



# Guardian Total Security

## User Manual

# Copyright & License Information

---

© 1994-2021 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411014.

## Trademarks

Quick Heal and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

## License Terms




Installation and usage of Guardian Total Security is subject to user's unconditional acceptance of the Guardian Total Security end-user license terms and conditions.

To read the license terms, visit <http://www.guardianav.co.in/eula> and check the End-User License Agreement for your product.

# About This Document

---

The following table lists the conventions that we followed to prepare this manual.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it may be a menu title, window title, check box, drop-down menu, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights information related to the topic being discussed.
	This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve a task in an easier way.
	This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

# Contents

---

<b>1. Getting started .....</b>	<b>1</b>
Prerequisites.....	1
System requirements .....	1
<b>How to download, install, and register Guardian Total Security .....</b>	<b>4</b>
Downloading and Installing Guardian Total Security .....	4
Registering Guardian Total Security .....	5
Registering Guardian Total Security online .....	5
Registering Guardian Total Security offline.....	6
Registering Guardian Total Security through SMS .....	7
Post Registration of Guardian Total Security .....	8
<b>2. Reactivation and renewal .....</b>	<b>9</b>
Reactivating Guardian Total Security .....	9
<b>How to renew Guardian Total Security.....</b>	<b>9</b>
Renewing Guardian Total Security online .....	10
Renewing Guardian Total Security offline.....	11
<b>3. Status .....</b>	<b>13</b>
<b>Why you should scan your computer .....</b>	<b>14</b>
Scan options .....	14
Quick Scan .....	14
Full System Scan .....	15
Custom Scan .....	15
Memory Scan.....	16
Boot Time Scan .....	16
<b>4. Protection .....</b>	<b>18</b>
Ransomware Protection.....	19
<b>How you can prevent ransomware attack.....</b>	<b>19</b>
Exclude Files & Folders .....	19
Configuring Exclude Files & Folders .....	20
Virus Protection.....	21
Scan Settings .....	23
<b>Take advantage of automatic scanning of your computer .....</b>	<b>23</b>

---

Scan Settings.....	23
Advance DNAScan .....	27
Block Suspicious Packed Files .....	29
Automatic Rogueware Scan .....	30
Scan Schedule .....	30
Exclude Files & Folders .....	33
Quarantine & Backup .....	35
Exclude File Extensions.....	36
Browsing Protection .....	36
Phishing Protection .....	37
Safe Banking .....	37
<b>Pay bills, transfer money online, and do banking without fear .....</b>	<b>37</b>
Setting Safe Banking .....	38
Launching Safe Banking.....	39
Firewall Protection .....	40
IDS/IPS .....	43
Email Protection .....	44
Email Protection .....	44
Trusted Email Clients Protection .....	46
USB Drive Protection .....	47
External Drive Protection .....	47
Autorun Protection.....	47
Scan External Drives .....	48
Browser Sandbox.....	49
Malware Protection.....	51
Anti Malware .....	52
Launching Guardian AntiMalware.....	52
Anti Rootkit.....	53
Using Guardian Anti-Rootkit.....	53
<b>5. Privacy.....</b>	<b>57</b>
Data Backup.....	57
<b>Take a backup of your data to avoid data loss.....</b>	<b>57</b>
Turning Data Backup on .....	57
Manage Backup .....	59
Restore Backup.....	60

---

Registry Restore .....	60
Data Theft Protection .....	61
<b>Prevent copying of data from your computer to a drive .....</b>	<b>61</b>
Screen Locker Protection .....	62
Anti-Keylogger .....	63
<b>6. Performance .....</b>	<b>64</b>
Auto Silent Mode .....	64
Track Cleaner .....	65
Hijack Restore .....	65
System Explorer .....	67
Using System Explorer .....	67
<b>7. Settings .....</b>	<b>68</b>
<b>Configure these settings to ensure enhanced security .....</b>	<b>68</b>
Automatic Update .....	68
View Quarantine Files .....	70
Report Settings .....	71
Report Virus Statistics .....	72
Restore Default Settings .....	72
Password Protection .....	72
Security Updates .....	73
Internet Settings .....	74
Self Protection .....	75
Create Emergency Disk .....	75
Import/Export Settings .....	76
<b>8. More option .....</b>	<b>78</b>
<b>9. Help &amp; Other Recommendations .....</b>	<b>79</b>
<b>Keep Guardian Total Security updated to be safe from new viruses .....</b>	<b>79</b>
Updating Guardian Total Security online .....	79
Updating Guardian Total Security offline .....	80
Update Guidelines for Network Environment .....	81
Cleaning Viruses .....	81
Cleaning viruses encountered during scanning .....	82
Cleaning virus detected in memory .....	82

About antivirus license .....	83
Submitting System Information .....	84
Generating System Information .....	84
Reports .....	85
Viewing Reports.....	85
Uninstalling antivirus software .....	86
<b>10. Support.....</b>	<b>88</b>
Technical Support.....	88

# 1. Getting started

---

To install Guardian Total Security, ensure that you comply with the following requirements.

[Prerequisites](#)

[System requirements](#)

## Prerequisites

Before installing Guardian Total Security on your computer, follow these guidelines:

- Remove any other antivirus software program from your computer if you have any. If multiple antivirus software products are installed on a single computer, it may result in system malfunction.
- Close all open applications, browsers, programs, and documents for uninterrupted installation.
- Ensure that you have administrative rights for installing Guardian Total Security.

## System requirements

To use Guardian Total Security, you must ensure the following requirements.

### General requirements

- 1.0 GB disk space.
- Internet Explorer 6 or later.
- Internet connection to receive updates.

## System requirements

The following table describes the system requirements for various operating systems.

Operating Systems (OS)	Minimum System Requirements
Windows 11	Processor: 1 gigahertz (GHz) or faster RAM: 4 gigabyte (GB)
Windows 10	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows 8.1 / Windows 8	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows 7 SP 1 and later	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit Make sure you have installed Microsoft patches KB4474419 and KB4490628 also. <b>How to check if the required patches are installed?</b> - Open Control Panel - Go to Windows Update - From the Windows Update page, click on 'View Update History'.
Windows XP (Service Pack 2 and later)	Processor: 300 Megahertz (MHz) Pentium or faster RAM: 512 MB



### Note:

- The requirements are applicable to all flavors of the operating systems.
- The requirements are applicable to the 32-bit and 64-bit operating systems unless specifically mentioned.
- System requirements may change from time to time. It is advisable that you check for the latest system requirements at <http://www.guardianav.co.in>.

## Supported POP3 email clients

Guardian Total Security supports the following email clients.

- Microsoft Outlook Express 5.5 and later
- Microsoft Outlook 2000 and later
- Netscape Messenger 4 and later
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail



Note: The Email Protection feature does not support encrypted email connections that use Secure Sockets Layer (SSL).

## Feature specific compatibility

The following table describes feature specific compatibility.

Features	Conditions
Anti-Keylogger	<ul style="list-style-type: none"><li>• Is not supported on Microsoft Windows XP 32-bit with Service Pack 1 or previous and Windows XP 64-bit.</li></ul>
Anti-Rootkit	<ul style="list-style-type: none"><li>• Is supported on 32-bit OS only.</li></ul>
Browser Sandbox	<ul style="list-style-type: none"><li>• Is not supported on Microsoft Windows XP 64-bit.</li><li>• This feature supports Internet Explorer, Google Chrome, and Mozilla Firefox browsers only.</li><li>• This feature does not support Microsoft Edge browser of Windows 10 and Windows 11 operating systems.</li></ul>
Emergency Disk	<ul style="list-style-type: none"><li>• Creating Emergency Disk using CD/DVD is not supported on Microsoft Windows 2003 and earlier versions. However, you can create Emergency Disk on USB drives.</li></ul>
Firewall	<ul style="list-style-type: none"><li>• The Monitor Wi-Fi Networks feature is not supported on Microsoft Windows XP 64-bit.</li></ul>
Safe Banking	<ul style="list-style-type: none"><li>• Is not supported on Microsoft Windows XP 64-bit.</li><li>• This feature supports Internet Explorer, Google Chrome, and Mozilla Firefox browsers only.</li><li>• This feature does not support Microsoft Edge browser of Windows 10 and Windows 11 operating systems.</li></ul>

Features	Conditions
Self-Protection	<ul style="list-style-type: none"><li>• For Microsoft Windows XP operating system, this feature is supported only if Service Pack 2 or later is installed.</li><li>• Process protection functionality of Self-Protection is supported on Microsoft Windows 7 Service Pack 1 and later.</li></ul>

## How to download, install, and register Guardian Total Security

### Downloading and Installing Guardian Total Security

To download and install Guardian Total Security, follow these steps:

1. Visit the following link <https://www.guardianav.co.in/setup>.

Alternatively, if you have the Guardian Total Security CD/DVD, enter the CD/DVD in the DVD drive. Double-click the setup. Click **Install** to initiate the installation process.

