this Agreement, and in the absence of accident, abuse or misapplication, Quick Heal warrants, to the original Licensee only, that the disk(s) on which the software is recorded is free from defects in the materials and workmanship under normal use and service for a period of thirty (30) days from the date of payment as evidenced by a copy of the Receipt. Quick Heal's only obligation under this Agreement is, at Quick Heal's option, to either (a) return payment as evidenced by a copy of the Receipt or (b) replace the disk that does not meet Quick Heal's limited warranty and which is returned to Quick Heal with the copy of the Receipt.

### **THIRD PARTY WEBSITE LINKS**

At some point the software product includes links to third party sites; you may link to such third party websites as the user of this software. The third party sites are not under the control of Quick Heal and Quick Heal is not responsible for the contents of any third party website, any links contained in the third party websites. Quick Heal is providing these links to third party websites to you only as a convenience and is not responsible for any kind of loss/ damage arising out of it.

### **SUPPORT**

Quick Heal offers support features during usage of this software i.e., Live Chat with technical support team and/ or the technical support team may, at your discretion, take remote computer access. The availing of this support will be solely at your discretion and you are solely responsible to take back up of the existing data/software/programs in your computer before availing such a support. Quick Heal will not be held responsible for any loss of data, any kind of direct/ indirect/ consequential loss or damage to data/ property arising during this entire process. If at any point of time the Technical Support team is of the opinion that it is beyond their scope, it will be the sole discretion of Quick Heal to suspend, cease, terminate or refuse such support as Quick Heal does not claim any warranty and/or guarantee of any kind in providing the support feature.

### **EMAIL/ELECTRONIC COMMUNICATION**

Once you register the software by activating the software product, Quick Heal may communicate with you on the contact information submitted during the registration process through email or other electronic communication device like telephone or a cell phone. The communication can be for the purpose of product renewal or product verification for your convenience.

### **STATUS UPDATE**

Upon every update of licensed copy, the Update module will send current product status information to the Quick Heal Internet Center. The information that will be sent to the Internet Center includes protection status like, which monitoring service is in what state in the system. The information collected does not contain any files or personal data. The information will be used to provide quick and better technical support for legitimate customers.

### **COLLECTION OF INFORMATION**

The software may collect the following information which may / may not contain any personally identifiable information either with or without your discretion/permission, solely for statistical purpose or enhancing and evaluating the ability, effectiveness and performance of the product in identifying and/or detecting the malicious behavioral pattern, inherently fraudulent websites and other Internet security threats/ risks. This information will not be correlated with any personally identifiable information and shall include, but not limited to:

- Any type of Executable files which the software may identify having a potentially malware behavioral pattern.
- Any type of information relating to the status of the software that whether there occurred any error while installing the software or the installation was successful.
- Any type of URLs of websites visited that the software deems inherently and potentially fraudulent.
- Any type of information that the software deems potentially fraudulent, posing security risks/ threats.
- Any type of information for identifying the Media Access Control (MAC) address of the Computer on which the software has been installed.
- Any type of information for identifying the Internet Protocol (IP) Address and information required for effective license administration and enhancing product functionality and usability.
- You admit that the information/data as collected above can be used for analyzing, preventing and detecting the potential internet security risks, publishing any type of data/ reports/ presentations on the trends collected, sharing the data to create awareness with any organizations, vendors.

**DISCLAIMERS**

This software package is provided as such without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness of the package. In no event will Quick Heal or its suppliers will be liable to you or anyone else for any damages arising directly/indirectly or consequential, including loss of data, lost profits or any other damages of data/ property arising out of the use or inability to use this software package ever.

Quick Heal reserves the right to co-operate with any legal process and may provide documents, information related to your use of the software.


The disclaimers and limitations set forth above will apply regardless of whether you accept the software.

ALL MATTERS SUBJECTED TO PUNE (INDIA) JURISDICTION

## ABOUT THIS DOCUMENT

This user guide contains all the information you need to install and use Guardian AntiVirus on Windows. Once familiar you can also use it for future reference. Full care has been taken to incorporate all details with the latest developments in the shipping.

The following are the list of conventions used in this document:

Convention	Meaning
<b>Bold Font</b>	Menu titles, commands, window titles, dialog elements, etc.
	Additional Information, Important Information, Notes etc.
<b>To do this</b> 1. Step 1 2. ....	Actions that must be performed
<b>Switch</b>	Command line switches.

## ABOUT GUARDIAN ANTI-VIRUS

Guardian AntiVirus gives your desktop needed protection from various Internet threats. It protects your desktop by automatically removing viruses, spyware, blocks malicious content from websites and much more.

### Complete Virus Protection

Guardian's powerful virus detection engine provides protection from new and more complex virus threats that are appearing. It automatically protects you from viruses, worms, Trojans and backdoors. It continuously scans the system in 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, riskware and other attack tools.

### Guardian AntiVirus Features

- Scans and cleans already infected PC before installation
- Cleans worms, backdoors and Trojans by cleaning registry and dropped files.
- Cleans virus-infected files automatically.
- Scans email messages and attachments before they reach to your inbox
- Downloads new updates automatically.
- Messenger service informs you about new Viruses, Hoaxes, general messages and Updates etc.
- Guardian Anti-Rootkit has been introduced. It detects and removes Rootkits from the system safely.

### Powerful email protection

- Guardian's unique on-line email protection scans email messages before they reach your inbox, no matter which email client you use.
- Prevents worms, Trojans and backdoors from sending infected emails.
- Attachment control for better protection from new and unknown worms.
- Remove email containing vulnerability e.g. IFRAME, MIME etc.

### AntiMalware

A new advanced malware scanning engine scans registry, files and folders at lightning speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

### Autorun Protection

Autorun malwares gain access to your system using Autorun feature of the Operating system, and autorun feature of removable drives such as CDs, DVDs or USB drives. This tool secures your PC against such malwares by disabling the autorun feature of your PC or USB drives

### Browsing Protection

Guardian AntiVirus blocks malicious content from the websites before the user can access them, using the Browsing Protection feature.

## TABLE OF CONTENTS

<b>INSTALLING GUARDIAN ANTIVIRUS</b> .....	<b>10</b>
GETTING STARTED .....	10
SYSTEM REQUIREMENTS .....	11
HOW TO INSTALL GUARDIAN ANTIVIRUS .....	13
UNINSTALLING GUARDIAN ANTIVIRUS .....	14
<b>REGISTERING AND RENEWING GUARDIAN ANTIVIRUS</b> .....	<b>15</b>
REGISTERING ONLINE WITH INTERNET CONNECTION ON THE SAME PC .....	15
REGISTERING OFFLINE WITH INTERNET CONNECTION ON SOME OTHER PC .....	16
IMPORTANT INFORMATION ABOUT MULTI-USER PACK REGISTRATION .....	17
REACTIVATION .....	17
RENEWAL .....	17
RENEWING ONLINE USING INTERNET ACCESS ON THE SAME PC .....	17
RENEWING OFFLINE USING INTERNET ACCESS ON SOME OTHER PC .....	18
CAN I INSTALL GUARDIAN ON ANOTHER COMPUTER? .....	19
WHAT TO DO IF MY PRODUCT KEY IS LOST? .....	19
<b>USING GUARDIAN ANTIVIRUS</b> .....	<b>20</b>
ABOUT GUARDIAN MAIN WINDOW .....	20
RIGHT SHELL MENU OPTIONS .....	22
USING HELP .....	22
PERFORMING MANUAL SCANS .....	23
SCHEDULING GUARDIAN ANTIVIRUS SCANNER .....	27
USING ONLINE PROTECTION .....	28
USING EMAIL PROTECTION .....	30
KNOWING ABOUT TRUSTED EMAIL CLIENTS .....	31
USING STARTUP SCAN .....	31
USING MESSENGER .....	32
VIEWING REPORTS .....	33
STATISTICS .....	34
VIEWING VIRUS LIST .....	36
QUARANTINE .....	36
AUTORUN PROTECTION .....	37
SYSTEM INFORMATION .....	40
CREATING EMERGENCY CD OR COMMAND LINE SCANNER .....	41
OVERVIEW OF NATIVE BOOT SCAN .....	42
USING GUARDIAN ANTIMALWARE .....	42
WHEN GUARDIAN ANTIMALWARE SHOULD BE USED? .....	44
USING EXTRA TOOLS .....	45
HIJACK RESTORE .....	45
WINDOWS SPY .....	46
TRACK CLEANER .....	46
ADVANCED SYSTEM EXPLORER .....	46
ABOUT SECTION .....	47
<b>USING ANTI-ROOTKIT</b> .....	<b>48</b>
SCANNING RESULTS AND CLEANING ROOTKITS .....	50
CLEANING ROOTKITS THROUGH GUARDIAN EMERGENCY CD .....	51
<b>CUSTOMIZING GUARDIAN ANTIVIRUS</b> .....	<b>52</b>

SCANNER - SCAN OPTIONS.....	53
SCANNER – MEMORY SCAN.....	57
SCANNER – DNASCAN.....	57
SCANNER – REGISTRY RESTORE.....	58
PROTECTION – ONLINE PROTECTION.....	59
PROTECTION - EMAIL PROTECTION.....	61
PROTECTION – PACKER IDENTIFICATION.....	63
UPDATES - AUTOMATIC UPDATES.....	64
UPDATES - MESSENGER.....	64
GETTING MESSAGES FROM LOCAL FOLDER OR NETWORK PATH.....	65
UPDATES - INTERNET SETTINGS.....	65
MISCELLANEOUS - EXCLUSIONS.....	66
MISCELLANEOUS - GENERAL.....	66
<b>CLEANING VIRUSES.....</b>	<b>68</b>
CLEANING VIRUSES ENCOUNTERED DURING SCANS.....	68
CLEANING VIRUS ENCOUNTERED IN MEMORY.....	69
CLEANING BACKDOOR, TROJAN, WORM AND MALWARES ENCOUNTERED IN MEMORY.....	69
<b>USING EMERGENCY CD AND COMMAND LINE SCANNER.....</b>	<b>70</b>
USING EMERGENCY CD.....	70
USING COMMAND LINE SCANNER.....	70
<b>UPDATING GUARDIAN ANTIVIRUS.....</b>	<b>72</b>
UPDATING GUARDIAN ANTIVIRUS FROM INTERNET.....	72
UPDATING GUARDIAN ANTIVIRUS WITH DEFINITION FILES.....	72
UPDATE GUIDELINES FOR NETWORK ENVIRONMENT.....	73
<b>TECHNICAL SUPPORT.....</b>	<b>74</b>

## INSTALLING GUARDIAN ANTI-VIRUS

Guardian has a simple installation procedure. During installation, read each installation screen, follow the instructions, and then click Next to continue.

Guardian should be installed on a virus-free machine. If you are sure that your computer is infected by a virus, use the Emergency CD to remove the viruses before installing Guardian. If you are not sure whether your computer is infected by viruses, continue with the installation. Guardian setup will scan your computer's critical area for viruses as a part of its installation process.

### GETTING STARTED

Before installing Guardian remember the following guidelines:

- If you have any other anti-virus software/hardware loaded, uninstall it before proceeding with Guardian installation. Two anti-virus software's co-existing on the same computer at the same time could be hazardous for your computer.
- Guardian requires approximately 750 MB of free disk space.
- Close all open programs before proceeding with Guardian installation.
- You must install with administrative rights.

## SYSTEM REQUIREMENTS

To use Guardian, your computer must meet the following minimum hardware requirements:

Operating System	Minimum Requirements
Windows 2000	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 256 MB of RAM</li><li>• 750 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li><li>• Service Pack 3 or above</li><li>• Internet Explorer 6 or higher</li></ul>
Windows XP	<ul style="list-style-type: none"><li>• 300 MHz Pentium Processor (or compatible) or higher</li><li>• 256 MB of RAM</li><li>• 750 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li><li>• Service Pack 2 or above</li></ul>
Windows Vista	<ul style="list-style-type: none"><li>• 1 GHz Processor (or compatible) or higher</li><li>• 512 MB of RAM</li><li>• 750 MB of free hard disk space</li><li>• DVD or CD-ROM drive</li></ul>
Windows 7	<ul style="list-style-type: none"><li>• 1 GHz Pentium Processor (or compatible) or higher</li><li>• For 32-bit 512 MB or higher RAM; for 64-bit 1 GB or higher RAM</li><li>• 750 MB of free hard disk space</li><li>• DVD-ROM / CD-ROM drive</li></ul>

### **Clients supporting Email scan**

Email scanning is supported for any of the following POP3 email clients:

- Microsoft Outlook Express 5.5 and above
- Microsoft Outlook 2000 and above
- Netscape Messenger 4 and above
- Eudora 5 and above
- IncrediMail
- Windows Mail

### **Clients not supporting Email scan**

Email scanning is not supported for the following protocol and email clients:

- IMAP
- AOL
- POP3s with Secure Sockets Layer (SSL)
- Web based email such as Hotmail and Yahoo! Mail
- Lotus Notes

### **SSL connections not supported**

Email Protection does not support encrypted email connections that use Secure Sockets Layer (SSL). If you are using SSL connections then your emails are not protected by Email Protection.



To send email through SSL connections, turn off Email Protection.

### **Guardian Anti-Rootkit Requirements**

- Guardian Anti-Rootkit is not supported 64-bit Operating Systems.
- It requires minimum 256 MB RAM installed on system.

### **Guardian Self-Protection**

- This feature is not supported for Microsoft Windows 2000 Operating System.
- For Microsoft Windows XP Operating System this feature is supported if Service Pack 2 or higher is installed.

## HOW TO INSTALL GUARDIAN ANTI-VIRUS

To start with installation, insert the Guardian CD in the CD-Drive. CD being enabled with auto-run feature will automatically prompt you with a list of available options.