You are redirected to the website of Guardian where all antivirus products are listed.

2. Click the **Download** button under Guardian Total Security.

The downloader setup is downloaded on your computer.

3. Double-click the downloaded setup to start the downloading.

The license agreement and privacy policy page appears. Accept the terms and conditions and privacy policy to proceed.

4. Click the **Let's Start** button.

Downloading and installation of the software starts.

Installation Location and disk space requirement screen appears.

Make sure that disk space required for installation is available on the default location. If required, you can change the location by clicking the **Browse** button.

5. When the installation completes, the Registration Information page appears with the options **Register Now** and **Register Later**.

It is advisable that you must register your product soon after you install it. To register, click **Register Now**.

If you want to register the product later, click **Register Later**. To register the product later, see [Registering Guardian antivirus](#).

6. Enter the **Product Key** and **Dealer Code**. All asterisk fields are mandatory to fill. Click **Register Now**.
7. On the next screen, enter your **Name**, **Email Address**, **Contact Number**, **Country**, **State**, and **City**. Click **Continue**.

A summary of the information that you entered appears. Click **Register**.

Guardian Total Security is downloaded, installed, and registered on your computer successfully.

8. To close the screen, click **Finish**.

## Registering Guardian Total Security

You can register/activate Guardian Total Security online, offline, or through SMS as per your convenience. Select one of the following options that suits you best.

[Registering online](#): Prefer this method if the computer on which you have installed the antivirus has Internet connection.

[Registering offline](#): Prefer this method if the computer on which you have installed the antivirus has no Internet connection. You need to generate an activation key and then you can register the antivirus.

[Registering through SMS](#): Prefer this method only if you are based in India.



---

Note: The options to register Guardian Total Security offline and through SMS appear only if you are not connected to the Internet.

---

## Registering Guardian Total Security online

To register Guardian Total Security online, follow these steps.

1. If you are on the installation screen, click the **Register Now** button.

If you are registering later, open **Guardian Total Security**. On the left pane, click **Status** and then click the **Register Now** button.

The Registration Information page appears.

2. On the Registration Information page, enter the **Product Key** and **Dealer Code**. All asterisk fields are mandatory to fill. Click **Register Now**.
3. On the next screen, enter your **Name**, **Email Address**, **Contact Number**, **Country**, **State**, and **City**. Click **Continue**.

A summary of the information that you entered appears. Click **Register**.

Guardian Total Security is registered on your computer successfully. The expiry date of your license is displayed.

4. To close the screen, click **Finish**.

## Registering Guardian Total Security offline

Before registering Guardian Total Security offline, ensure that you have the product key, installation number, and activation license key ready with you.

### Registering Guardian Total Security offline

To Register Guardian Total Security offline, follow these steps.

1. If you are on the installation screen, click the **Register Now** button.

If you are registering later, open **Guardian Total Security**. On the left pane, click **Status** and then click the **Register Now** button.

If your computer is not connected to the Internet the Offline Registration options appear.

2. Click **Register Offline**.

The Offline Registration page appears with a 12-digit Installation Number and an offline activation URL. Note down these details as you will need them to generate an activation key.

You need to [generate an activation key](#) and register your license using the activation key.

3. Click **Browse** to select the **<license>.key**. Click **Register**.

Your license is registered successfully and the expiry date of your license is displayed.

4. To close the screen, click **Finish**.

## Generating activation license key

To generate an activation license key, follow these steps:

1. Visit the offline activation page at <https://www.guardianav.co.in/act2015>.

An Off-Line Registration page appears.

Ensure that you have the Product Key and Installation Number ready with you.

You can find your Product Key in your product packaging. If you have purchased the product online, the Product Key is sent to the email address confirming your purchase order.

2. Enter the **Product Key** and **Installation Number** in the relevant fields and click **Submit**.
3. On the registration form, enter the relevant information and then click **Submit**.

All asterisk (\*) fields are mandatory to fill.

A new offline activation license key is generated. This key is unique and can be used only once. Save this key to register Guardian Total Security offline. This key is also sent to your email address that you provided during registration of the product.

## Registering Guardian Total Security through SMS



---

Note: Currently, the Registration through SMS facility is available to the subscribers based in India only.

---

To register Guardian Total Security through SMS, follow these steps:

1. If you are on the installation screen, click the **Register Now** button.

If you are registering later, open **Guardian Total Security**. On the left pane, click **Status** and then click the **Register Now** button.

If your computer is not connected to the Internet the Offline Registration options appear.

2. Click **SMS Registration**.

A screen with the conditions related to registering through SMS appears. Read the conditions carefully.

3. Click **Next**.

4. Enter the **Product Key** and **Dealer Code**. All asterisk fields are mandatory to fill. Click **Register Now**.

5. On the next screen, enter your **Name, Email Address, Contact Number, Country, State, and City**. Click **Continue**.

A summary of the information that you entered appears. Click **Register**.

A unique code along with a mobile number is displayed.

6. Type the code and send it as an SMS to one of the numbers displayed.

After successful registration, you will receive an SMS on your registered mobile number that contains an alphanumeric activation code.

7. Type this activation code in the text box displayed and click **Register**.

Guardian Total Security is registered on your computer successfully and the expiry date of your license is displayed.

8. To close the screen, click **Finish**.

## Post Registration of Guardian Total Security

### Run a complete scan

It is recommended that you carry out a complete scan on first time installation. This will ensure that your computer is fully clean and secure and also minimize the scanning process for new malware and virus.

### Optimum security

Most of the required security settings are turned on by default. However, you may need to configure some settings for the desired result such as Parental Control. It is advisable that you explore this product to take maximum advantage.

## 2. Reactivation and renewal

---

This chapter includes the following sections.

[Reactivating Guardian Total Security](#)

[Renewing Guardian Total Security](#)

### Reactivating Guardian Total Security

Reactivation is a facility that ensures that you use the product for the entire period until your license expires. Reactivation is helpful in case you format your system when all software products are removed, or you want to install Guardian Total Security on another computer.

Every time you install the antivirus, you need to reactivate it. The reactivation process is similar to the activation process, with the exception that you do not need to enter the complete personal details again.

It is advisable that you select the option [Remove Guardian and keep update definitions files](#) during uninstallation. This will help you retain product update definition files and process reactivation easily.

### How to renew Guardian Total Security

We recommend to renew your license before it expires so that your computer system remains protected uninterruptedly. You can buy the renewal code from the website of [Guardian](#) or from the nearest distributor or reseller.

You can renew Guardian Total Security in any of the following ways.

[Renewing online](#): Prefer this method if the computer on which you have installed the antivirus has Internet connection.

[Renewing offline](#): Prefer this method if the computer on which you have installed the antivirus has no Internet connection. You need to generate an activation key and then you can renew the antivirus.



Note: The option to renew Guardian Total Security offline appears only if you are not connected to the Internet.

---

## Renewing Guardian Total Security online

To renew Guardian Total Security online, follow these steps.