1. Click **Install Guardian AntiVirus** to initiate the installation process.
2. Installation program will first perform Pre-install virus scan on your system to scan system memory, master boot record and system files for known viruses.
3. During Pre-install virus scan if a virus is found active in memory then follow below given procedures:
  - a. The installer automatically sets native scanner to scan and disinfect the system on next boot.
  - b. After disinfection restart your system and continue with installation. For more details refer to **Native Scan** in **User Guide**.
4. During the Pre-install virus scan, if viruses are not found in the critical system areas then installation would proceed further.
5. Click **Next**.
6. Read the License Agreement carefully; if you agree then choose **I Agree**. If you disagree then you cannot continue with the installation.
7. Click **Next**.
8. Click **Browse** to change the installation path if you want to install Guardian in different folder.
9. Click **Next**.
10. Read the important information relating to the product.
11. Click **Next**.
12. On Finish, **Registration/Re-activation** and **Updating** will be performed. In case if you wish to perform these activities later on then uncheck the above options and click **Finish**.

### If the CD auto-run menu does not appear

In some systems, CD-ROM drive does not automatically start a CD when it is inserted. In such case, to start the installation, please perform the following steps:

1. Double click the **My Computer** icon on your Desktop.
2. Right click the CD-ROM drive and select **Explore** option.
3. Double click **Autorun.exe** to start the installation.

## UNINSTALLING GUARDIAN ANTI-VIRUS

If due to any reason you wish to uninstall Guardian, please perform the following steps:

1. Click **Start -> Programs -> Guardian AntiVirus -> Uninstall Guardian AntiVirus** to initiate the un-installation process.
2. Guardian Uninstaller will prompt for the deletion of Reports, Quarantine and Backup files. If you wish to reinstall Guardian after some time then you can uncheck **Remove Report Files** and **Remove Quarantine/Backup Files**. Otherwise proceed by clicking **OK**.
3. If you are a registered user, a dialog will be displayed showing **Product key** of your copy. You are requested to note down your Product key as it will be needed in case you want to reinstall and reactivate Guardian.
4. Uninstaller will finally prompt you to **restart** your system for changes to take effect.



- Before proceeding with uninstallation, ensure that all other running programs are closed.
- To uninstall Guardian AntiVirus, administrative privilege is required.

## REGISTERING AND RENEWING GUARDIAN ANTI-VIRUS

After installation of Guardian AntiVirus, you will need to register your copy to get it activated. It is strongly recommended that you register and activate your copy immediately after installation; otherwise without activation it cannot be further updated. Registered users can get other benefits like technical support and messenger service. If your copy of Guardian is not registered within 20 days time period from the date of installation, it will expire and its further use will be considered as void.

Registration can be done by any of the following options:

- Online with Internet Connection on the same PC
- Offline with Internet Connection on some other PC

### REGISTERING ONLINE WITH INTERNET CONNECTION ON THE SAME PC

If your PC has Internet connection then you can activate Guardian AntiVirus online. To register Guardian online, please perform the following steps:

1. Click **Start** -> **Programs** -> **Guardian AntiVirus** -> **Activate Guardian AntiVirus** to launch the registration wizard.
2. Click **Next** to continue.
3. Select **Yes to I have Internet access on this computer** and click **Next** to continue.
4. Select **Activate the copy** and click **Next** to continue.
5. The **Activation Information** screen appears. Provide the 20-digit Product key and click **Next** to continue.
6. Provide details for **Purchased from** and **Register for** fields. Click **Next**.
7. The **Personal Information** screen appears. Provide details as requested. The fields marked with \* are mandatory fields. Click **Next** to continue.
8. The **Submit the Information** screen appears. Verify the information displayed. If any modifications are needed click **Back** and make the necessary modifications; else click **Next** to continue.
9. The screen indicating successful activation is displayed. The validity of Guardian AntiVirus is displayed. Click **Finish** to complete the Activation process.



1. You can find the Product key for your copy pasted on your User Guide and / or inside the box. If you have purchased the software online using credit card then you will find the Product key in the e-mail confirming your order.
2. Kindly stay connected to the Internet during the Registration process.

## REGISTERING OFFLINE WITH INTERNET CONNECTION ON SOME OTHER PC

In case if Internet connection is not available on your computer, you will need to register your copy by filling the registration form on our website. You can visit off-line activation page on our web site at <http://www.guardianav.co.in/offact.htm> with any system having Internet Connection. For example: Cyber cafe.

### This involves following important steps

- Getting details of your Guardian AntiVirus installation
- Visiting and filling off-line registration web form through some other PC having Internet access
- Receiving license.key file through email.
- Activating the Guardian AntiVirus installation using newly obtained license.key file.

### Detail procedure

When filling the registration form on our website you would also need following information of your installed copy:

- Product key
- Installation Number
- A valid email address.



1. You can find Product key for your copy pasted on your User Guide and / or inside the box. If you have purchased the software online using credit card then you will find the Product key in the email confirming your order.
2. Installation Number is available in Off-line Registration section of Guardian AntiVirus Registration Wizard. Choose **No** to '**I have Internet access on this computer**' and click **Next**. Choose **Offline registration through web** and click **Next** to get your **Installation Number**.

### Obtaining License File

Once the Product key and Installation Number are verified, you will have access to the Personal Information page wherein you are required to fill the relevant contact details. Once the registration details are submitted successfully you will get your unique License.key file via email on the email address provided by you at the time of registration. You will also get an option to download your License.key file on successful registration/activation. Take this License.key file to the computer where activation needs to be done.

### Activating Offline

Now proceed with the following process to activate your copy:

1. Click **Start** -> **Programs** -> **Guardian AntiVirus** -> **Activate Guardian AntiVirus** to launch the registration wizard.
2. Click **Next**.
3. Choose **No** to **I have Internet access on this computer**.
4. Click **Next**.
5. Select **Offline Registration through web**.
6. Click **Next**.
7. Click **Browse** and open the **License.Key** file.
8. On completion you will get successful activation message. The validity of Guardian AntiVirus is displayed.
9. Click **Finish** to complete the registration process.

## IMPORTANT INFORMATION ABOUT MULTI-USER PACK REGISTRATION

For Multi-user pack when the first Product key of Guardian is registered, registration information of the first Product key is automatically applied for all the other Product keys in the pack. As a result the Product keys that are registered after the registration of first Product key will have same user information and subscription expiry date.

## REACTIVATION

If due to any reason you need to reinstall your operating system or Guardian AntiVirus, it is necessary to reactivate your copy after reinstallation.

Reactivation is very easy and similar to the registration process. The changes in case of Reactivation are:

- On a PC where you have Internet access, you are required to choose **Re-activate the copy** option and provide the Product key of your copy and click **Next**.
- Offline Reactivation is similar to the corresponding registration process.

## RENEWAL

To renew your copy of Guardian you need to buy renewal code. You can purchase a renewal code from Guardian, or from nearest distributor or reseller.

## RENEWING ONLINE USING INTERNET ACCESS ON THE SAME PC

If your PC has Internet connection then you can renew Guardian online by performing the following steps:

1. Click **Start** -> **Programs** -> **Guardian AntiVirus** -> **Guardian AntiVirus**.
2. If your subscription to Guardian AntiVirus has expired then **Information** section of the **Status** window will show that the subscription to your copy of Guardian has expired. Click **Renew Now** button. If your subscription to Guardian has not expired, then click **About** menu and then click **Renew Now** button.
3. The Product key of the product will be displayed in the **Product key** field. Enter the renewal code in **Renewal Code** field. Enter the distributor name or reseller name in the **Purchased from** field.
4. Click **Next** to continue.
5. The subscription information such as **Current Expiry Date** and **New Expiry Date** will be displayed.
6. Click **Renew** to continue.
7. Your copy of Guardian AntiVirus will be renewed. Click **OK** to complete the renewal process.



If you have purchased an additional renewal code, then the renewal can be performed only after 10 days of the current renewal.

## RENEWING OFFLINE USING INTERNET ACCESS ON SOME OTHER PC

In case if Internet connection is not available on your computer, you will need to renew your copy by filling the renewal form on our website. You can visit off-line renewal page on our web site at <http://www.guardianav.co.in/offrenew.htm> with any system having Internet Connection. For example: Cyber cafe.

### This involves following important steps

- Getting details of your Guardian AntiVirus installation
- Visiting and filling off-line renewal web form through some other PC having Internet access
- Receiving license.key file through email.
- Renew the Guardian AntiVirus using newly obtained license.key file.

### Detail procedure

When filling the renewal form on our website you would also need following information of your installed copy:

- Product key
- Installation Number



Installation Number and Product key are available in Offline Renewal section of Guardian AntiVirus Renewal Wizard. Select '**Renew Offline**' and click **Next**. You will find the **Installation Number** along with the **Product key**.

### Obtaining License File

1. Once the Product key, Installation Number and Renewal code are verified, next page will be displayed with **User Name** and **Email Address** field. In case if your email address has been changed then please update the email address in this form.
2. Click the **Submit** button, to get unique License.key file via email on the email address provided by you. You will also get an option to download your License.key file on successful renewal. Take this License.key file to the computer where renewal needs to be done.


### Renewing Offline

Now proceed with the following process to renew your copy:

1. Click **Start** -> **Programs** -> **Guardian AntiVirus** -> **Guardian AntiVirus**.
2. If your subscription to Guardian AntiVirus has expired then **Information** section of the **Status** window will show that the subscription to your copy of Guardian has expired. Click **Renew Now** button. If your subscription to Guardian AntiVirus has not expired, then click **About** menu and then click **Renew Now** button.
3. Select **Renew Offline** option on this window.
4. Click **Next**.
5. Click **Browse** and open the **License.Key** file.
6. On completion you will get successful renewal message. The new validity of Guardian AntiVirus is displayed.
7. Click **OK** to complete the renewal process.

## CAN I INSTALL GUARDIAN ON ANOTHER COMPUTER?

If you install Guardian AntiVirus on another computer, after installation it is necessary to register your software. You must perform the registration procedure by providing new Product key. Any previously obtained Product key and License Keys are invalid and will not work on another computer.

 One Product key can only be used for one computer.

## WHAT TO DO IF MY PRODUCT KEY IS LOST?

Product key will serve as the users Identity. In case you lose the Product key, you can obtain your Product key by contacting Guardian Technical Support by paying nominal charges.

## USING GUARDIAN ANTI-VIRUS

All the features related to Guardian can be accessed from Guardian main window. In addition, you can also access Guardian main window or the features from Windows system tray. Proceeding by the default installation, Guardian protects your entire system. You do not have to manually start Guardian AntiVirus to protect your system in such cases.

You can manually start Guardian by any of the following ways:

- Click **Start -> Programs -> Guardian AntiVirus -> Guardian AntiVirus**.
- In Windows system tray, double click the **Guardian Online Protection** icon or right click **Guardian Online Protection** icon in system tray and select **Open Guardian**.
- At the prompt in DOS window, change the path to the directory where Guardian AntiVirus is located. Type **Scanner** and press **Enter**.

## ABOUT GUARDIAN MAIN WINDOW

The main window lets you access features, configure the options and access online help.

On the left side of the main window select the option that you want. You have following options:

<b>Status</b>	View the status of Guardian AntiVirus. This section provides status of important security scanning.
<b>Scan</b>	Virus scanning is obviously the most important component of any Anti-Virus software. Guardian scanner detects viruses in boot records, partition tables, executable files, compressed files, compressed exes, mailboxes, OLE files, script files, scrap etc.
<b>Tools</b>	Important tools can be accessed from this section such as Anti-Rootkit, Quarantine, Virus List, Scheduling Scan, System Information, Emergency CD, Autorun Protection and Messenger.
<b>Extra</b>	This section provides extra tools for system diagnosis and repair. Advanced tools like Hijack Restore, Windows Spy, Track Cleaner and Advanced System Explorer can be accessed from here.
<b>Reports</b>	View the activity reports of all the important modules.
<b>About</b>	This section provides details about Version, Virus Database, Subscription details and Technical Support. You can also Register or Re-activate Guardian AntiVirus from here.

Following are the other options available on the main screen:

<b>Options</b>	Customize the general options for Guardian AntiVirus.
<b>Update</b>	Update the virus definition files and Guardian AntiVirus components.
<b>Launch AntiMalware</b>	Scans for malicious softwares (Adwares, Dialers, Pornwares, Potentially unwanted software, Rouge applications, Spyware) and provides cure against them.
<b>Help</b>	Access help for Guardian AntiVirus.

## RIGHT SHELL MENU OPTIONS

<b>Open Guardian</b>	Launch Guardian AntiVirus.
<b>Launch AntiMalware</b>	Launch Guardian AntiMalware.
<b>Check New Messages</b>	Displays new messages received from Guardian.
<b>Enable/Disable Entertainment Mode</b>	Enables/Disables all Guardian prompts and notifications.
<b>View Messages</b>	Displays the messages received from Guardian.
<b>Enable/Disable Online Protection</b>	Enables/Disables Guardian Online Protection.
<b>Option</b>	Check or configure various Guardian AntiVirus options.
<b>Statistics</b>	Provides statistical information from Online Protection and Email Protection.
<b>Update Now</b>	Update Guardian AntiVirus.
<b>Scan Memory</b>	Scan System Memory for viruses.

## USING HELP

Help system consists of extensive topics, index, commands and procedures with general FAQs. Guardian provides online help for most of the message windows. You can get help on all the topics by any of the following ways:

1. Launching Help by clicking **Help** button from Scanner or Scanner Options.
2. Pressing **F1** when you need help.
3. Clicking the **Help** button in a dialog box.

## PERFORMING MANUAL SCANS

If Online Protection is enabled with default setting, you normally would not need to scan manually. However, you can manually scan your entire computer, or individual floppy disks, drives, network drives (mapped drives), USB data storage drives, folders, or files if you wish to. Although the default settings for manual scanning are usually adequate, you can adjust the options for manual scanning in the **Options** of Guardian AntiVirus.

### Performing a full system scan

A full system scan scans all boot records, drives, folders and files on your computer. To perform a full system scan:

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **My Computer**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After reviewing the statistics and report click **Close**.

### Performing My Documents scan

My Documents scan scans all the documents, spreadsheets, presentation and other files kept in My Documents folder. To perform My Document Scan:

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **My Documents**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After reviewing the statistics and report click **Close**.

### Performing a System Memory scan

Now you scan System Memory for viruses. To perform a System Memory scan:

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **System Memory**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After reviewing the statistics and report click **Close**.

### Performing a Windows folder scan

Windows folder is the primary folder of the Operating System. To perform a Windows folder scan:

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Windows Folder**.
4. Click **Scan**.
5. When the scan is complete, scan statistics and report will be provided.
6. After reviewing the statistics and report click **Close**.

### Performing scan on folder

Occasionally you would also like to scan specific folders. To perform scan on desired folder:

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, double click the **Scan Folder**.
4. Select the folder you want to scan. You can also choose multiple folders for a single scan. Select **Exclude Subfolder** if you do not wish to scan subfolders.
5. Click **OK** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. After reviewing the statistics and report click **Close**.

### Performing scan on specific files

Occasionally you would also like to scan specific file(s). To perform scan on desired file(s):

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, double click **Scan File**.
4. Select the file(s) you want to scan.
5. Click **OK** to initiate the scan.
6. When the scan is complete, scan statistics and report will be provided.
7. After reviewing the statistics and report click **Close**.

### Performing Native Boot Scan

Native Boot Scan is very useful to disinfect the system. In case the system is badly infected by a virus and it cannot be cleaned because the virus is active, use Native Boot Scan. This scan will be performed on next boot using Windows NT Boot Shell.

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Native Boot Scan**.
4. Click **Scan**.
5. A confirmation prompt will be displayed to set boot time scanner on next boot. Click **Yes**.
6. If you wish to scan your system immediately then click **Yes** to restart the system. If you wish to scan later when you boot the system next time then click **No**.

### Performing Mailbox Scan

Mailbox scan scans inside Outlook Express and Windows Mail's mailboxes for viruses. It deletes the infected mail ensuring your mailboxes remains clean and virus free.

1. Start **Guardian Scanner**.
2. In the Guardian Scanner main window, click **Scan** on the left pane.
3. In the Scan pane, click **Mailbox Scan**.
4. Click **Scan**. When the scan is complete, scan report will be generated.
5. After reviewing the statistics and report click **Close**.

### **Adding Item in My Profile for regular scan**

You can add a custom scan if you regularly scan a particular area of your computer and don't want to specify that area to be scanned every time. You can delete the scan when it is no longer necessary.

#### **To create a custom scan**

1. Start **Guardian AntiVirus**.
2. In the Guardian AntiVirus main window, click **Scan** on the left pane.
3. In the **Scan** pane, click **Add Item**.
4. If want to scan a folder or multiple folders then click **Add Folders** and select the desirable folder(s) and click **OK**. You can configure **Exclude Subfolder** while scanning of a specific folder. This will ignore scanning inside the subfolders while scanning. e.g. If you select C:\ drive for scan along with selecting Exclude Subfolder option, this will initiate scan for files available at the root of C:\ drive only.
5. You can add your desirable files to scan in a single custom scan. To add specific files, click on Add Files and browse for files and click **OK**.
6. Click **Next**.
7. Give a name to your custom scan.
8. Click **Finish** to save the custom scan.

#### **To scan a custom scan item**

1. Start **Guardian AntiVirus**.
2. In the Guardian AntiVirus main window, click **Scan** on the left pane.
3. In the **Scan** pane, select the custom scan item and click **Scan**.
4. When the scan is complete, scan statistics and report will be provided.
5. When you are done reviewing the statistics and report, click **Close**.

#### **To edit a custom scan**

You can edit your custom scan any time to add or remove the scan items. To edit a custom scan:

1. Start **Guardian AntiVirus**.
2. In the Guardian AntiVirus main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on the custom scan which you created previously.
4. Click **Edit Item**.
5. Make the changes and click **Finish** to save the changes.

#### **To remove a custom scan**

You can remove your custom scan any time. To remove a custom scan:

1. Start **Guardian AntiVirus**.
2. In the Guardian AntiVirus main window, click **Scan** on the left pane.
3. In the **Scan** pane, click on the custom scan item which you want to delete.
4. Click **Remove Item**.
5. A confirmation prompt will come. Click **Yes** to delete the custom scan item.

## To scan one or more drives

You can scan all or specific drive(s) available on your system. To scan the drive(s):

1. Start **Guardian AntiVirus**.
2. In the Guardian AntiVirus main window, click **Scan** on the left pane.
3. In the **Scan** pane, click the **Drives** section.
4. **Select Drive** dialog box appears. Herein check the drives you want to scan from the drives list box. You can check special selection for multiple drives by checking items in the Drive Types group.
5. Now click **Scan** button.

## Schedule Scan

You can schedule the scanner to scan automatically at predetermined time and intervals. For more details please see [Scheduling Guardian AntiVirus](#).

## Scan initiated by right click handler

You can easily initiate scan by using right click handler. To scan:

1. Right click on the object (Drive, Folder and File) you want to scan.
2. Select **Guardian Scan** from the right click menu.

## Scanning through DOS command line

If you are working in a DOS window, you can easily initiate scan for a specific drive, file or folder, from DOS command line. To scan:

1. In the DOS window prompt, changed to the directory path where you have installed Guardian AntiVirus.
2. At the prompt, type **SCANNER.EXE** and give the path to scan. **For example: Scanner.exe C:\Windows**
3. Press **Enter** to start the scan.

## Scan using DUMB mode

If you are working in a DOS window, you can easily initiate scan for a specific drive, file or folder, from DOS command line. To scan:

1. In the DOS window prompt, changed to the directory path where you have installed Guardian AntiVirus.
2. At the prompt, type **SCANNER.EXE /DUMB**. **For example: Scanner.exe /DUMB**
3. Press **Enter**. Guardian AntiVirus will start in dumb mode.
4. Now select the item you wish to scan.

## Scanning through DOS command line using DUMB mode

Using DOS command line you can scan in dumb mode. To scan using dumb mode:

1. In the DOS window prompt, changed to the directory path where you have installed Guardian AntiVirus.
2. At the prompt, type **SCANNER.EXE /DUMB** and give the path to scan. **For example: Scanner.exe /DUMB C:\Windows**
3. Press **Enter** to start the scan.

## Overview of DUMB mode scanning

Dumb mode scanning is recommended if no virus was detected during an ordinary scanning procedure but the system is still behaving strangely (for example, slow performance of applications, and so on). Otherwise, we do not recommend dumb scanning mode as it noticeably slows down the scanning speed of Guardian AntiVirus.

## SCHEDULING GUARDIAN ANTI VIRUS SCANNER

You can schedule the scanner to scan automatically at predetermined time and intervals. You can schedule the scan at first boot, one time, daily and weekly. This will supplement other automatic protection features to ensure that your computer remains virus-free.

You can easily schedule custom scan. Frequency can be set for daily and weekly scans, which additionally can refine your request to schedule it to occur every two days or every three days instead. Further you can also schedule the task to repeat at specific intervals.

### To create a new schedule scan

1. On the left pane of the main window, under Guardian AntiVirus, click **Tools**.
2. In the **Tools** pane, click **Schedule Scan**. Scan Scheduler wizard will appear.
3. Select **Create new Schedule Scan** and click **Next**.
4. Name your custom schedule scan under **Name of the Schedule Scan /Task**. For example: My Scan.
5. Select **First Boot** to schedule the scanner to scan at first boot of the day. When you select First Boot in this case you don't have to specify the time of the day to start the scan. Scan will take place only during the first boot no matter at what time you start the system. Otherwise set the frequency and time at which you want to scan the system. Most of the frequency options include additional options (Every day (s) and Repeat Task) that let you further refine your schedule scan. You can also configure the scanner to scan silently (without any user intervention) by selecting **Silent Scan** option. By default the **Schedule AntiMalware** option will be checked. This will perform a malware scan along with the virus scan. Select the schedule scan priority from **High, Normal** and **Low**. Set the additional options as necessary.
6. Provide **User Name** and **Password**.
7. Under **Setting**, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advance options while scanning. By default, setting has been set for adequate options for scanning.
8. When you are done, press **Next**.
9. Click **Add Folders**.
10. Select the Drives, folder or multiple folders to be scanned and press **OK**. You can configure **Exclude Subfolder** while scanning of a specific folder. This will ignore scanning inside the subfolders while scanning. e.g. If you select C:\ drive for scan along with selecting Exclude Subfolder option, this will initiate scan for files available at the root of C:\ drive only.
11. Click **Next**.
12. Review the summary of your custom scheduled scan.
13. When you are done, click **Finish**.

### To edit a scheduled scan

You can change the schedule of any scheduled scan. To edit a scheduled scan:

1. On the left pane of the main window, under Guardian AntiVirus, click **Tools**.
2. In the Tools pane, click **Schedule Scan**. Scan Scheduler wizard will appear.
3. Click **Modify Schedule Scan** and select schedule scan created previously.
4. Click **Next**.
5. Change the schedule as desired.
6. When you are done, click **Next**.
7. Change the scan area as desired.
8. Click **Next**.
9. Review the summary of your custom scheduled scan.
10. When you are done, click **Finish**.

### To delete a scan schedule

You can delete any scan schedule. To delete a scan schedule:

1. On the left pane of the main window, under Guardian AntiVirus, click **Tools**.
2. In the Tools pane, click **Schedule Scan**. Scan Scheduler wizard will appear.
3. Click **Delete Schedule Scan**.
4. To delete a single schedule scan, select the schedule scan and click **Remove**. To delete all the scheduled scans click **Remove All**.

## USING ONLINE PROTECTION

Online Protection prevents your system from virus attack by continuously monitoring the system and prevents virus infection from email attachments, Internet Downloads, network, ftp, floppy, Data storage devices, CD-DVD ROM file executables and during suspected file copying. All this is done in the background and you are notified only when a virus infected file is found or a virus like activity is detected.

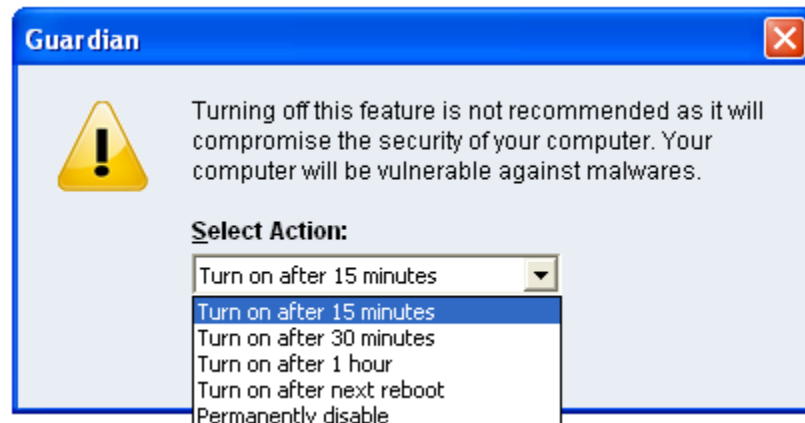
Guardian AntiVirus Online protection is configured to load automatically whenever you start your computer. Online Protection icon appears on the Windows taskbar.

### Disabling Online Protection

It is not recommended to disable Guardian AntiVirus Online Protection. It could be hazardous for your computer and data. But if you wish to do so, it can be done as follows:

### To disable Online Protection temporarily

1. Right-click **Guardian Online Protection** icon on the Windows task bar.
2. Click **Disable Online Protection**.
3. A prompt that recommends against turning off Online Protection appears. Select the time period for Online Protection to automatically enable itself or permanently disable using the **Select Action** drop-down box.



**Figure 3-2:** Disable Online Protection

4. Click **OK** to disable Online Protection.

You can now see that Online Protection icon's color is changed from Blue to Red in Windows System Tray. It means that Online Protection has been disabled temporarily or permanently based on your selection. If you have selected **Turn on after 15 minutes / 30 minutes / 1 hour** then the icon's color will change back from Red to Blue based on the time frame selected, to indicate that Online Protection has been enabled. If you have selected **Turn on after next reboot**, then the icon's color will change back to Blue at the next reboot. If you select **Permanently disable** then the icon's color will remain Red until you enable Online Protection manually.

### To disable Online Protection permanently

1. Start **Guardian AntiVirus**.
2. Click **Options**, under main windows menu of the Guardian AntiVirus.
3. Click **Online Protection** tab.
4. Uncheck the **Load Online Protection at Windows Startup** option.
5. Press **OK** to apply the changes.

## USING EMAIL PROTECTION

Email is the most common medium for spreading viruses and other malicious programs. Since email is most widely used for communication, newer viruses are using email as a medium to spread. Virus authors are always looking for new methods to automatically execute their viral codes using some vulnerability amongst popular email clients. Hence, for every user it is very important to have robust mail protection, which will block viruses or malicious programs at transferring level itself. Guardian Mail Protection has been redesigned to provide utmost & best protection to its users. Guardian AntiVirus provides reliable and robust email protection. It supports all email programs that use POP3 communications protocol. Your email messages are scanned automatically for any malicious code content within, and hence you are assured of virus free safe emails.

Email protection protects you from following threats:

- Viruses received in email and attachments.
- Partial messages.
- Email containing vulnerability such as MIME, IFRAME etc.

**The following features are supported in email protection:**

- Scanning of Incoming Mail.
- Silent mode (does not prompt) scanning.
- Remove multiple extension attachment(s).
- Remove Message/Partial type of mails.
- Actions if viruses are found are **Delete automatically** and **Repair automatically, delete if unsuccessful**.
- Backup before cleaning action.
- Scanning of ZIP attachments.
- Attachments Control.
- Trusted email clients allow only trusted email clients to send mails. This prevents new worms from further spreading to a greater extent.

See [Customizing Email Protection](#) for further set-up options.

### Disabling Email Protection

It is not recommended that you disable Guardian Email Protection. Your email communication may not remain safe any further, and your system shall be open for vulnerable virus infection through email.

**Email Protection can also be disabled as follows:**

1. Start **Guardian AntiVirus**.
2. Click **Options**, under main windows menu of the Guardian AntiVirus.
3. Click **Mail Protection** tab.
4. Uncheck the **Enable Email Protection** option.
5. Click **OK** to apply the changes.