1. Open **Guardian Total Security**.
2. On the left pane, click the More option and then select the **About** option.  
  
If your product license has expired, the **Renew Now** button is displayed on the dashboard in **Status**. To renew your license, click **Renew Now**.  
The Registration Wizard appears. Your product details are displayed.
3. If you have already purchased the renewal code, click **I have a key** and enter the renewal code. Click **Renew Now**.  
  
If you do not have a license, you can [buy the license](#) online.
4. Relevant information in the **Email Address** and **Contact Number** text boxes appears pre-filled. Enter the **Dealer Code** and then click **Continue**.  
  
You can modify your contact details, if required.  
The license information such as **Current expiry date** and **New expiry date** is displayed for your confirmation.
5. Click **Renew**.  
  
The license of Guardian Total Security is renewed successfully.
6. To close the screen, click **Finish**.

## Buying the license online

If you want to buy a license online, click the **Buy Now** option. This option will redirect you to the online portal.

As soon as you buy the license, your license is renewed instantly. The new license expiry date is displayed.



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

---

## Renewing Guardian Total Security offline

Before renewing Guardian Total Security offline, ensure that you have the product key, installation number, renewal code, and activation license key ready with you.

### Renewing Guardian Total Security offline

To renew Guardian Total Security offline, follow these steps.

1. Open **Guardian Total Security**.
2. On the left pane, click the More option and then select the **About** option.

If your product license has expired, the **Renew Now** button is displayed on the dashboard in **Status**. To renew your license, click **Renew Now**.

If your computer is not connected to the Internet the Offline Renewal options appear.

3. Click **Renew Offline**.

The Renew Offline page appears with a 12-digit Installation Number, a Product Key, and an offline renewal URL. Note down these details as you will need them to generate an activation key.

You need to [generate an activation key](#) and renew your license using the activation key.

4. Click **Browse** to select the **<license>.key**. Click **Renew**.

Your license is renewed successfully and the expiry date of your license is displayed.

5. To close the screen, click **Finish**.

### Generating activation license key

To generate an activation license key, follow these steps:

1. Visit the offline renewal page at [https://www.guardianav.co.in/renew\\_off](https://www.guardianav.co.in/renew_off).

An Off-Line Renewal page appears.

Ensure that you have the Product Key and Installation Number (as described in the preceding section), and renewal code with you.

2. Enter the **Product Key**, **Installation Number**, and **Renewal Key** and then click **Submit**.

Upon verification of the provided data, the succeeding screen displays the user name, registered email address, and contact number. If your email address and contact number have changed, you can update them or else click **Submit**.

A new offline activation license key is generated. This key is unique and can be used only once. Save this key to renew Guardian Total Security offline. This key is also sent to your email address that you provided during registration of the product.

## 3. Status

---

You can open Guardian Total Security in any one of the following ways.

- On the taskbar, double-click the **Guardian Total Security** icon or right-click the **Guardian Total Security** icon and select **Open Guardian Total Security**.
- Select **Start > Programs > Guardian Total Security > Guardian Total Security**.
- Select **Start > Run**, type the word `scanner` and press ENTER.

When you open Guardian Total Security, Status section appears. Status includes the following topics.

Menu/Section	Description
Status	<p>Status is the baseboard where you can see the current status whether any virus threat has been detected and how many threats or trackers have been blocked.</p> <p><b>Green Status:</b> Shows the protection status of your computer system. If your computer is secure, status is displayed in green (●).</p> <p><b>Orange Status:</b> If your computer needs your attention at your earliest convenience but not immediately, it is displayed in orange (●).</p> <p><b>Red Status:</b> If your computer is not configured with optimal settings and your immediate attention is needed, it is displayed in red (●). The action corresponding to the message needs to be carried out immediately to keep your computer protected.</p>
License validity	Displays days until the license is valid. To know more details about the license, you can click the <b>License</b> link.
Threats Detected	Displays the threats detected till date.
Security Updates	Displays the latest updates about security from Guardian Total Security. You can see all the news by clicking <b>See All</b> .
<a href="#">Scan Now</a>	Provides you with various scan options such as Full System Scan, Custom Scan, Memory Scan, and so on.
Feedback	You can share feedback about your experience of using our product.

Menu/Section	Description
Virtual Keyboard	Virtual Keyboard helps you enter the required information without pressing any keys on the physical keyboard. It reduces the risk of getting your information recorded by a possible keystroke logger malware.
<a href="#">Support</a>	Support option displays all the support sources that Guardian Total Security provides.
Facebook Like	The Facebook Like link redirects you to the <a href="#">Facebook page</a> of Guardian antivirus products. You can follow us to read posts on cyber security and virus threats and alerts by clicking the <b>Like</b> link.

## Why you should scan your computer

It is recommended that you carry out a complete scan on first time installation. This will ensure that your computer is fully clean and secure and also minimize the scanning process next time.

## Scan options

In Guardian Total Security, there are various types of scan options to suite your requirements. You can initiate scanning of your entire system, or certain drives, network drives, USB drives, folders or files, locations and drives, memory scan, and boot time scan. Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan as you prefer.

### Quick Scan

This feature completes the scanning of your system on faster pace. With Quick Scan, only the predefined locations that can be vulnerable to malicious attacks are scanned.

To initiate a quick scan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Status**. Click **Scan Now** or click the spilt button and then select **Quick Scan**.

The scan starts.

On completion of the scan, you can view the scan report under **Reports**.

## Full System Scan

This feature helps you initiate a complete scan of all boot records, drives, folders, files, and vulnerabilities on your computer (excluding mapped network drives).

Full System Scan is advisable soon after first installation. Our Full System Scan is smart to run a complete scan for the first time. Next time, it scans only new files or those files that have been changed. This differential scanning optimizes scanning time.

To initiate a full system scan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Status**. Click the spilt button available next to **Scan Now** and then select **Full System Scan**.

The scan starts.

On completion of the scan, you can view the scan report under **Reports**.

## Custom Scan

This feature helps you scan specific drives and folders on your system. This is helpful when you want to scan only certain items and not the entire system.

To scan specific folders, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Status**. Click the spilt button available next to **Scan Now** and then select **Custom Scan**.
3. On the Custom Scan screen, a list of items is displayed in the Scan Item list if you have added any items to scan. If you have not added any item before or you want to scan some new items, click **Add** to add the scan items.

- On the **Browse for Folder** list, select the folders that you want to scan.

You can add multiple folders for scanning. All the subfolders in the selected folder will also be scanned. You can exclude subfolder from scanning if required. To exclude the subfolder, select the **Exclude Subfolder** option and then click **OK**.

4. Select an item from the Scan Item list and then click **Start Scan**.

The scan begins.

Upon completion of the scanning, you can view the scan report in the Reports menu.

## Memory Scan

This feature scans memory of your computer system.

To perform a memory scan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Status**. Click the spilt button available next to **Scan Now** and then select **Memory Scan**.

The scan starts.

On completion of the scan, you can view the scan report under **Reports**.

The following fields are displayed during a scan.

Fields	Description
Files scanned	Displays the total number of files scanned.
Archive/Packed	Displays the number of archive or packed files scanned.
Threats detected	Displays the number of threats detected.
DNAScan warnings	Displays the number of files detected by DNAScan.
Boot/Partition viruses	Displays the number of Boot/Partition viruses.
Files repaired	Displays the number of malicious files that have been repaired.
Files quarantined	Displays the number of malicious files that have been quarantined.
Files deleted	Displays the number of malicious files that have been deleted.
Scanning status	Displays the status of the scan being performed.

## Boot Time Scan

This feature helps to clean even highly infected systems. Some viruses tend to be active if the system is running and they cannot be cleaned. Using Boot Time Scan, you can clean such viruses. This scan will be performed on next boot using Windows NT Boot Shell.

To set Boot Time Scan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Status**. Click the spilt button available next to **Scan Now** and then select **Boot Time Scan**.