Online Protection will not be loaded when you start your system thereafter

## KNOWING ABOUT TRUSTED EMAIL CLIENTS

Email is the most common medium for spreading viruses and other malicious programs. Since email is most widely used for communication, newer viruses are using email as a very easy medium to spread. Virus authors are always looking for new methods to automatically execute their viral codes using some vulnerability amongst popular email clients. **Worms** are also using their own SMTP engine routine to spread their infection.

Trusted email client is an advanced option which authenticates email-sending application on the system before they are sending emails. This option will prevent new 'Worms' from further spreading from your system. It contains a default email client list, which is allowed to send emails. Email client in the default list are Microsoft Outlook Express, Microsoft Outlook, Eudora and Netscape Navigator.

- ! 1. In case if the prompt comes for an application, which is known to you for sending email but not added in the Trusted email client list, click **Yes** to add the same.
- 2. In case if the prompt comes for an application, which is not known to you for sending email then select **No** as it could be a new **Worm**. We also request you to send the same file to [analyze@quickheal.com](mailto:analyze@quickheal.com) for further analysis of the same.

## USING STARTUP SCAN

Guardian Startup Scan keeps a watch on the programs trying to get automatic execution control. It also keeps a watch on some of the system files, which are commonly patched (or replaced) by certain worms/backdoors/trojans.

By default it is configured to check these on every boot operation. When a program takes an automatic execution control it can be:

- A program installed by you.
- A program installed without your knowledge, which in case might be a malicious program.

Guardian Startup Scan warns you in both the cases.

**It provides you three options:**

<b>Accept</b>	This registers the program or changes with Startup Scan and does not warn from the next boot. If you have installed a program or upgraded an existing program you shall get the warning, which should be registered, once with the Startup Scan. Press A to accept.
<b>Delete / Repair</b>	If it discovers a new entry in the system, it gives the option to delete. If selected to Delete, it removes the entry of the particular program and sends the file to Quarantine.  If it discovers that some old entry or system file has been modified it gives the option to repair. If Repair is selected it restores the old settings and sends the new file to Quarantine.
<b>Help</b>	It shows in detail what the alarm means. This will help you in deciding the course of action.

**General guideline for choosing the response is:**

If you have installed some program and you receive a Startup Scan warning for that program select **Accept**. If you have not installed any application knowingly and you get a Startup Scan warning choose **Repair / Delete** as this may be a new Trojan/Worm/Backdoor.

- ! This feature is not supported on Windows Vista, or above operating systems.

## USING MESSENGER

Guardian AntiVirus Messenger provides the trusted link for message delivery between Guardian Team and you (the User). It automatically gathers information from our web site and informs you about New Viruses, Hoaxes, Upgrade availabilities and other information. It can be also used from Local Folder or Network path.

Guardian AntiVirus Messenger icon on the tray indicates that the messenger is running. By default Guardian AntiVirus Messenger is configured to load automatically.

The messenger starts blinking whenever there is a new message. Click the blinking ball to view the message. A detailed log of messages is also maintained.

Color	Indicates
Red	Virus Alert
Amber	Hoax Information
Green	Upgrade
Blue	General

### Viewing Messages

To view the messages, do the following steps:

1. Right click **Guardian AntiVirus** icon from windows system tray.
2. Click **View Messages** to open the Newsletter Viewer containing the list of all the messages with date, type and subject.
3. Select the message you want to view.
4. Click **View** to see the particular message. The message is displayed instantly. You can use **Prev** and **Next** buttons to browse through the other messages. Click **Close** to move back to the Newsletter Viewer.
5. Click **Close Newsletter Viewer**.
6. Click **Minimize** to minimize the Messenger.

### Disabling Messenger

If you turn off Guardian AntiVirus Messenger then you are going to miss the important information related to new threats, updates and other information about Guardian AntiVirus.

#### Guardian Messenger can also be disabled as follows:

1. Start **Guardian AntiVirus**.
2. Click **Options**, under main windows menu of the Guardian AntiVirus.
3. Click **Messenger** tab.
4. Uncheck the **Enable Messenger** option.
5. Press **OK** to apply the changes.

### To check the Message Instantly:

By default the messenger is configured to check for the message automatically from Internet. See [Customizing Guardian AntiVirus Messenger](#). You can also check the message any time instantly. To check the message instantly:

1. Right Click **Guardian AntiVirus** icon from windows system tray.
2. Select **Check New Messages**.

This checks the new message if available on Guardian website instantly (subject to the availability of internet). You can also see the status of the messenger, configure Messenger and view message log from here.

## VIEWING REPORTS

Guardian AntiVirus Reports provide detailed information about the different module's functioning & virus scans sessions. Activity Log generates log for the following module:

- Scanner
- Online Protection
- Email Protection
- Startup Scan
- Scheduler
- Quick Update
- Memory Scan
- Registry Restore
- Native Scanner
- AntiMalware Scan
- Browsing Protection

### To view reports

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Reports**.
3. Now click the desirable report section which you want to see.

Reports contain a list of activity logs for each module with details such as scan date, scan time & report for different scan session.

- Click **Details** to view details about the selected log entry. The Detail information consists of additional information regarding viruses detected and action taken against those viruses. To see previous log, click **Prev**. To see Next log, click **Next**.
- Click **Delete** to delete selected scan log entry.
- Click **Delete All** to delete all scan log entries for that particular module.



**Print** and **Save As** add-ons are provided in Reports.

## STATISTICS

Guardian now provides statistics for Online Protection, and Email Protection. Following are the statistics provided by Guardian:

Online Protection Statistics	
<b>Number of files scanned</b>	Provides information about total number of files scanned.
<b>Number of infected files</b>	Provides information about total number of infected files found.
<b>Number of suspicious files</b>	Provides information about total number of suspicious files found.
<b>Number of packed files identified</b>	Provides information about the number of packed files found.
<b>Last file scanned</b>	Provides information about the last scanned file.
<b>Last file found infected</b>	Provides information about the last file which was found infected.
<b>Last infection name</b>	Provides information about the Virus or Malware which was recently detected.
<b>Last file found suspicious</b>	Provides information about the file which was found suspicious recently.
<b>Last packed file identified</b>	Provides information about the last packed file that was identified.
<b>Last packer identified</b>	Provides information about the last type of packer that was identified.

<b>Email Protection Statistics</b>	
<b>Number of emails scanned</b>	Provides information about total number of emails scanned for infection.
<b>Number of emails with attachments</b>	Provides information about total number of email received along with attachments.
<b>Number of infected emails</b>	Provides information about total number of emails found infected.
<b>Number of attachments</b>	Provides information about total number of attachments received.
<b>Number of infected attachments</b>	Provides information about total number of attachments found infected.
<b>Number of suspicious attachments</b>	Provides information about total number of attachments found suspicious.
<b>Number of multiple extensions attachments blocked</b>	Provides information about total number of attachments blocked having multiple extensions. e.g. .doc.exe.
<b>Number of vulnerable emails blocked</b>	Provides information about total number of vulnerable emails blocked.
<b>Number of attachments blocked by attachment control</b>	Provides information about total number of attachments blocked as per the Attachment control policy.
<b>Type of attachments received by user mostly</b>	Provides information about attachments which is mostly received by the user. e.g. .doc (Office Document file).
<b>Type of attachments blocked mostly</b>	Provides information about attachments which is being blocked mostly as per the Attachment control policy.
<b>Last application blocked attempting to send mail</b>	Provides information about an un-trusted application which was blocked while sending mails as per Trusted Email Client policy.
<b>Number of attempts to send mail blocked</b>	Provides information about total number of attempts of sending mails by un-trusted email clients that were blocked as per Trusted Email Client policy.
<b>Since System Start</b>	Under this category, Guardian provides statistics since system start. Statistics under this category are purged on every shutdown or restart.
<b>Since Installation</b>	Under this category, Guardian provides statistics since installation.

## VIEWING VIRUS LIST

Guardian AntiVirus Virus List provides an exhaustive database of respective virus names along with their category.


### Viewing Virus List

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Tools**.
3. Click **Virus List**. For the first time Virus List will take considerable time to load the list.

### Virus List Overview

To find for a virus in the virus list:

1. Click **Find**.
2. Type the name of virus you want to find.
3. Click **Find**.

 Click **Print** to take a print-out of the virus list.

<b>Latest</b>	Latest section contains the threats, added in the daily updates.
---------------	--

## QUARANTINE

Quarantine helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Guardian AntiVirus encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of infected file before repairing. Backup functionality is available by selecting **Backup before repairing** option under Scanner's settings.

### To launch Quarantine

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Tools**.
3. Click **Quarantine**.

You can perform the following tasks with the Quarantine feature:

<b>Add</b>	Add a file to the Quarantine module.
<b>Remove (Delete)</b>	Delete a quarantine file.
<b>Remove All</b>	Delete all the Quarantine files.
<b>Restore</b>	Restore a file from Quarantine to its original location.
<b>Send</b>	You can send the quarantined file to our research lab for further analysis. Select the file which you wish to submit and click <b>Send</b> .

In the Quarantine feature, when a suspicious file is selected and the **Send** button is clicked, a prompt appears requesting permission to obtain your email address. You also need to provide a reason for submitting the files. Select from the following reasons:

<b>Suspicious File</b>	Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
<b>File is unrepairable</b>	Select this reason if Guardian has been able to detect the malicious file on your system during its scans, but has not been able to repair the infection of the file.
<b>False positive</b>	Select this reason if a non malicious data file that you have been using and are aware of its function, has been detected by Guardian as a malicious file.

## AUTORUN PROTECTION

Autorun malwares gain access to your system using Autorun feature of the Operating system, and autorun feature of removable drives such as CDs, DVDs or USB drives. This tool secures your PC against such malwares by disabling the autorun feature of your PC or USB drives.

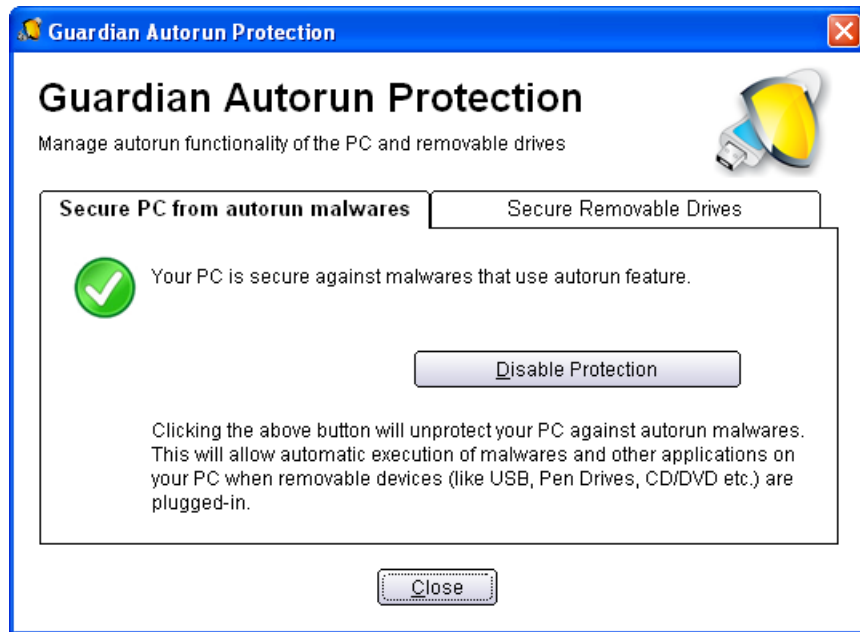
Autorun Protection provides two types of protection:

- Secure PC from autorun malwares.
- Secure removable drives.

### Secure PC from autorun malwares

To safeguard your PC against autorun malwares, please perform the following steps:

1. Click **Tools** -> **Autorun Protection** from the Guardian AntiVirus main window.
2. **Guardian Autorun Protection** window opens. In the **Secure PC from autorun malwares** tab, click **Enable Protection** button.
3. Autorun feature is now disabled on your PC protecting it from autorun malwares.



**Figure 3-3:** Secure PC from autorun malwares

- ! Although Guardian recommends that you keep the autorun feature of your PC disabled, but if you wish to enable the Autorun feature of your PC, just follow the steps mentioned earlier, and in Step 2 click the **Disable Protection** button to enable autorun on your PC.

## Secure Removable Drives

Guardian AntiVirus safeguards your USB devices from autorun malwares. Autorun feature of the removable drive is one of the mediums for malwares to gain access into the system. The **Secure Removable Drives** feature prevents autorun malwares from using your removable device as an infection spreading medium. Securing the removable drive also ensures that the drive, if connected to an infected system, cannot be used for spreading autorun malwares on other system.

To safeguard removable drives please perform the following steps:

1. Click **Tools** -> **Autorun Protection** from the Guardian AntiVirus main window.
2. Click the **Secure Removable Drives** tab.
3. The removable drives plugged into your system will be listed in the **Select a removable drive** drop-down box. Select the drive and click **Secure Removable Drive** button.
4. The drive will be secured against autorun malwares when used in other systems.



**Figure 3-4:** Secure Removable Drives

**!** Although Guardian recommends that you keep the autorun feature of your USB drive disabled but if you wish to enable the Autorun feature of the USB drive, just follow the steps mentioned earlier and in Step 2 click the **Un-secure Removable Drive** button to enable autorun on your USB drive. Insert the same removable drive for un-secure that has been secured using Guardian AntiVirus.

## SYSTEM INFORMATION

Guardian AntiVirus System Information is an essential tool to gather critical information of a Windows based system for following cases:

<b>To detect new Malwares</b>	This tool gathers information to detect new Malwares from Running processes, Registry, System files like Config.Sys, Autoexec.bat etc.
<b>To get Guardian AntiVirus information</b>	It gathers information of the installed version of Guardian AntiVirus, its configuration settings and Quarantined file(s), if any.

### Submitting System Information file

This tool generates an INFO.QHC file at C:\ and submits the same automatically to [sysinfo@quickheal.com](mailto:sysinfo@quickheal.com).



INFO.QHC file contains information in text and binary format. It contains critical system details and installed Guardian AntiVirus version details. Information contains automatic execution of files (through Registry, Autoexec.bat, System.ini and Win.ini) and Running processes along with their supported library details. These details are used to analyze the system for new Malwares and proper functioning of Guardian AntiVirus. The above information is used to provide better and adequate services to customers. This tool doesn't collect any other personally identifiable information, passwords etc. We respect your privacy; rest assured this information will not be shared or disclosed.

### Generating System Information

To generate system information follow the below given steps:

1. Start **Guardian AntiVirus**.
2. Click **Tools** from the left pane.
3. Click **System Information**.
4. Select the system information generating reason. If you are suspecting new Malwares in your system then select **I suspect my system is infected by new Malwares** or if you are facing problem while using Guardian AntiVirus then select **I am having problem while using Guardian**. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Guardian Technical Support.

## CREATING EMERGENCY CD OR COMMAND LINE SCANNER

You can create your own emergency bootable CD that will help you to boot your Windows PC and scan and clean all the drives including NTFS partitions. This helps in cleaning badly infected PC from file infecting viruses which cannot be cleaned from inside Windows. This feature works on Windows 2000 and above operating system.

You can create an emergency CD or command line scanner from Guardian AntiVirus at any time. This will be created with the latest virus signature pattern file used by Guardian AntiVirus on your system.

### To create an Emergency CD

To create Guardian Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

### Creating Emergency CD

1. Start **Guardian AntiVirus**.
2. Click **Tools** from the left pane.
3. Click **Emergency CD**.
4. Click **Next**.
5. Select **Create Emergency CD**, click **Next**.
6. Bootable files required to make the CD bootable. Select **Operating System Installation** CD option and insert the Operating CD (Windows XP and Windows 2003 operating system CD only). Select the CD-Rom drive.
7. Click **Next**.
8. System files will be fetched from the installation CD.
9. Remove the Operating System Installation CD and insert a blank writable CD.
10. Select the CD-Rom drive.
11. Click **Next**.
12. Emergency CD will be created.

### Creating Emergency CD using system files

If you have created emergency CD earlier by providing Microsoft Windows Installation CD using Emergency CD Creation Wizard, then you can quickly burn the emergency CD again by performing the steps that follow:

1. Start **Guardian AntiVirus**.
2. Click **Tools** from the left pane.
3. Click **Emergency CD**.
4. Click **Next**.
5. Select **System files used earlier while creating emergency CD**.
6. Click **Next**.
7. System files used earlier for CD creation will be fetched automatically.
8. Remove the Operating System Installation CD and insert a blank writable CD.
9. Select the CD-Rom drive.
10. Click **Next**.
11. Emergency CD will be created.

## To create Command line scanner

You can create DOS Command line scanner using Emergency CD wizard.

1. Start **Guardian AntiVirus**.
2. Click **Tools** from the left pane.
3. Click **Emergency CD**.
4. Click **Next**.
5. Select **Save Command line scanner** at option provided.
6. Browse the folder or type the path where you wish to create command line scanner.
7. Click Next.
8. Command line scanner will be created.

In case if you wish to disinfect the badly infected system it is recommended that write a CD by copying Command line Scanner folder.

 See [Using Emergency CD or Command Line Scanner](#).

## OVERVIEW OF NATIVE BOOT SCAN

Native Boot Scan is an advance administration tools. In short it schedules the system to boot in Windows NT boot shell on next boot. On next start Native Boot scan will start before the desktop is loaded. It scans all drives and detect/clean virus infections on your computer. This activity is quite fast and reliable, without the risk of spreading the infection any further. This will help you in detecting and cleaning even the most cunning Rootkits, spywares, special purpose Trojans and loggers. Additionally Native Boot Scan cleans the registry entries created/modified by malwares.

Native Boot Scan works with all **Windows-supported file systems**, i.e. **FAT32, NTFS**, as well as less common storage devices, such as SCSI/RAID. See [Performing Native Boot Scan](#).

## USING GUARDIAN ANTIMALWARE

Guardian AntiMalware is a new advanced malware scanning engine. It scans registry, files and folders at lightening speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

### Start Guardian AntiMalware

Guardian AntiMalware Scan can be started from:

#### Start Guardian AntiMalware from Guardian AntiVirus Program Group

To launch Guardian AntiMalware, click **Start -> Programs-> Guardian AntiVirus -> Guardian AntiMalware**.

#### Start Guardian AntiMalware from Guardian AntiVirus

1. Start **Guardian AntiVirus**.
2. Click **Launch AntiMalware**.
3. Guardian AntiMalware program will start.
4. Click **Scan Now** to initiate AntiMalware Scanning.


### Start Guardian AntiMalware from Guardian AntiVirus system tray icon

1. Right click Guardian AntiVirus system tray icon.
2. Click **Launch AntiMalware**.
3. Click **Scan Now** to initiate AntiMalware Scanning.

### Guardian AntiMalware Action on Malware found

While scanning for malwares Guardian AntiMalware displays malicious files, folders and registry entries related to various malwares. Once the scanning is complete, a list will be displayed for detected malwares containing malicious files, folders and registry. You can un-check specific file, folder or registry entries within displayed list, but be ensured that all un-checked items are not malicious and belongs to a genuine application.

You can take following action once the scanning is complete:

<b>Clean</b>	Selecting this action will clean the malwares and its remnants from the system. If you have un-checked specific file, folder or registry entry then you will be prompted whether you wish to exclude those items in future scan. If you wish to permanently exclude those items then click <b>Yes</b> , otherwise click <b>No</b> for temporary exclusion.
<b>Skip</b>	Selecting this will not take any action against malwares in your system.
<b>Set System Restore point before cleaning</b>	Selecting this option will create System Restore point before the cleaning process starts in your system. This enables you to revert the cleaning done by Guardian AntiMalware by using Windows System Restore facility.  <b>Set System Restore</b> point feature is not available on Windows 2000 operating system.
<b>Malware Details</b>	Malware details are available at <a href="http://www.guardianav.co.in">http://www.guardianav.co.in</a> website.

### Guardian AntiMalware Report

To view detailed AntiMalware scanning report, please refer [Guardian AntiVirus Reports](#) section.

## Guardian AntiMalware Settings

<b>Scan for suspicious items</b>	<p>A signature free scanning to detect malware traces based on heuristic. To enable Scan for Suspicious items please follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Start <b>Guardian AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Select <b>Scan for Suspicious items</b>.</li><li>4. Click <b>OK</b> to save the changes.</li></ol>
<b>Exclusion</b>	<p>You can configure Guardian AntiMalware to skip scanning of certain files and folders.</p> <p><b>To exclude a file from AntiMalware scanning:</b></p> <ol style="list-style-type: none"><li>1. Start <b>Guardian AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Click <b>Add File</b>.</li><li>4. Select the file to be excluded and click <b>Open</b>.</li><li>5. Click <b>OK</b> to save the changes.</li></ol> <p><b>To exclude a folder from AntiMalware scanning:</b></p> <ol style="list-style-type: none"><li>1. Start <b>Guardian AntiMalware</b>.</li><li>2. Click <b>Settings</b>.</li><li>3. Click <b>Add Folder</b>.</li><li>4. Select the folder to be excluded and click <b>OK</b>.</li><li>5. Click <b>OK</b> to save the changes.</li></ol>

## WHEN GUARDIAN ANTIMALWARE SHOULD BE USED?

Guardian AntiMalware should be used in following cases:

- Guardian Online Protection has detected a malware and recommending you to scan your system using Guardian AntiMalware.
- Guardian AntiVirus Scanner has detected a malware during scan and recommending you to scan your system using Guardian AntiMalware.
- In case of visible changes in your system. e.g. Desktop wallpaper changed, Internet Explorer functionalities changed such as default website and search page are changed, Rougeware applications are installed etc.

## USING EXTRA TOOLS

Guardian AntiVirus consists of advanced tools which can help user by performing following activities:

- Restore the default Internet Explorer settings.
- Restore the important system settings.
- Remove all known lists that can expose your privacy.
- Provide important information of an application.
- Provide all important information related to your computer such as running process, installed BHO's, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection.

## HIJACK RESTORE

Hijack Restores, restores the important Internet Explorer settings to default settings. Internet Explorer settings modified by Malwares, Spywares, Genuine applications and even by you can be easily restored to default setting using Hijack restore. This tool also restores certain other critical operating system settings like registry editor and task manager.

### Using Hijack Restore

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Extra**.
3. Click **Hijack Restore**.

Restoring Internet Explorer Browser Settings	
<b>Settings</b>	This section displays the important Internet Explorer settings which can be restored using Hijack Restore.
<b>Current Settings</b>	This section displays the current Internet Explorer settings.
<b>Previous/Default Settings</b>	This sections displays the last or default Internet Explorer settings.
<b>Check All</b>	Select all Internet Explorer to restore previous or default settings.
<b>Restore default Host file</b>	Select this option to restore default Host file. Click Default Host file to configure your own Host file so that during restore of the host file your settings are well preserved. Type the IP address and Host name and click Add. To edit the existing entry select the entry and click Edit. To delete select the entry and click Delete.
<b>Restore important system settings</b>	Critical system settings can be restored using this option. This setings generally modified by the Malware/Spywares to disable specific and important feature of the Operating System such as Registry Editor, Task Manager etc.
<b>Restore Now</b>	Restores the Internet Explorer settings to its default or at previous stage. You can restore specific settings by selecting specific settings and click <b>Restore Now</b> . To restore all the settings select <b>Check All</b> and click <b>Restore Now</b> .
<b>Undo</b>	This feature revert the last restoration and giving a chance to user to undone the changes.

## WINDOWS SPY

This tool can be used to find out more information about an application or process whenever required. At times it happens that we keep on getting dialog boxes or messages that are shown by spyware or some malware and we are not able to locate the malware. In such situation this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

- Application Name
- Original File Name
- Company Name
- File Description
- File Version
- Internal Name
- Product Name
- Product Version
- Copyrights Information
- Comments

### Using Windows Spy

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Extra**.
3. Click **Windows Spy**.
4. Click **Drag** and move the mouse pointer on the application.
5. A window will be opened displaying above mentioned information.
6. If you wish to terminate that application or window then click **Kill Process**.

## TRACK CLEANER

Track Cleaner removes the entire list that expose your privacy. Many applications store the list of recently opened files in their internal format to help you open them again for easy of use purpose. This feature of Windows is good but at the same time on the systems which is used by more than one user it may happen that the users privacy is compromised. Track Cleaner helps delete all the tracks of such applications and prevent privacy.

### Using Track Cleaner

1. Start **Guardian AntiVirus**.
2. In the left pane of the Guardian AntiVirus main window, click **Extra**.
3. Click **Track Cleaner**.
4. To clear the privacy item, select the application and item that should be cleaned and click **Start Cleaning**.
5. The selected items will be cleaned.
6. To clear all the privacy item, select **Check All** and click **Start Cleaning**.
7. All items will be cleaned.

## ADVANCED SYSTEM EXPLORER

This tool provides all important information related to your computer such as running process, installed BHO's, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection. This will help diagnose the system for tracing existence of any new malware or riskware.

## ABOUT SECTION

Guardian AntiVirus About section provides following information:

- Guardian AntiVirus Version
- Guardian AntiVirus Virus Database
- License Information

Following options are also available in About Section:

<b>License Details</b>	License Information and End User License Agreement (EULA) are available under this section.  <b>Update License Details:</b> Click <b>Update License Details</b> button to synchronize any updates in your License information with Guardian Activation Server.  <b>Print License Details:</b> Click <b>Print License Details</b> to print the existing subscription information.
<b>Activate Now</b>	If Guardian AntiVirus is not activated then Activate Now button is available in About section. Activate Now helps you to activate your copy.
<b>Support</b>	Support section provides information about Technical Support guidelines and Guardian Support's contact details. You can locate the nearest Guardian Support team.

## USING ANTI-ROOTKIT

Guardian Anti-Rootkit is a program that proactively detects and cleans rootkits that are active in the system. This program scans objects like running Processes, Windows Registry and Files and Folders for any suspicious activity and detects the rootkits without any signatures. It detects most of the existing rootkits and is designed to detect the upcoming rootkits and also provides the option to clean them.

It is recommended that Guardian Anti-Rootkit should be used by person having certain knowledge of the operating system or with the help of Guardian Technical Support engineer. Improper usage of this program could result in unstable system.

### To Start Guardian Anti-Rootkit from Guardian AntiVirus

1. Start **Guardian AntiVirus**.
2. In the left pane of main window click **Tools**.
3. Click **Guardian Anti-Rootkit** (icon with R on the shield).
4. Guardian Anti-Rootkit program will start.

### Using Guardian Anti-Rootkit

1. Start **Guardian Anti-Rootkit**.
2. In the left side of the main window click **Start Scan**.
3. Guardian Anti-Rootkit will start scanning your system for suspicious rootkit activity in running Processes, windows registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry, Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

<b>Stop Scanning</b>	During scan you can select Stop Scan to stop the scan, Guardian Anti-Rootkit will prompt before stopping the scan.
<b>Close</b>	Click Close to quit Guardian Anti-Rootkit. If you choose to close the application while scanning is in progress, it will prompt to stop the scan.
<b>Error Report Submission</b>	Due to infection or some unexpected conditions in system, scanning of Guardian Anti-Rootkit may fail. On failure you will be asked to re-scan your system and submit error report to Guardian Team for further analysis.

With the help of Scan Settings you can select what item to scan during scan process.

### Configuring Guardian Anti-Rootkit for Scan

1. Start **Guardian Anti-Rootkit**.
2. Click on the **Settings** button on top bar of Guardian Anti-Rootkit.
3. Settings dialog box will appear.
4. By default Guardian Anti-Rootkit is configured for Auto Scan where it scans appropriate predefined system areas.