Boot Time Scan has the following options:

- Quick Scan: Scans only system pre-defined locations that are at high risk to viruses.
  - Full System Scan: Scans the entire system. This may be time consuming.
3. Click **Yes**.
  4. To restart the system for scanning immediately, click **Yes**. To scan the system later, click **No**.



Note: In case Boot Time Scan takes time or it has been initiated by mistake, you can stop it by pressing the **ESC** key.

---

## 4. Protection

---

While working on your computer system, you may be connected to the Internet, external drives, and may send and receive email communications. Your system may be exposed to viruses or malwares that try to infiltrate into your system.

Protection section includes those features that allow you to secure your systems, folders, files, and data against any possible threats of malware, viruses, worms, and data theft.

Protection includes the following features.

[Ransomware Protection](#)

[Virus Protection](#)

[Scan Settings](#)

[Browsing Protection](#)

[Phishing Protection](#)

[Safe Banking](#)

[Firewall Protection](#)

[IDS/IPS](#)

[Email Protection](#)

[USB Drive Protection](#)

[External Drive Protection](#)

[Browser Sandbox](#)

[Malware Protection](#)

[Anti Malware](#)

[Anti Rootkit](#)

# Ransomware Protection

## How you can prevent ransomware attack

Ransomware attackers drop ransomware on your computer that locks up your computer. They leave a message to blackmail you to pay money to let you access your computer.

Ransomware Protection detects such ransomware attacks. This feature [backs up data](#) on your computer that you can [restore](#) when required. Most of the popularly known documents including tally data are protected.

Your computer may be infected by ransomware in several ways such as:

- Browsing infected or fake websites.
- Opening emails or email attachments from phishing attackers.
- Opening malicious links from websites or social networking sites.
- Installing fake apps and tools.
- Playing online games from untrusted sites.

## Configuring Ransomware Protection

To configure Ransomware Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Ransomware Protection**.
3. On the Ransomware Protection screen, turn **Ransomware Protection** on.

## Exclude Files & Folders

With this feature, you can specify which files and folders should not be included during scanning for ransomware and other malicious attacks. Exclusion of files helps you avoid unnecessary scanning of files that have already been scanned or you are sure that certain files should not be scanned.

You can exclude files from being scanned from the following scanning modules.

- Known virus detection
- DNAScan
- Suspicious packed files scan

- Behavior detection
- Ransomware detection

## Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Ransomware Protection**.
3. On the Ransomware Protection screen, click **Exclude Files & Folders**.

The Exclude Files & Folders details screen appears. Here you see the list of excluded files and folders that have been added.

4. To add a new file or folder, click **Add**.

The New Exclude Item screen appears.

5. In the **Item** text box, provide the path to the file or folder. You can also click the file or folder icon to select the path.

Ensure that you provide the path to the correct file or folder, else a message appears.

6. Under Exclude From, select the modules from which you want to exclude the selected file or folder.

You can select either Known virus detection or any from DNAScan, Suspicious packed files scan, and Behavior Detection and Ransomware detection options.

7. Click **OK**.
8. To save your settings, click **Save Changes**.



### Note:

- If you are getting warning for a known virus in a clean file, 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 from being scanned for DNAScan.
-

## Virus Protection

Viruses from various sources such as email attachments, Internet downloads, file transfer, and file execution try to infiltrate your system. This feature helps you to continuously keep monitoring your system for viruses. Importantly, this feature does not re-scan the files that have not changed since the previous scan, thereby lowering resource usage.

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. By default, Virus Protection is turned on.

### Configuring Virus Protection

To configure Virus Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Virus Protection**. Turn **Virus Protection** on.
3. To configure, click the settings icon for **Virus Protection**.

The Virus Protection details screen appears.

4. Set the following options as per requirement:
  - **Display alert message** – Select this option if you want to get the alerts on various events. For example, when malware is detected. This option is selected by default.
  - **Select action to be performed when virus is found** – Select an appropriate action to be taken when a virus is detected during the scan.
  - **Backup before taking action** – Select this option if you want to take a backup of a file before taking an action. Files that are stored in the backup can be restored from Quarantine.
  - **Enable sound when threat is detected** – Select this option if you want to be alerted with sound whenever a virus is detected.
5. To save your setting, click **Save Changes**.

## Action to be taken when a virus is detected

The following table describes various actions and their description.

Action	Description
Repair	If a virus is detected during a scan, the file is cleaned and repaired. If the file cannot be repaired, it is quarantined automatically.
Delete	Deletes a virus-infected file without notifying you.
Deny Access	Restricts access to a virus infected file from use.

## Turning off Virus Protection

It is recommended that you always keep Virus Protection turned on to keep your system clean and secure from any potential threats. You can turn Virus Protection off when required. While you turn Virus Protection off, you have a number of options to turn off the feature temporarily, so that it turns on automatically after the select time interval passes.

To turn off Virus Protection, follow these steps.

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Virus Protection**. Turn **Virus Protection** off.
3. To turn off Virus Protection, select one of the following options:
  - Turn on after 15 minutes
  - Turn on after 30 minutes
  - Turn on after 1 hour
  - Turn on after next reboot
  - Permanently disable
4. To save your settings, click **OK**.

After you turn Virus Protection off, the icon color of the Scan Options option on Status changes from green to red and a message "System is not secure" is displayed.

## Scan Settings

With this feature, you can configure the protection settings for files and folders in your system.

Scan Options includes the following protection settings.

- [Scan Settings](#)
- [Advance DNAScan](#)
- [Block Suspicious Packed Files](#)
- [Automatic Rogueware Scan](#)
- [Scan Schedule](#)
- [Exclude Files & Folders](#)
- [Quarantine & Backup](#)
- [Exclude File Extensions](#)

Take advantage of automatic scanning of your computer

## Scan Settings

This feature helps you define about how to initiate the scan of your system and what action should be taken when a virus is detected. The default settings are optimal that ensures the required protection to your system.

### Setting scan mode

To configure Scan Settings, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Scan Settings**.
4. Under [Select scan mode](#), select **Automatic (Recommended)** to initiate the scan automatically, or select **Advanced** for [advanced level scanning](#).
5. Under [Select action to be performed when virus is found](#), select an appropriate action.

6. If you want to take a backup of the files before taking an action on them, select **Backup before taking action**.
7. To save your settings, click **Save Changes**.

## Scan modes

**Automatic (Recommended):** It is the default scan type and is recommended as it ensures the optimal protection to your system. This setting is an ideal option for novice users.

**Advanced:** This helps you customize the scan option. This is ideal for experienced users. When you select the Advanced option, the Configure button is activated and you can configure the Advanced settings for scanning.

## Action to be performed when a virus is found

You can configure the following actions to be taken when a virus is detected on your computer.

Action	Description
Repair	Select this option if you want to repair an infected file. If a virus is found during a scan in a file, it repairs the file. If the file cannot be repaired, it is quarantined automatically. If the infectious file has a Backdoor, Worm, Trojan, or Malware, Guardian Total Security automatically deletes the file.
Delete	Select this option if you want to delete an infected file. The infected file is deleted without notifying you. Once the files are deleted, they cannot be recovered.
Skip	Select this option if you want to take no action on an infected file.
Backup before taking action	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from Quarantine.

## Configuring Advanced Scan Mode

To configure Advanced Scan mode, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Scan Settings**.

4. Under [Select scan mode](#), select **Advanced**.  
The Configure button is activated.
5. Click **Configure**.  
The advanced scan setting details screen appears.
6. Under **Select item to scan**, select **Scan executable files** if you want to scan only the executable files or select **Scan all files** if you want to scan all files.  
By default, the Scan executable files option is selected.  
It takes time to carry out **Scan all files** and the process may slow down your system.
7. Select one of the following items for scanning:
  - [Scan archive files](#): Select this option if you want to scan the archive files such as zip files and RAR files.
  - **Scan packed files**: Select this option if you want to scan packed files.
  - **Scan mailboxes**: Select **Quick scan of mailboxes** for a brief scan or else select **Through scan of mailboxes** to scan thoroughly.
8. Click **OK**.
9. To save your settings, click **Save Changes**.