<b>Auto Scan</b>	<p>Auto Scan is default scan option provided by Guardian Anti-Rootkit. Under Auto Scan Guardian Anti-Rootkit scans appropriate predefined system areas. During Auto Scan, scanning is performed for:</p> <ul style="list-style-type: none"> <li>• Hidden Processes.</li> <li>• Hidden Registry entries.</li> <li>• Hidden Files and Folders.</li> <li>• Executable ADS.</li> </ul>
<b>Custom Scan</b>	<p>By selecting Custom Scan radio button, you can configure following options:</p>
<b>Detect Hidden Process</b>	To scan for running hidden processes in the system.
<b>Detect Hidden Registry Items</b>	To scan for hidden items in Windows Registry.
<b>Detect Hidden files and folders</b>	<p>To scan for hidden files and folders in the system and executable ADS (Alternate Data Streams). You can choose option:</p> <ol style="list-style-type: none"> <li>1. Scan drive on which Operating System is installed.</li> <li>2. Scan All Drives to perform scanning in all fixed drives.</li> <li>3. Alternate Data Streams (ADS) to scan for executable ADS.</li> </ol>
<b>Scan drive on which operating system is installed</b>	Will scan for hidden files and folders on the drive on which operating system is installed.
<b>Scan all fixed drives</b>	Will scan for hidden files and folders on all the fixed drives of the system.
<b>Alternate Data Streams (ADS)</b>	To scan for suspicious items in Alternate Data Streams of NTFS File system.
<b>Report File Path</b>	Guardian Anti-Rootkit creates a scan report file at the location from which it is executed. You can specify different location by specifying report file path.

### Overview of Alternate Data Streams - ADS

ADS allows data to be stored in hidden files that are linked to a normal visible file. Streams are not limited in size and there can be more than one stream linked to a normal file. The primary reason why ADS is a security risk is because streams are almost completely hidden and represent possibly the closest thing to a perfect hiding spot on a file system - something trojans can and will take advantage of. Streams can easily be created/written to/read from, allowing any trojan or virus author to take advantage of a hidden file area.

## SCANNING RESULTS AND CLEANING ROOTKITS

### Guardian Anti-Rootkit Scanning

1. Start **Guardian Anti-Rootkit**.
2. In the left side of the main window click on **Start Scan**.
3. **Guardian Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process or rename the rootkit Registry entry or Files.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

### Action to be taken on Scan Results

<b>Process</b>	<p>After scanning Guardian Anti-Rootkit will detect and display a list of hidden Processes. You can select process or process for termination, but make sure that list of Processes for termination doesn't include any know trusted process.</p>
<b>Terminating Hidden Process</b>	<p>Guardian Anti-Rootkit also displays summary of process scanning as total number of Processes scanned and number of hidden Processes detected.</p> <p>After selecting list of Processes for termination click on Terminate button. If a process is successfully terminated then its PID (Process Identifier) field will show <b>n/a</b> and process name will be appended by <b>Terminated</b>. All terminated Processes will be renamed after a restart.</p>
<b>Registry</b>	<p>Similar to process scan Guardian Anti-Rootkit will display a list of hidden Registry key's. You can select keys for renaming, but make sure that list of key's for renaming doesn't include any known trusted registry key.</p>
<b>Renaming Hidden Registry Key</b>	<p>Guardian Anti-Rootkit also displays summary of Registry scanning as total number of items scanned and number of hidden items detected.</p> <p>After selecting list of key's for renaming click on Rename button. Renaming operation requires reboot hence Key name will be prefixed by Rename Queued.</p>
<b>Files and Folders</b>	<p>Similar to process and Registry Guardian Anti-Rootkit will display a list of hidden Files and Folders. You can select Files and Folders for renaming, but make sure that list of Files and Folders for renaming doesn't include any know trusted file.</p>
<b>Renaming Hidden Files and Folders</b>	<p>Guardian Anti-Rootkit also displays list of executable Alternate Data Streams.</p> <p>Guardian Anti-Rootkit also displays summary of File scanning as total number of files scanned and number of hidden files detected.</p> <p>After selecting list of Files and Folders for renaming click on Rename button. Renaming operation requires reboot hence Files and Folders name will be prefixed by Rename Queued.</p>

## CLEANING ROOTKITS THROUGH GUARDIAN EMERGENCY CD

In some cases it may happen that rootkits are not being cleaned. They are reappearing during Guardian Anti-Rootkit scan. In such case you can also use Guardian AntiVirus Emergency CD for proper cleaning. All you have to do is create a Guardian Emergency CD and boot your system through it. To create a Guardian Emergency CD and clean your system through it, please follow the below given steps:

### Steps 1

#### To create an Emergency CD

To create Guardian Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003 or above)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

#### Creating Emergency CD:

1. Start **Guardian AntiVirus**.
2. Click on **Tools** from the left pane.
3. Click on **Emergency CD**.
4. Click **Next**.
5. Select **Create Emergency CD**, click **Next**.
6. Bootable files required to make the CD bootable. Select **Operating System Installation CD** option and insert the Operating CD (Windows XP and Windows 2003 operating system CD only). Select the CD-Rom drive.
7. Click **Next**.
8. System files will be fetched from the installation CD.
9. Remove the Operating System Installation CD and insert a blank writable CD.
10. Select the CD-Rom drive.
11. Click **Next**.
12. Emergency CD will be created.

### Steps 2

1. Start **Guardian Anti-Rootkit**.
2. In the left side of the main window click on **Start Scan**.
3. **Guardian Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit process or rename the rootkit registry entry or files.

### Steps 3

1. Boot your system using Guardian Emergency CD.
2. Guardian Emergency CD will automatically scan and clean the rootkits from your system during native scan.

## CUSTOMIZING GUARDIAN ANTI-VIRUS

Guardian AntiVirus is provided with various options for customizing. You can easily configure Guardian AntiVirus as per your requirements. By default, Guardian AntiVirus is configured to provide the ideal protection for most of the computing environments.



We recommend you not to change the preset options unless they are specifically required.

### To configure options

All the options related to the customization are available under **Options**, in the main window menu of Guardian AntiVirus. To configure the options do following:

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of the Guardian AntiVirus.

### To restore default settings of Guardian

You can change any or all of the options provided under the **Options** tab. Also, you can restore the default settings at any point of time.

<b>To restore default settings on the Options page</b>	On the page for which you want to restore default settings, click Default.
<b>To restore default settings for all options</b>	On any page in the Options window, click Default All.

## SCANNER - SCAN OPTIONS

The Scanner settings will affect the scanning during manual scans. Scanner primarily contains the following options:

### What items to scan?

You can specify which files to scan by specifying their extensions. By default, Guardian AntiVirus scans for the executable extensions. Scanning executable files is adequate in most of the situations as viruses only infect and spread from these types of files.

<b>Executable Files</b>	<p>It covers the most common executable extensions. Guardian AntiVirus looks at the file and finds if it contains executable code or not and scans only the files having executable codes.</p>
<b>All files</b>	<p>It scans for all the files irrespective of whether it contains executable code or not. This reduces the scanning speed and hence is recommended only after a virus attack is discovered.</p>
<b>User Specified Extensions</b>	<p>This choice allows you to specify extensions of the files to be scanned. On selecting this option you can enter the executable file extensions of your choice. From the next scan, the scanner will scan all the files with these extensions.</p> <p><b>Customizing User Specified Extensions</b></p> <ol style="list-style-type: none"><li>1. Select <b>User Specified Extensions</b></li><li>2. Press <b>Customize</b> button.</li><li>3. The default list includes most of the program file extensions. In case some of your applications use some other extensions, add them to this list to include it for scanning.</li></ol> <p><b>To add an extension</b></p> <ol style="list-style-type: none"><li>1. Feed the extension <b>Add</b> box.</li><li>2. Click <b>Add</b>.</li></ol> <p><b>To remove a program file extension</b></p> <ol style="list-style-type: none"><li>1. Select the file extensions in the <b>User Defined Extensions</b> list box.</li><li>2. Click <b>Delete</b>.</li></ol> <p>To reintroduce the original list, click <b>Default</b>.</p>

## How to respond when a virus is found

This option allows the user to configure following activities when a virus is found during a scan:

<b>Repair Automatically, Delete if unsuccessful</b>	During a scan if a virus is found, then it will repair the virus without any interaction with you. If the file cannot be repaired it will be automatically deleted from your computer. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware then Guardian AntiVirus automatically deletes the file.
<b>Repair Automatically, Quarantine if unsuccessful</b>	During a scan if a virus is found, then it will repair the file or automatically quarantine it, if it cannot be repaired. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware then Guardian AntiVirus automatically deletes the file.
<b>Delete Automatically</b>	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. Files deleted in such a manner cannot be recovered.
<b>Prompt</b>	<p>Informs you when a virus is found and allows you to choose how to respond. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. Herein following options are provided, to act upon the infected file:</p> <ul style="list-style-type: none"><li>• Repair, delete if unsuccessful</li><li>• Repair, quarantine if unsuccessful</li><li>• Skip</li><li>• Delete</li><li>• Quarantine</li></ul>
<b>Report Only</b>	<p><b>Apply action to all:</b> This option automates the action for all the infections found during the same scan.</p> <p>In this mode the scanner scans for viruses, skips them, when the scan is over a summary window (report) appears providing all the scan details.</p>
<b>Backup before repairing</b>	Scanner will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

## Using Advanced Options while scanning

The Advanced options determine how to perform a scan. You can set following options as per your requirements:

<b>Scan Archive Files</b>	When this option is selected Guardian AntiVirus scans files inside the archive files. Guardian AntiVirus can scan archive files like ARJ, CAB, CHM, GZ, MSEXPAND, RAR, SIS, TAR, TNEF and ZIP. Scanning inside compressed files increases scanning time. Guardian AntiVirus can detect viruses inside the compressed file; however it cannot remove the virus from these files. You are advised to decompress such files, remove the viruses from them and compress the same again. This will ensure that the compressed copy is also virus free.
<b>Scan Packed files</b>	When this option is selected Guardian AntiVirus scans packed executable files (.exe's) packed by popular packages like COM2EXE and LZEX.
<b>Show Packed/Archive info</b>	This feature provides packed and archive information in the scan report about packed files and archive scanned files during the scan.
<b>DNAScan</b>	DNAScan technology is used to detect new and unknown malicious threats.
<b>List files while scanning</b>	All files will be listed in the Report section during scanning along with their status i.e. Clean or Infected.
<b>Scan Mailboxes</b>	Guardian AntiVirus can scan Outlook Express 5.x Mail Box (inside .DBX files). Viruses like KAK, JS.Flea.B etc. remain inside DBX files and can reappear from there, if patches are not applied for OE. It also scans for email attachments with Outlook Express 5.0. It scans email attachments encoded with UUENCODE/MIME/BinHex (Base 64).  <b>Quick Scan</b> : If this option is selected then Guardian scans new mails and does not scan previously scanned emails. By default this option is selected.  <b>Thorough Scan</b> : If this option is selected then Guardian always scans all mails every time. This scan takes a long time.

## Configuring Archive Settings

Archive scan settings are different from the normal scan. You can set which archives to be scanned and action to be taken if a virus is found in an archive. This option allows the user to configure following activities when a virus is found during scan:

<b>Delete Automatically</b>	Deletes an archive containing virus-infected file without notifying you.
<b>Prompt</b>	<p>Informs you when a virus is found in an archive and allows you to choose how to respond. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. It provides you with the following options for an infected file:</p> <ul style="list-style-type: none"><li>• Skip</li><li>• Delete</li><li>• Quarantine</li></ul> <p><b>Apply action to all:</b> This option automates the action for all the infections found during the same scan.</p>
<b>Report Only</b>	In this mode the scanner scans for viruses under archive, skips the virus and archive file without taking any action.
<b>Quarantine</b>	During scan if a virus is found in an archive file, then the archive will be moved to Quarantine.
<b>Archive Scan level</b>	Set the level to scan inside an archive. By default it is set to level 2. Increasing the default Archive Scan Level may affect the scanning speed.

## SCANNER – MEMORY SCAN

Guardian AntiVirus scans the system memory every time it is started. It ensures that any infectious object is not running in the memory. Guardian AntiVirus Memory scan is smart enough to scan executable processes and additionally their supporting dynamic link libraries (.DLL).

### Memory scanning mode

<b>Quick Scan</b>	Scans memory for running executable processes only.
<b>Thorough Scan</b>	Scans memory for running executable processes along with their supporting dynamic link libraries. This scan will take considerable time.
<b>DNAScan</b>	This feature scans for new malicious threats in the memory using Quick Heal's indigenous DNAScan technology. When a new threat is found running in the memory it will clean the same. You will also have the option to send the suspicious file to our research lab for further analysis of that file. If that file is behaving like a malware then it will be added in the known threat signature database.

## SCANNER – DNASCAN

### Objective

DNAScan is Quick Heal's indigenous technology to detect and eliminate new and unknown malicious threats in the system. Additionally it copies the suspected file in the Quarantine directory before taking any action. Quarantined suspicious files can be submitted to our research lab for further analysis. This submission is important to curb the wild spread of new malicious threats. Suspicious file submission ensures the detailed analysis of the file in our research lab. After the detailed analysis it can be added in the known threat signature database which will be provided in updates to all the users. This can be only possible if they are detected and eliminated before their wild spread. DNAScan technology successfully traps suspected files with very less false alarms.


### Process

Whenever DNAScan detects a new malicious threat in your system it informs you, or asks for your action during memory scanning if the scanning is set with Prompt settings. One copy of DNAScan suspected files will always be quarantined which can later be submitted to research lab for further detailed analysis. The submission can be done automatically or manually through email. The submission takes place whenever Guardian AntiVirus updates itself and finds new DNAScan suspected files in the Quarantine folder. It sends new DNAScan suspicious quarantined files in an encrypted file format to Guardian research lab.

## Setting the submission settings

DNAScan suspected files can be submitted to research lab of Guardian through email. Submission of the suspected files is at your liberty. Submission of the DNAScan suspected files depend on the below mentioned settings:

<b>Do not submit files</b>	This option does not let DNAScan submit the suspected files to Guardian research lab.
<b>Submit suspicious files</b>	<p>DNAScan suspected files can be submitted to Guardian research lab.</p> <p>If <b>Show notification while submitting the files</b> option is checked, then Guardian prompts for permission before submission of samples to Guardian Research Lab.</p> <p>If <b>Show notification while submitting the files</b> option is not checked, then Guardian submits the suspicious files without notifying you.</p>

 Manual submission can be done through the Quarantine tool.

## SCANNER — REGISTRY RESTORE

The Registry is a database used to store settings and options of Microsoft Windows Operating Systems. It contains information and settings for all the hardware, software, users, and preferences of the system. Whenever a user makes changes to a Control Panel settings, or File Associations, System Policies, or installed new software, the changes are reflected and stored in the Registry. Malwares usually target the system Registry to restrict specific features of the Operating Systems or other applications. They may modify the system registry so that it behaves according to the benefit for their activities. Most of the time it creates problem for the system.

**Guardian Registry Restore** - restores the critical system registry area and other areas for the changes made by malwares and repair the system registry.

### Registry Restore settings

<b>Critical System Registry Restore</b>	Selecting this option allows Guardian AntiVirus to restore the critical system registry during scan. Critical System Registry areas are generally changed by malwares to perform certain task automatically or to avoid detection or modification by system applications. e.g. Disabling Task Manager, Disabling Registry Editor etc.
<b>Repair malicious registry entries</b>	Selecting this option allows Guardian AntiVirus to scan system registry for malware related entries. Malwares and their remnants will be repaired automatically during scan.

## PROTECTION — ONLINE PROTECTION

Guardian AntiVirus Online Protection continuously scans the system and prevents virus infection from Email Attachments, Internet Downloads, Network, File Execution and Copying.

### To Customize Online Protection

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of the Guardian AntiVirus.
3. Select **Online Protection** under Protection tab.

### General Settings

<b>Load Online Protection at Windows Startup</b>	By default this option is enabled and starts protecting your system, right from the time it is started.
<b>Display Alert Message</b>	Alert message will be displayed whenever a virus is found.
<b>DNAScan</b>	This feature detects and eliminates new malicious threats and protects your system from the latest threats. When a new malicious threat is detected it will be quarantined. You will also have the option to restore the file back to the same location if you are sure that the file is not a malicious threat.

### Specifying which files to scan Online

<b>Executable Files</b>	Scans files that are most likely to get infected by a virus.
<b>User Specified Extensions</b>	<p>This choice allows you to specify extensions of the files to be scanned. On selecting this option you can enter the executable file extensions of your choice. From the next scan, the scanner will scan all the files with these extensions.</p> <p><b>Customizing User Specified Extensions</b></p> <ol style="list-style-type: none"><li>1. Select <b>User Specified Extensions</b>.</li><li>2. Press <b>Customize</b> button.</li><li>3. The default list includes most of the program file extensions. In case some of your applications use some other extensions, add them to this list to include it for scanning.</li></ol> <p><b>To add an extension</b></p> <ol style="list-style-type: none"><li>1. Feed the extension in <b>Add</b> box.</li><li>2. Click <b>Add</b>.</li></ol> <p><b>To remove a program file extension</b></p> <ol style="list-style-type: none"><li>1. Select the file extensions in the <b>User Defined Extensions</b> list box.</li><li>2. Click <b>Delete</b>.</li></ol> <p>To reintroduce the original list, click <b>Default</b>.</p>

## How to respond when a virus is found

<b>Deny Access</b>	Prevents you from using a virus-infected file.
<b>Repair Automatically, delete if unsuccessful</b>	Attempts to repair the file from virus infection, in case if the file cannot be repaired, it will be deleted.
<b>Delete Automatically</b>	Deletes a virus-infected file without notifying you. Files deleted in such a manner cannot be recovered.
<b>Repair Automatically, Quarantine if unsuccessful</b>	Attempts to repair the file and quarantines it automatically in case if it cannot be repaired.
<b>Backup before repairing</b>	Online Protection will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

## Floppy Activities

<b>Check Floppy for Boot viruses on Access</b>	Boot sector of floppy will be scanned whenever a floppy is accessed.
<b>Check Floppy for Boot viruses during Shutdown</b>	Boot sector of floppy will be scanned if a floppy exists in the floppy drive during shutdown.

## PROTECTION - EMAIL PROTECTION

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of the Guardian AntiVirus.
3. Select **Email Protection** under Protection tab.

### General Settings

<b>Enable Protection</b> <b>Display Alert Message</b>	<p>This option enables scanning of emails while downloading.</p> <p>Virus found alert will be shown in case a virus is found in an email or attachment. Display Alert Message will contain following information:</p> <ul style="list-style-type: none"><li>• Virus Name</li><li>• Sender Email Address</li><li>• Recipient Email Address</li><li>• Email Subject</li><li>• Attachment Name</li><li>• Action Taken</li></ul>
--	--

### How to respond when a virus is found

You can specify how to respond when a virus is found in an email attachment. You will get a prompt from Guardian Email protection about the action taken if the Display Alert option is enabled. Action taken details are also logged into the Activity Log.

<b>Delete infected attachments</b> <b>Repair automatically, Delete if unsuccessful</b> <b>Backup before repairing</b>	<p>Selecting this option will delete the infected attachment while downloading mails.</p> <p>Attempts to repair the virus without interacting with you. If the attachment cannot be repaired then it will be deleted.</p> <p>Email Protection will keep a copy of infected email before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)</p>
---	--

## Control attachments to your incoming email

<b>Block attachments with multiple extensions</b>	Worms commonly use multiple extensions. Enabling this option will block multiple extension attachments in incoming emails. It prevents infection from new worms, and thus protects your system. Common multiple extensions are .exe, .scr, .mpg, etc.
<b>Block emails crafted to exploit vulnerability</b>	Enabling this option will block emails, which contain vulnerability like MIME, IFRAME, etc. Sending an email into broken parts is known as partial mail. Microsoft Outlook Express and Microsoft Outlook have an option of breaking message into separate parts.

### Enable Attachment Control – Enable attachment blocking in incoming email.

<b>All attachments</b>	Selecting this option will delete all the attachments in incoming emails. This option is only recommended for users who require high security or prefer text based emails only.
<b>User specified extensions</b>	<p>This choice allows you to specify extensions of the files (attachments) to be blocked. On selecting this option you can either use provided default extension list or enter the file extensions of your choice.</p> <p>To add your own extension follow the below given steps:</p> <ol style="list-style-type: none"><li>1. Select <b>User specified extensions</b>.</li><li>2. Press <b>Customize</b>.</li><li>3. Type the extension name. For example: 'mpg'.</li><li>4. Click <b>Add</b> to add the extension in the list.</li><li>5. Click <b>Ok</b> to save the settings.</li></ol>

## Prevent new worm infection filtering email clients

<b>Email clients allowed to send mails</b>	<p>Guardian Email protection is by default configured to support most of the popularly used email clients like Eudora. If your email client is different from the ones provided in the list, then you can simply add the same in the trusted email client list. To add email client, perform the following steps:</p> <ol style="list-style-type: none"><li>1. Select <b>Enable trusted email clients</b>.</li><li>2. Press <b>Configure</b> button.</li><li>3. Click <b>Add</b> to add the email client into trusted email client list.</li><li>4. Click <b>Ok</b> to save the changes.</li><li>5. Press <b>Default</b> to load the default email client list.</li></ol>
--	---

## PROTECTION — PACKER IDENTIFICATION

Packers are files that pack together many files, or compress a single file to reduce file size. These files do not need a third party application to get unpacked. They have an inbuilt functionality of packing and unpacking. Packers can also be used as tools to spread malware by packing a malicious file amidst a set of files. There are certain packers that are used specifically to spread malicious files. These packers, when unpacked can cause harm to your PC. By default Guardian Packer Identification scans the system for a select list of highly suspicious packers and alerts you if such a packer is found.

You can also customize the list of packers that Guardian Packer Identification can scan. To include additional packers in the scan please customize the Packer Identification by performing the following steps:

1. Start **Guardian AntiVirus**.
2. Click **Options** under main windows menu of the Guardian AntiVirus.
3. Double click **Protection** to collapse the Protection menu.
4. Select **Packer Identification**.

### General Settings

<b>Identify packed files</b>	Check this feature to identify packer files during the scan. You can customize the list of packers to be detected by clicking the <b>Customize</b> button. For novice users we recommend not to change the settings as the default settings will provide optimum safety.
------------------------------	--

### How to respond when a packer is found

<b>Action for scanner</b>	Select the action that the scanner needs to take when a suspicious packer is detected while scanning. The following actions can be performed when the scanner detects a suspicious packer file: <ul style="list-style-type: none"><li>• <b>Report only:</b> Leaves the infected packer as it is and generates a report of the infections detected.</li><li>• <b>Quarantine:</b> The infected packer will be moved to the quarantine folder.</li></ul>
<b>Action for scanner in case of archive files</b>	Select the action that the scanner needs to take if an archive is found while scanning. The following actions can be performed by the scanner: <ul style="list-style-type: none"><li>• <b>Report only:</b> Leaves the infected archive file as it is and generates a report of the infections detected.</li><li>• <b>Quarantine:</b> The infected archive file will be moved to the quarantine folder.</li></ul>
<b>Action for Online Protection</b>	The following actions can be performed when Online Protection detects a suspicious packer file: <ul style="list-style-type: none"><li>• <b>Deny access:</b> Completely blocks access to the infected packer.</li><li>• <b>Quarantine:</b> The infected packer file will be moved to the quarantine folder.</li></ul>

## UPDATES - AUTOMATIC UPDATES

1. Start **Guardian AntiVirus**.
2. Click **Option**, under the top menu of Guardian AntiVirus.
3. Select **Automatic Update** under Updates tab.

### General Settings

<b>Enable Automatic Update</b>	Automates the Guardian AntiVirus update process.
<b>Silent Update</b>	Enabling this option sets Guardian AntiVirus to update in non-interactive mode.
<b>Show Update Notification</b>	This option lets Guardian AntiVirus show the update notification after the successful updates.

### Select the updating mode

<b>Download from Internet Centre</b>	Download and update through Internet.
<b>Pick from specified path</b>	Download and update through local or network folder.

### Backup update files

<b>Keep a backup of update files</b>	This option allows saving the definition files while updating through Internet. Saved definition files can be used to deploy the updates to all other computers within a network.
--------------------------------------	---

## UPDATES - MESSENGER

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of Guardian AntiVirus.
3. Select **Messenger** under Updates tab.

### General Settings

<b>Enable Messenger</b>	This option enables Guardian AntiVirus Messenger service which provides important information about latest threats, updates and other information related to Guardian AntiVirus.
<b>Show Messenger icon in system tray</b>	This option shows Guardian AntiVirus Messenger icon in the system tray. If this option is unchecked then the Guardian AntiVirus Messenger icon will not be visible in the system tray but you will still receive messages and notifications.

### Select the mode to get message

<b>Download from Internet Centre</b>	Download and notify the messages through Internet.
<b>Pick from specified path</b>	Download and notify the messages through local or network folder.

## Keep a backup of message

<b>Keep a backup of message</b>	This option allows saving the message while notifying through Internet. Saved message can be used to deploy the notification message to all other computers within a network.
<b>Delete messages if older then</b>	You can delete message at scheduled intervals or just after viewing. To manage messages: <ol style="list-style-type: none"><li>1. Select <b>Delete messages if older then</b>.</li><li>2. Choose the desired intervals for deleting the viewed messages.</li><li>3. Press <b>Ok</b> to save the changes.</li></ol>

## GETTING MESSAGES FROM LOCAL FOLDER OR NETWORK PATH

Guardian AntiVirus Messenger can be configured to gather messages from a Local Folder or the Network Path. This feature enables Guardian AntiVirus Messenger's full functioning on systems where Internet connection is not available but systems are connected to LAN.

To get messages from local folder/network path please follow the below given steps:

1. Take a system, which is connected, to the Internet. This system will download messages from Guardian Internet centre.
2. Create a folder on that system. For example: **C:\QHMSGR**
3. Share this folder with Read access rights on the network.
4. Now click **Start -> Programs -> Guardian AntiVirus -> Guardian AntiVirus**.
5. Click **Options**.
6. Select **Messenger** from the Updates tab.
7. Select **Keep a backup of message**.
8. Specify the folder where you want to keep a backup of messages. For example: **C:\QHMSGR**
9. Click **OK** to save the changes.
10. On workstations go to **Messenger** settings under Updates option tree.
11. Select **Pick from specified path** and specify the shared backup messages folder path. For example: **\\SERVER\QHMSGR**
12. Click **OK** to save the changes.

## UPDATES - INTERNET SETTINGS

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of Guardian AntiVirus.
3. Select **Internet Settings** under the Updates tab.

Your Internet Connection will be automatically detected. Change the settings only if you have trouble with the default connection settings.

### Enabling and configuring proxy settings

If you are "using a proxy server on your network" or "using Socks Version 4 & 5 network" then you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Connection settings. Username & password are mandatory for the logon credential. Following Guardian modules require these changes:

- **Registration Wizard**
- **Quick Update**
- **Messenger**

### To enable and configure HTTP proxy settings

1. On the Internet Settings, select **Enable proxy settings**.
2. Choose **HTTP Proxy**, **Socks V 4** or **SOCKS V 5** as per your settings and then do the following:
  - In **Server**, type IP address of the proxy server or domain name (For example: proxy.yourcompany.com).
  - In **Port**, type the port number of the proxy server (For example: 80).
  - In **User name** and **Password**, type your server logon credentials, when required.
3. Click **OK** to save the settings.

## MISCELLANEOUS - EXCLUSIONS

You can configure Guardian AntiVirus to skip scanning of certain files or folders. Scanning can be excluded in both cases, of known virus detection as well as DNAScan.

### Following scanning modules can be excluded

- Scanner
- Online Protection
- Memory Scanner
- DNAScan

### To exclude Files or Folders from scanning

1. Start **Guardian AntiVirus**.
2. Click **Options**, under the top menu of Guardian AntiVirus.
3. Select **Exclusion** under the Miscellaneous tab.
4. Click **New**.
5. Click File Icon or Folder icon for the exclusion.
6. Select the options of **Exclude** from.
7. Click **OK** to complete the process.

For selecting **Exclude from** follow these guidelines:

- If you are getting a warning for a known virus in a clean file and Guardian AntiVirus still gives you warning, you can exclude it for scanning of **Known Virus Detection**.
- If you are getting a DNAScan warning in a clean file, you can exclude it for scanning of **DNAScan**.