## Scanning archive files

This feature helps you configure the scan rules for archive files such as ZIP files, RAR files, and CHM files.

To configure the Scan archive files feature, follow these steps:

1. On the [Advanced scan setting](#) screen, select **Scan archive files**.  
The Configure button is activated.
2. Click the **Configure** button.  
The Scan archive files details screen appears.
3. Under **Select action to be performed when virus is found**, select one of the following options: Delete, Quarantine, and Skip.
4. In **Archive Scan Level**, select the level to which you want to scan the files and folders.

The default scan level is set to level 2. Increasing the default scan level may affect the scan speed.

5. Under **Select the type of archive that should be scanned**, select the archive files types.
6. To save your settings, click **OK**.

## Action to be taken when a virus is found

The following table describes various actions and their description.

Action	Description
Delete	Select this option if you want to delete an infected file. The-infected file is deleted without notifying you.
Quarantine	Select this option if you want to quarantine an infected archive if a virus is found in it.
Skip	Select this option if you want to take no action on an infected file.

## Selecting the type of archive to be scanned

A list of archives that can be included for scan during the scanning process is available in this section. Few of the common archives are selected by default that you can customize based on your requirement.

The following table describes the archive types.

Buttons	Description
Select All	Helps you select all the archives in the list.
Deselect All	Helps you clear all the archives in the list.

## Scanning packed files

This feature helps you scan packers or compressed files. Packers are the files that group many files or compress them into a single file to reduce the file size. Moreover, these files do not need a third-party application to get unpacked. They have an inbuilt functionality for packing and unpacking.

Packers can also be used as tools to spread malware by packing a malicious file along with a set of files. When such packers are unpacked they can cause harm to your computer system. If you want to scan packers, select the **Scan packed files** option.

## Scanning mailboxes

This feature allows you to scan the mailbox of Outlook Express 5.0 and later versions (inside the **DBX** files). Viruses such as KAK and JS.Flea.B, remain inside the DBX files and can reappear if patches are not applied for Outlook Express. The feature also scans the email attachments encoded with UUENCODE/MIME/BinHex (Base 64). **Scan mailboxes** is selected by default which activates the following two options.

Options	Description
Quick scan of mailboxes	Helps you skip all the previously scanned messages and scan only new messages. This option is selected by default.
Thorough scan of mailboxes	Helps you scan all the mails in the mailbox all the time. This may affect the speed as the size of the mailbox increases.

## Advance DNAScan

DNAScan is an indigenous technology in the Guardian products that detects and eliminates new and unknown malicious threats on your system. Advance DNAScan technology successfully traps suspected files with very less false alarms. Additionally, it quarantines the suspected file so that malware does not harm your system.

The quarantined suspicious files can be submitted to the Guardian research labs for further analysis that helps in tracking new threats and curb them on time. After the analysis, the threat is added in the known threat signature database and the solution is provided in the next updates to the users.

## Configuring Advance DNAScan

To configure Advance DNAScan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Advance DNAScan**.

The Advance DNAScan details screen appears.

4. Select either of the following options as per requirement:
  - **Enable DNAScan:** Select this option to enable DNAScan.

- **Enable Behavior detection system:** Select this option if you want to enable Behavior detection system. The running applications will be monitored for their behavior. You can also set a security alert level from the **Select Behavior detection level** list either as High, Moderate, or Low.
  - High: If you select this security level, Guardian Total Security will closely monitor the behavior of a running application and will alert you if any unusual application behavior is noticed. You may receive more alerts and sometimes even for genuine files.
  - Moderate: If you select this security level, Guardian Total Security will send alert if any suspicious activity of a running application is noticed.
  - Low: If you select this security level, Guardian Total Security will send alert only if any malicious activity of a running application is noticed.

Note: If you have selected Moderate or Low security level, **Behavior detection system\*** will also block many unknown threats in the background without prompting you for any action if it finds the application behavior suspected.
- **Do not submit files:** Select this option if you do not want to submit suspicious files to the Guardian Total Security research labs.
- **Submit files:** Select this option if you want to submit the suspicious files to the Guardian Total Security research labs for further analysis. You can also select **Show notification while submitting files** to get prompts for permission before submitting the files.



---

Tip: If the option **Show notification while submitting files** is not selected, Guardian Total Security will submit the suspicious files without notifying you.

---

Advance DNAScan detects files by studying their characteristics and behavior.

## Detection by Characteristics

Thousands of new and polymorphic threats (which change their code/file information) are born daily. Detecting them by their signature requires time. Our Advance DNAScan technology detects such threats in real time, with zero-time lapses.

Whenever DNAScan detects a new malicious threat in your system, it quarantines the suspicious file and displays a message along with the file name. If you find that

the file is genuine, you can also restore that file from quarantine by using the option provided in the message box.

## Detection by Behavior

If the option **Behavior detection system** is enabled, DNAScan continuously monitors the activities performed by an application in your system. If the application deviates from its normal behavior or carries out any suspicious activity, **Behavior detection system** suspends that application from executing further activities that may cause potential damage to the system.

Upon detecting such an application, it prompts you to take an appropriate action from the following options:

- **Allow:** Take this action if you want to allow the application to run. Select this action if you are sure the applications are genuine.
- **Block:** Take this action if you want to block the application from running.

## Submitting Suspected Files

You can submit the suspicious files either automatically or manually. The submission takes place automatically whenever Guardian Total Security updates itself and finds new quarantined DNAScan-suspected files. This file is sent in an encrypted file format to the Guardian Total Security research labs.

You can also submit the quarantined files manually if you think they should be submitted immediately. You can submit the files in the following way:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **View Quarantine Files**.

The Quarantine dialogue appears.

A list of the files that have been quarantined is displayed.

3. Select the files that you want to submit to the Guardian Total Security labs and then click **Send**.
4. To close the Quarantine dialogue, click **Close**.

## Block Suspicious Packed Files

Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious

harm to the computer systems. This feature helps you identify and block such suspicious packed files.

It is recommended that you always keep this option enabled to ensure that the suspicious files are not accessed and thus prevent infection.

### Configuring Block Suspicious Packed Files

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, turn **Block Suspicious Packed Files** on.

By default, Block Suspicious Packed Files is turned on.

### Automatic Rogueware Scan

This feature automatically scans and removes rogueware and fake anti-virus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.

### Configuring Automatic Rogueware Scan

To configure Automatic Rogueware Scan, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, turn **Automatic Rogueware Scan** on.

By default, Automatic Rogueware Scan is turned on.

### Scan Schedule

Scanning regularly helps you keep your system free from virus and other types of infections. This feature allows you to define a schedule when to begin scanning of your system automatically. You can define multiple numbers of scan schedules to initiate scan at your convenience.

## Configuring Scan Schedule

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Scan Schedule**.

The Scan Schedule details screen appears.

4. To define a new scan schedule, click **New**.
5. In **Scan Name**, type a scan name.
6. Under Scan Frequency, select the following options based on your preferences:
  - Scan Frequency:
    - Daily: Select this option if you want to initiate scanning of your system daily. This option is selected by default.
    - Weekly: Select this option if you want to initiate scanning of your system on a certain day of the week. When you select the Weekly option, the Weekdays drop-down list is activated so you can select a day of the week.
  - Scan time:
    - Start at first boot: This helps you schedule the scanner to begin at the first boot of the day. If you select this option, you do not need to specify the time of the day to start the scan. Scanning takes place only during the first boot regardless what time you start the system.
    - Start at: Select this option to initiate the scanning of your system at a certain time. If you select this option, the time drop-down list is activated where you can set the time for scanning. By default, this option is selected.

You can further define how often the scan should begin in the **Everyday** and **Repeat scan after every** options.

- Scan priority.
  - High: Helps you set high scan priority.
  - Low: Helps you set low scan priority . By default, this option is selected.