## MISCELLANEOUS - GENERAL

### Quickly scan system at Windows startup

<b>Enable Startup Scan</b>	This option lets Guardian AntiVirus to scan the starting area of the system from wherein the programs are trying to get automatic execution control to trap new and unknown virus. It also keeps a watch on some of the system files, which are commonly patched (or replaced) by certain worms/backdoors/trojans.
----------------------------	--



This feature is not supported on Windows Vista and above Operating system.

### Get the status of a file by checking its Property

<b>Enable Property Sheet Scanner</b>	This option registers Guardian AntiVirus Scan tab in every file's properties tab. It provides information about the file status (Clean or Infected). You will also get the Guardian AntiVirus version and virus database information here.
--------------------------------------	--

## Schedule for deleting Reports and Quarantine file

<b>Delete Reports after</b>	You can delete the reports of Guardian AntiVirus at specific intervals.
<b>Delete Quarantine/Backup files after</b>	You can delete the quarantine files (including backup of the infected files) at specific intervals.

## Prevent unauthorized access to option settings of Guardian

To protect Guardian AntiVirus options from being changed without your permission, you can choose to protect it by enabling password protection for the same. If you specify a password, you are asked to enter a password every time when you wish to view or change the Options.

<b>Enable password protection</b>	<b>To specify a password:</b> <ol style="list-style-type: none"><li>1. At the top of the main window, click <b>Options</b>.</li><li>2. In the Options window, under the Miscellaneous tab, click <b>General</b>.</li><li>3. Select <b>Enable password protection</b> and press <b>Change Password</b>.</li><li>4. In the password dialog box, type a password.</li><li>5. Click <b>OK</b>.</li></ol>
-----------------------------------	--

## Application Status

<b>Show application icon at system tray</b>	If this option is enabled, Guardian AntiVirus icon will be visible at the system tray. User can easily access Guardian AntiVirus from this icon directly.
---	---

## Scan removable devices

<b>Scan removable device when plugged into the system</b>	<p>If this option is enabled, then Guardian will prompt you to perform a scan of removable device except CDs or DVDs. The user has two options:</p> <ul style="list-style-type: none"><li>• Scan files on root of drive only</li><li>• Scan full drive</li></ul> <p>Select the necessary option and click <b>Scan</b> button. We recommend that you scan any USB removable storage devices before using it, but if you wish to use the device without scanning it first, then click <b>Do Not Scan</b> button to exit from the scanner prompt.</p>
---	--

## Self Protection

<b>Start Self Protection at Windows Startup</b>	If this option is enabled, then Guardian AntiVirus will protect itself by safeguarding Guardian files, folders, configurations and registry entries against malwares and also against tamper from other applications.
---	---

## CLEANING VIRUSES

Guardian warns you for a virus infection when:

- A virus is encountered during a manual or scheduled scan.
- A virus is encountered in the memory.
- A virus is encountered by Guardian AntiVirus Online Protection/Email Protection.
- A virus is detected through Start-up Scan.

## CLEANING VIRUSES ENCOUNTERED DURING SCANS

Guardian AntiVirus is adequately configured with the default installation to protect your system. If a virus is detected during scanning with default settings, Guardian AntiVirus tries to repair the virus and if it fails in doing so, it will delete the file. If you have changed the default scanner settings, then action will be taken accordingly when a virus is found. See [How to respond when a virus is found](#).

### Scanning Options

During scanning you are provided with the following options for your ease of operation:

<b>Statistics</b>	View statistics of a scan provided under this section.
<b>Skip Folder</b>	During the scan if you want to avoid scanning the current folder, just press on Skip folder. Scanning will be moved to other location. This option can be used while scanning a folder which contains non-suspicious items.
<b>Skip File</b>	During the scan if you want to avoid scanning the current file, just press on Skip file. Scanning of the current file will be skipped. This option can be used while scanning a big archive of files.
<b>Stop</b>	To stop the scanning process.
<b>Close</b>	To stop and terminate the scanning process.
<b>Shut down PC when finished</b>	Check this option when you to shut down your system after finishing the scan. This feature will work only if the scanning is completed.

<b>Reports</b>	During the scan you can also check the reports of the scan simultaneously. While scanning just press Reports window tab. By default setting, reports will be having infection event only. If you want to have the list of entire scan including clean files, select List files while scanning in the Scanner's option page.
<b>Settings</b>	You can check the settings used during the scan. To view these settings, just press Settings window tab.

## CLEANING VIRUS ENCOUNTERED IN MEMORY

"Virus Active in memory" means that virus is active, spreading to other files, computer (if connected to network) and doing malicious activity as per its payload. When Guardian AntiVirus detects a virus in memory, it warns in the following manner:

You can schedule Native Scanning of your PC at next boot which will scan and clean all drives including NTFS partitions at boot time before desktop is completely loaded. This will help you in detecting and cleaning even the most cunning Rootkits, spywares, special purpose Trojans and loggers. After disinfection restart your system and continue with installation. See [Performing Native Boot Scan](#) for more detail.

## CLEANING BACKDOOR, TROJAN, WORM AND MALWARES ENCOUNTERED IN MEMORY

During memory scanning if backdoor, trojan, worm, and other malwares are found, then Guardian AntiVirus will try to disable them and will ask you to scan the system for complete disinfection.

### Restart required during cleaning for some malwares

Some malwares drop and inject their dynamic link libraries into system's running processes such as explorer.exe, Iexplorer.exe, svchost.exe, etc. which cannot be disabled or cleaned. During memory scan when they will be detected, they will be set for deletion in the next boot automatically. Guardian AntiVirus memory scan will provide complete detail or action recommendation for you in such cases.

### Cleaning of Boot/Partition viruses

In case if Guardian AntiVirus memory scanner detects a boot or partition virus in your system then it will recommend you to boot your system using a clean bootable disk and scan it using Guardian Emergency disk to clean the virus. See [Using Emergency disk](#) for more details.

### Responding to virus found alerts from Online Protection

Guardian AntiVirus Online Protection continuously scans your system for viruses in the background as you work. By default, Online Protection repairs the infected files automatically. You will also get a prompt after the action is taken by Guardian AntiVirus Online protection.

## USING EMERGENCY CD AND COMMAND LINE SCANNER

Guardian AntiVirus Emergency CD, - create your own emergency bootable CD that will help you to clean boot your Windows PC and scan and clean all the drives including NTFS partitions. This helps in cleaning badly infected PC from file infecting viruses which cannot be cleaned from inside windows.

If your computer is badly infected by a virus in such a case while installing Guardian AntiVirus, Pre-install scan of Guardian AntiVirus installer will detect the active virus resident in memory. Hence you are unable to proceed with Guardian AntiVirus Installation. You are required to remove the virus from memory and other critical system areas before proceeding with Guardian AntiVirus Installation. To create Guardian AntiVirus Emergency CD, your system should fulfill following requirements:

- Licensed copy of Microsoft Windows Operating System. (Windows 2000/XP/2003 or above).
- Microsoft Windows Installation CD. (Windows XP/2003 or above)
- A blank writable CD and a CD-Writer drive.
- Emergency CD can only be used to scan and clean drives of the same system for which you have licensed Microsoft Windows operating system.

### How to make Emergency CD

Emergency CD and Command line scanner can be created using installed Guardian AntiVirus software. See [Creating Emergency CD or Command line scanner](#).

## USING EMERGENCY CD

1. Insert **Emergency CD** into your CD-Rom/DVD-Rom drive.
2. Restart your system.
3. Emergency CD will be automatically start and starts scanning all the drives. It will automatically disinfect the infection if found.
4. Once the scanning is over remove the Emergency CD from CD-Rom/DVD-Rom drive.
5. Restart your system.

## USING COMMAND LINE SCANNER

Command line Scanner is executed using EMGSCAN.EXE command at the DOS command prompt. EMGSCAN.EXE usage is:

```
Emgscan.exe [drive/path] [options]
```

## Emgscan Options

For specified options '-' inverts the default meaning.

<b>/DELETE</b>	Delete infected files.
<b>/REPAIR</b>	Disinfect whenever possible.
<b>/DUMB</b>	Do a "dumb" scan of all files.
<b>/WARE</b>	Scan for Adware/Spyware.
<b>/MIME</b>	Scan for .eml files.
<b>/HELP or /?</b>	Display this help.
<b>/LIST</b>	List all files checked.
<b>/NOSUB</b>	Do not scan subdirectories.
<b>/ARCHIVE[-]</b>	Scan inside archive files.
<b>/PACKED[-]</b>	Unpack compressed executables.
<b>/REPORT=FileName</b>	Create a report file.
<b>/TEMPDIR=DirPath</b>	Temporary Directory name.

### To remove viruses using Emergency Disk:

1. Shutdown your computer.
2. Switch on the computer.
3. Insert Windows 95/98 Startup Disk or a clean DOS bootable disk. This will boot your system in A:\ Dos Shell.
4. Insert the Guardian Emergency disk.
5. Type **EMGSCAN C: /REPAIR** at the DOS command prompt and press **Enter**.
6. Guardian will scan entire C drive of your system and will try to disinfect the boot sectors or files if found infected during the scan.
7. When Guardian removes all the viruses and completes the scan, it will provide you with the respective scan summary.

## UPDATING GUARDIAN ANTI-VIRUS

Updates for Guardian AntiVirus are posted regularly on its website containing detection and removal of newly discovered viruses. To prevent newly discovered viruses from infecting your computer, your system should have latest updated copy of Guardian AntiVirus. By default Guardian AntiVirus is set to update automatically from the Internet. This is done without user's intervention. Only basic requirement in this case, is the availability of a valid Internet connection for availing automatic updates. Automatic updates can also be applied from local or network path, but that path should have the latest set of definitions.

### Some important facts about Guardian AntiVirus Updates

- All Guardian AntiVirus Updates are complete updates including Definition File Update and Engine Updates.
- All Guardian AntiVirus updates also provide you version up gradation, thus making available the new features and technology for your protection.
- Guardian Quick Update is a single step upgrade.

## UPDATING GUARDIAN ANTI-VIRUS FROM INTERNET

Quick Update by default automatically updates your copy of Guardian AntiVirus through the Internet. For this, you only need to have a valid Internet Connection. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.)

To update Guardian AntiVirus manually through Internet

1. Click **Start -> Programs -> Guardian AntiVirus -> Quick Update.**
2. Follow the instructions and click **Next** button.
3. Check **Download from Guardian Internet Centre.**
4. Ensure that the Internet connection is active, and then click **Next** to initiate the update procedure.
5. Quick Update connects to the Guardian site, downloads the appropriate upgrade files for your copy of Guardian, and applies it thereafter to your copy, thus updating it to the latest available update file.

## UPDATING GUARDIAN ANTI-VIRUS WITH DEFINITION FILES

If you already have the upgraded definition file with you, you can upgrade Guardian AntiVirus without connecting to the Internet. It is specifically useful for Network environments with more than one PC. You are not required to download the upgrade file from the internet on all the PCs within the network using Guardian.

To update Guardian AntiVirus through definition file:

1. Click **Start -> Programs -> Guardian AntiVirus -> Quick Update.**
2. Follow the instructions and click Next button.
3. Click **Pick from specified path.**
4. Click **File** to locate the definition file.
5. Provide the index file for the definition i.e. Index.dat.
6. Click **Next.**

Quick Update picks up the definition file from the designated path, verifies its applicability on the installed version and upgrades your copy of Guardian AntiVirus accordingly.

## UPDATE GUIDELINES FOR NETWORK ENVIRONMENT

Guardian AntiVirus can be configured to provide hassle free updates across the network. You are suggested to follow these guidelines for best results:

1. Setup one computer (may be the server) as the master update machine. Suppose server name is **SERVER**.
2. Configure Guardian AntiVirus on this computer to upgrade automatically from the Internet as per your desired schedule.
3. Make **QHUPD** folder in any location. For example: **C:\QHUPD**
4. Assign Read-Only sharing rights to this folder.
5. Start Guardian AntiVirus and press the **Option** button.
6. Go to **Automatic Update** page under Updates section.
7. Select **Keep a backup of definition files**.
8. Click **Folder** and locate the **QHUPD** folder. Click **Open**.
9. Click **OK** to save this setting.
10. On all user computers within the network launch **Guardian AntiVirus**.
11. Go to **Automatic Update** page under Updates section.
12. Select **Pick from Specified path**.
13. Click **Folder**.
14. Locate the **SERVER\QHUPD** folder from Network Neighborhood. Alternatively you can type the path as **\\SERVER\QHUPD**.
15. Click **OK** to save the settings.

With the above steps all the machines will be upgraded automatically without user intervention at all. Following the steps as mentioned below can further extend the functionality:

1. In case of major out breaks, Guardian AntiVirus also provides intermediate upgrades. Messenger flashes the notice about the same, on your machine.
2. On receipt of the message, circulate a network notice requesting other Guardian AntiVirus users to click on **Update Now** button by right clicking on Guardian AntiVirus icon in the system tray.

## TECHNICAL SUPPORT

### When is the best time to call?

Guardian AntiVirus provides technical support between 9:30 AM to 6:30 PM (Indian Standard time).

### What should I have ready before calling?

If you call Technical Support and have the necessary information on hand we will be able to help you more efficiently.

- Your Product key which is included in the boxed version of the products. If you have purchased our products on-line then you will find the Product key in the mail confirming your order.
- Information about your computer: brand, processor type, RAM capacity, the size of your hard drive and free space on it, as well as information about other peripherals.
- Your operating system: name, version number, language.
- What is the version of installed anti-virus and what is the virus database.
- What software is installed on your computer?
- Is your computer connected to a network? If yes — contact your system administrators first. If they can't solve your problem they should contact technical support themselves.
- Details: when did the problem first appear? What had you been doing before the problem appeared?

### What should I say to the technical support personnel?

Please be as specific as possible and provide maximum details. Remember that the specialist is basing on the information that you provide.



Very often this information allows us to resolve your problem quickly.

---

#### SUPPORT CENTER

---

Guardian AntiVirus

Tel: +91-253-6576106/07/08

Email: [support@guardianav.co.in](mailto:support@guardianav.co.in)

Web: <http://www.guardianav.co.in>

---

For more information please visit us at <http://www.guardianav.co.in>

---