7. Under **Scan Settings**, you can specify scan mode, define the advanced options for scanning, action to be performed when virus is found and whether you want a backup of the files before taking any action on them. The default setting is adequate for scanning to keep your system clean.
8. In the **Username** text box, enter your username and your password in the **Password** text box.
9. **Run task as soon as possible if missed**: Select this option if you want to initiate scanning when the scheduled scan is missed. This is helpful in case your system was switched off and the scan schedule passed, later when you switch on the system, the scan schedule will automatically start as soon as possible.

This option is available only on Microsoft Windows 7 SP 1 and later operating systems.

10. Click **Next**.

The Configure Scan Schedule screen for adding folders to be scanned appears.
11. Click **Add Folders**.
12. In the Browse for Folder Window, select the drives and folders to be scanned. You can add multiple numbers of drives and folders as per your requirement.

If you want to exclude subfolders from being scanned, you can also select **Exclude Subfolder**. Click **OK**.
13. On the Configure Scan Schedule screen, click **Next**.
14. A summary of your scan schedule appears. Verify and click **Finish** to save and close the Scan Schedule dialogue.
15. Click **Close** to close the Scan Schedule screen.

### Editing a scan schedule

This feature allows you to change the scan schedule if required. To edit a scan schedule, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Options screen, click **Scan Schedule**.

The Scan Schedule details screen appears.

4. Select the scan schedule that you want to edit and then click **Edit**.
5. Make the required changes in the scan schedule and then click **Next**.
6. On the Configure Scan Schedule screen, you can add or remove the drives and folders as per your preference and then click **Next**.
7. Check the summary of the modification in the scan schedule.
8. Click **Finish** to close the Scan Schedule dialogue.
9. Click **Close** to close the Scan Schedule screen.

## Removing a scan schedule

You can remove a scan schedule whenever required. To remove a scan schedule, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Options screen, click **Scan Schedule**.

The Scan Schedule details screen appears.

4. Select the scan schedule that you want to remove and then click **Remove**.

The confirmation screen appears.

5. Click **Yes** to remove the selected scan schedule.
6. To close the Scan Schedule screen, click **Close**.

To know about how to configure Scan Settings, see [Scan Settings](#).

## Exclude Files & Folders

With this feature, you can specify which files and folders should not be included during scanning for ransomware and other malicious attacks. Exclusion of files helps you avoid unnecessary scanning of files that have already been scanned or you are sure that certain files should not be scanned.

You can exclude files from being scanned from the following scanning modules.

- Known virus detection

- DNAScan
- Suspicious packed files scan
- Behavior detection
- Ransomware detection

## Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Exclude Files & Folders**.

The Exclude Files & Folders details screen appears. Here you see the list of excluded files and folders that have been added.

4. To add a new file or folder, click **Add**.

The New Exclude Item screen appears.

5. In the **Item** text box, provide the path to the file or folder. You can also click the file or folder icon to select the path.

Ensure that you provide the path to the correct file or folder, else a message appears.

6. Under Exclude From, select the modules from which you want to exclude the selected file or folder.

You can select either Known virus detection or any from DNAScan, Suspicious packed files scan, and Behavior Detection and Ransomware detection options.

7. Click **OK**.
8. To save your settings, click **Save Changes**.



Note:

- If you are getting warning for a known virus in a clean file, 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 from being scanned for DNAScan.
-

## Quarantine & Backup

This feature allows you to safely isolate the infected or suspected files. The suspected files are quarantined in an encrypted format to prevent from being executed. This helps prevent infection.

If you want a copy of the infected file before it gets repaired, select the option **Backup before taking action** in Scan Settings.

You can also set when the quarantined files should be removed from Quarantine and have a backup of the files if you need.

## Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Quarantine & Backup**.

The Quarantine & Backup details screen appears.

4. Select **Delete quarantine/backup files after** and set the number of days after which the files should be removed from Quarantine automatically. By default, **30 days** is set.
5. To see which files have been quarantined, click **View Files**. A list of the quarantine files appears. You can take any of the following actions on the quarantined files:
  - **Submit for Analysis**: Helps you send a quarantined file to the Guardian research labs for analysis. We will analyze the file and create an appropriate solution in future.
  - **Add**: Helps you quarantine a file manually.
  - **Restore** : Helps you restore a quarantined file to its original location.

When you find a quarantined file trustworthy and try to restore it, an option for adding the file to the exclusion list appears. You can add the file to the exclusion list so that the same file is not treated as suspected and quarantined again.

- **Delete:** Helps you delete a quarantined file. Select a quarantined file and click **Delete**.
  - **Delete All:** Helps you delete all the quarantined files at one go.
6. To close the Quarantine dialog, click the **Close** button.

## Exclude File Extensions

You can create a list of file extensions that you want to exclude from Virus Protection. It is advisable that you exclude only the trusted file extensions. Virus Protection will not scan the listed file extensions and concentrate only on those files that are prone to malicious behavior.

### Creating Exclusion List

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Scan Settings**.
3. On the Scan Settings screen, click **Exclude File Extensions**.
4. In the Add text box, enter the file extension and then click **Add**.  
  
If the added extension is incorrect, select the extension in the list and click **Remove** to remove it.
5. To save the list, click **OK**.

## Browsing Protection

When users visit malicious websites, some files may get installed on their systems. These files may spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious websites are blocked while the users access the Internet. Once the feature is enabled, any website that is accessed is scanned and blocked if found to be malicious.

## Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Browsing Protection**.
3. Turn **Browsing Protection** on.

Browsing Protection is activated.

## Phishing Protection

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and websites such as banks, companies and services seeking your personal information such as credit card number, social security number, account number or password.

Phishing Protection prevents the users from accessing phishing and fraudulent websites. As soon as a website is accessed, it is scanned for any phishing behavior. If found so, it is blocked to prevent any phishing attempts.

## Configuring Phishing Protection

To configure Phishing Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Phishing Protection**.
3. Turn **Phishing Protection** on.

Phishing Protection is activated.

## Safe Banking

Pay bills, transfer money online, and do banking without fear

With online banking, you can check your accounts, pay bills, buy and sell shares, and transfer money between different accounts. For doing these activities, you visit a

banking website, enter your identity credentials, and carry out the required transactions.

While visiting a banking website, you can become a prey to a fake banking website or when you type your credentials, the information can be phished to a fraudster. As a result, you may lose your money.

Safe Banking shields you from all possible situations where your identity or credentials can be compromised. Safe Banking launches your entire banking session in a secure environment that protects your vital data.

Safe Banking has the following features:

- Browser is launched in an isolated environment to prevent zero-day malware from infecting the computer.
- Your banking activity is isolated from the Internet threats.
- All types of keystroke recording tools are blocked to safeguard against key logging of confidential data.
- Employs secure DNS to prevent hacking attacks.
- Ensures that you visit only verified and secured websites.

To work in the Safe Banking environment, follow these steps:

- [Setting Safe Banking](#)
- [Launching Safe Banking](#)

## Setting Safe Banking

You can use the Safe Banking feature with the default settings. You may also configure the Safe Banking feature for enhanced security according to your requirement.

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Safe Banking**.
3. On Safe Banking, click the **Settings** icon. Select the following options as required:
  - **Protect against DNS based attacks:** Select this option to protect your system from visiting fraudulent websites. You may select a DNS network

from the given DNS list or provide an alternate ID. The network connection will be established through the configured network only.

- **Clipboard Sharing:** Select this option to allow clipboard sharing. You may allow sharing either or both from default desktop to isolated safe banking environment or other way round.
- **Keyboard Shortcut Preference:** Select this option to create a shortcut key to switch from Safe Banking desktop to Windows desktop. Safe Banking is launched in an isolated environment and hence you cannot access any system or folder from this window. Creating a shortcut key helps you to switch between Safe Banking and Windows desktop.

4. To save your settings, click **Save Changes**.

## Launching Safe Banking

You can access Safe Banking feature separately. When you install Guardian Total Security on your desktop, Safe Banking is also installed. A shortcut icon to Safe Banking is created on the desktop.

To launch a website in the Safe Banking shield, follow these steps:

1. Click the shortcut icon to **Safe Banking**. Or right-click the Guardian Total Security icon in the system tray and click **Safe Banking**.

Safe Banking is launched. You can browse the websites that you want using the supported browsers available on the task bar.

You can also bookmark a website so that you can browse such a website easily in future.

2. Click **Add Bookmark** and type the URL of the website on the Add Bookmark dialog. Click **Add**.  
You may also add a website to a category so that it is easy to search your preferred website later.
3. Click **View Bookmark** and click the URL that you want to run in the secure browser.



Note: This feature is supported on Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. This feature is not supported on Microsoft Edge browser of Windows 10 operating system.

# Firewall Protection

Firewall shields your system from intruders and hackers by monitoring and filtering incoming and outgoing network traffic. Any suspicious program that may be harmful to your computers or systems is blocked. Firewall protects your computers from malicious programs either from outside internet connection or from within networks incoming into your system.

## Configuring Firewall Protection

To configure Firewall Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Firewall Protection**.
3. Turn **Firewall Protection** on or off by using the toggle button.  
By default, Firewall Protection is turned on.
4. To set Firewall Protection, click anywhere in the Firewall Protection area.
5. To enable monitoring of unsafe Wi-Fi Networks, turn **Monitor Wi-Fi Networks** on.

If you have enabled this option and try to connect to the unsecured Wi-Fi connections, an alert will be shown. You can decide whether you want to connect to such unsecured connections.

6. To configure rules for accessing the Internet and control network traffic, set the following policies:
  - [Program Rules](#): Create rules for programs accessing the Internet.
  - [Advanced Settings](#): Create rules for incoming and outgoing network traffic.

## Program Rules

With Program Rules, you can allow or block programs from accessing the Internet.

To create rules for programs, follow these steps:

1. On the Firewall Protection screen, click the **Configure** button next to Program Rules.
2. On the Configure Program Rules screen, click the **Add** button to add a program.

Only an executable program can be added.

3. The program that you added is enlisted in the program list. Under the Access column, select **Allow** or **Deny** for accessing the network as required.
4. To save your setting, click **OK**.

### Allow only trustworthy programs

Trustworthy programs are those programs that are verified and their identity is known while untrustworthy programs are those ones that are not verified or are suspicious. Malicious programs mask their identity to run a covert operation. Such programs may be harmful to the network and computers.

You can block all untrustworthy programs from accessing the Internet by selecting the **Allow only trustworthy programs** checkbox.

### Security Level

Firewall security level includes the following:

- Low: Allows all incoming and outgoing connections.
- Medium: Monitors incoming traffic and displays the message as per suspicious behavior of an application.
- High: Monitors both incoming and outgoing traffics and displays the message as per suspicious behavior of an application.
- Block all: Blocks all incoming and outgoing connections. If you set this security level, Internet connection for all applications including Guardian Total Security will be blocked. For example, Guardian Total Security update and sending [system information](#) among other features may not work.

## Advanced Settings

To create rules for incoming and outgoing network traffics, follow these steps:

1. On the Firewall Protection screen, click the **Configure** button next to Advanced Settings.
2. On the Advanced Settings page, select the following as required:
  - **Display Alert Message:** Select this option if you want to get alert messages if connections matching exceptions rule are made for blocked outbound connections. This applies to outbound connections only.

- **Create Reports:** Select this option if you want a report to be created. You may also configure a different path to save the report.
- **Network Connections:** Using this option, set a network profile for network connections.
- **Traffic Rules:** Using this option, set rules for network traffic.

3. To save the settings, click **OK**.

### Network Connections

With Network Connections, you can set a Firewall profile for network connections. Under Network Profile Settings, you can see the following settings.

Settings	Description
Network Profile	Home: All incoming and outgoing connections are allowed except exceptions. Work: All incoming and outgoing connections are allowed except exceptions. Public: All incoming and outgoing connections are allowed except exceptions. Restricted: All incoming and outgoing connections are blocked except exceptions. Note: The logic for network profile may be changed based on your requirement. For example, if a network environment is considered less risky, you may turn stealth mode on or off. Similarly, you may allow or block sharing of the file and printer. The default setting is ideal for required security.
Stealth Mode	Enabling Stealth Mode hides the system in the network making it invisible to others thus preventing attacks.
File & Printer Sharing	Allowing this option will enable you to share file and printer between other users and you. With sharing of file and printer, the files may be accessed by unauthorized entities.

### Traffic Rules

With Traffic Rules, you can allow or block network traffic. You can add exception to allow or deny incoming and outgoing communications through IP addresses and ports.

To configure a policy, follow these steps:

1. On the Advanced Settings screen, click the **Traffic Rules** tab.

2. Click the **Add** button.
3. In the **Exception Name** text box, write a rule name and then select a protocol. Click **Next**.  
  
The protocol includes: TCP, UDP, and ICMP.
4. Under **Local IP Address**, select either **Any IP Address**, **IP Address**, or **IP Address Range**. Type the IP Address accordingly and then click **Next**.
5. Under **Local TCP/UDP Ports**, select either **All Ports**, **Specific Port(s)**, or **Port Range**. Type the Ports accordingly and then click **Next**.
6. Under **Remote IP Address**, select either **Any IP Address**, **IP Address**, or **IP Address Range**. Type the IP Address accordingly and then click **Next**.
7. Under **Remote TCP/UDP Ports**, select either **All Ports**, **Specific Port(s)**, or **Port Range**. Type the Ports accordingly and then click **Next**.
8. Under **Select Action**, select either **Allow** or **Deny**.
9. Under **Network Profile**, select either or a combination of the profile options such as **Home**, **Public**, **Work**, or **Restricted**.
10. Click **Finish**.

The following table describes the buttons and their functions.

Buttons	Description
Add	Helps you create an exception rule.
Delete	Helps you delete an exception rule from the list. Select the rule and then click <b>Delete</b> .
Up	Helps you move a rule upward to arrange according to your preference.
Down	Helps you move a rule downward to arrange according to your preference.
Default	Helps you set the rules to default settings.
OK	Helps you save your settings.
Cancel	Helps you cancel your settings and close the Advanced Settings dialog.

## IDS/IPS

With IDS/IPS, your computer remains secure from unwanted intrusion attempts or attacks by the hackers.

## Turning IDS/IPS on

To turn IDS/IPS on, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **IDS/IPS**.
3. Turn **IDS/IPS** on.

## Email Protection

With this feature, you can configure the protection rules for all incoming emails. These rules include blocking infected attachment/s (malware, spam and viruses) in the emails. You can also set an action that needs to be taken when malware is detected in the emails.

Email Security includes the following features.

- [Email Protection](#)
- [Trusted Email Clients Protection](#)

## Email Protection

This feature is turned on by default that provides optimal protection to the mail inbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection.

## Configuring Email Protection

To configure Email Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Email Protection**.
3. On the Email Protection screen, turn **Email Protection** on.

By default, Email Protection is turned on.

Protection against malware coming through emails is activated.

4. To set further protection rules for emails, click **Email Protection**.
5. Select **Display alert message** if you want a message when a virus is detected in an email or attachment.



Note: The message on viruses includes the following information: Virus Name, Sender Email Address, Email Subject, Attachment Name, and Action Taken.

6. Under **Select action to be performed when virus is found**, select **Repair** to get your emails or attachment repaired when a virus is found, or select **Delete** to delete the infected emails and attachments.



Note: If the attachment cannot be repaired then it is deleted.

7. Select **Backup before taking action** if you want to have a backup of the emails before taking an action on them.
8. Under **Attachment control settings**, select an option for blocking certain email types and attachments.
9. To save your settings, click **Save Changes**.

## Attachment Control Settings

Options	Description
Block attachments with multiple extensions	Helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
Block emails crafted to exploit vulnerability	Helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients.
Enable attachment control	<p>Helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are activated:</p> <p><b>Block all attachments:</b> Helps you block all types of attachments in emails.</p> <p><b>Block user specified attachments:</b></p> <p>Helps you block email attachments with certain extensions. If you select this option, the Configure button is activated. For further settings, click <b>Configure</b> and set the following options:</p> <ul style="list-style-type: none"> <li>Under User specified extensions, select the extensions that you want to retain so that the email attachments with such extensions are blocked and all the remaining extensions are deleted.</li> <li>If certain extensions are not in the list that you want to block, type such extensions in the extension text box and then click Add to add them in the list.</li> <li>Click <b>OK</b> to save changes.</li> </ul>

## Configuring user specified attachments

To configure user specified attachments, follow these steps:

1. On the Email Protection screen, select **Enable attachment control**.
2. Select **Block user specified attachments**.

The Configure button is activated.

3. Click **Configure**.

In the User specified extensions list, there are a number of extensions that are blocked by default. You can add more extensions, if required.

4. To add an extension, type the extension in the text list and click **Add**.
5. To remove an extension, select the extension and click **Delete**.
6. To save your settings, click **OK**.

## Trusted Email Clients Protection

Because email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.

## Configuring Trusted Email Clients Protection

To configure Trusted Email Clients Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Email Protection**.
3. On the Email Protection screen, turn **Trusted Email Clients Protection** on.
4. To add a new email client, click **Trusted Email Clients Protection**.

The Trusted Email Clients Protection details screen appears.

5. Click **Browse** and select a trusted email client
6. Click **Add** to add the email client in the list.
7. To save your settings, click **Save Changes**.

## USB Drive Protection

Whenever any external drives are connected to your system, the autorun feature starts automatically and all programs in the drive may also start. The autorun malware may also be written in the drives so that it starts as soon as the drive is connected and spreads malware to your system. This feature helps you safeguard your USB devices from autorun malware.

To configure USB Drive Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **USB Drive Protection**.

The Tools details screen appears.

3. In the Select a removable drive list, all the removable drives plugged into your system are listed. Select the drive and click the Secure Removable Drive button.

The drive will be secured against autorun malwares when used in other systems.



Tip: Guardian Total Security recommends that you always keep the autorun feature of your USB drive turned off.

---

## External Drive Protection

Whenever any external devices such as USB drives or CDs/DVDs are used with your computer, your system is at risk from the viruses and malwares that may infiltrate through the external devices. This feature allows you to set protection rules for external devices such as CDs, DVDs, and USB-based drives.

External Drive Protection includes the following features.

- [Autorun Protection](#)
- [Scan External Drives](#)

## Autorun Protection

The autorun feature of USB-based devices or CDs/DVDs tends to run as soon as such devices are attached to the computer. Autorun malware may also start with the

devices and spread malware that can cause substantial harm to the computer. This feature helps you protect your computer from autorun malware.

## Configuring Autorun Protection

To configure Autorun Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **External Drive Protection**.
3. On the External Drive Protection screen, turn **Autorun Protection** on.

Autorun Protection is activated.

## Scan External Drives

The USB-based drives are external devices that can transfer malware to your system. With this feature, you can scan the USB-based drives as soon as they are plugged in to your computer.

## Configuring Scan External Drives

To configure Scan External Drives, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **External Drive Protection**.
3. On the External Drive Protection screen, turn **Scan External Drives** on.

Scan External Drives is activated.

4. For further settings, click **Scan External Drives**.
5. Select one of the following options:
  - **Scan files on the root of the drive only:** Select this option if you want to scan the files on the root of the drive only. The files within the folders on the root drive are skipped. This scan takes little time but is less safe. By default, this option is selected.
  - **Scan full drive:** Select this option if you want to scan all the files on the USB-based drive. This scan takes time but is safer.
6. Click **Save Changes** to save your settings.



---

Tip: Scan External Drives does not work if [Data Theft Protection](#) is turned on, and its option Block complete access to external drives is selected

---

## Browser Sandbox

When you browse the Internet, you are clueless about which sites are trusted and verified. Trusted sites are those that publish their identity so that they are established as known entities. However, all untrusted sites are not fake sites or phishing sites. Untrusted websites may be commercial websites, suppliers, sellers, third parties, advertisements, and entertainment websites.

Malicious sites mask their identity to run a covert operation. These sites can hack your confidential credentials, infect your computer, and spread spam messages.

Browser Sandbox keeps you safe from any kind of malicious attacks. Browser Sandbox applies a strict security policy for all untrusted and unverified websites. If you open any downloaded files with Browser Sandbox turned on, such files open in Browser Sandbox to isolate any possible infection.

## Configuring Browser Sandbox

To configure Browser Sandbox, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Browser Sandbox**. Turn **Browser Sandbox** on.
3. From the **Browser Sandbox** security level drop-down list, select the security level.

The default setting is optimum and ideal for the novice users.

4. Select **Show border around browser window** to indicate that your browser is running in Browser Sandbox.

Note: This is not a mandatory feature for security and you may turn it off, if you prefer.

5. Select [Open the downloaded documents in sandbox environment](#)\* to open any downloaded documents in isolated environment to prevent spread of virus infection.

6. Under **Control browser access to your personal data**, set the following options as required:

- To protect your confidential data (such as bank statements, pictures, important documents) while you are surfing, select **Prevent browser from accessing confidential folders** and then select the folder that you want to protect.

The data in the confidential folder will not be accessible by the browser and other applications running under Browser Sandbox. Therefore, your data is safe from being siphoned off.

- To protect your data from being manipulated, select **Prevent browser from modifying the protected data** and then select the folder that you want to protect.

The data in the protected folder will be accessible but the data cannot be manipulated or modified.

- To download content to a certain folder while surfing, select **Allow browser to store all downloads in the specified folder** and then give the path to the folder.

This helps you download content that you need for future use to a certain folder while surfing.

7. To clean Sandbox cache, click the **Delete** button.

This helps you clean temporary files.

8. To save your settings, click **Save Changes**.



Note:

- (\*) This feature is supported on Windows 7 operating systems and later.
  - This feature is supported on Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. This feature is not supported on Microsoft Edge browser of Windows 10 operating system.
-

# Malware Protection

This feature helps you protect your system from threats such as spyware, adware, keyloggers, and riskware while you are connected to the Internet.

## Configuring Malware Protection

To configure Malware Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Malware Protection**. Turn **Malware Protection** on.

Malware Protection is enabled.

3. To set further security measures for malware protection, click anywhere on Malware Protection and then set the following options.
  - **Enable Adware detection:** If you want to detect any adware, select this option. If you enable this option, further actions to be performed are displayed.
  - **Select action to be performed when adware is found:** Select one of the following actions to be performed when any adware is detected – Prompt, Repair, Skip.

Action	Description
Prompt	If you select this option, a message will appear when an adware is detected. The message will display the following options: <ul style="list-style-type: none"><li>• <b>Allow:</b> Click this button to allow the adware to execute.</li><li>• <b>Remove:</b> Click this button to remove the adware. In case, the adware is not removed successfully, the adware is quarantined and will be cleaned in next Boot Time Scan.</li><li>• <b>Close:</b> Click this button to close the message. The same message will keep appearing until you take an action.</li></ul>
Repair	Select this option if you want to repair a file. If an adware is found in a file during scan, the file is repaired. If the file cannot be repaired, it is quarantined and will be cleaned in the next Boot Time Scan.
Skip	Select this option if you want to take no action on a file.

## Anti Malware

Guardian AntiMalware, with its improved malware scanning engine, scans registry, files and folders at a very high speed to thoroughly detect and clean spyware, adware, rogueware, dialers, riskware and lots of other potential threats in your system.

## Launching Guardian AntiMalware

You can launch Guardian AntiMalware in any of one the following ways:

- On the left pane, click **Protection** and then click **AntiMalware**.
- Right-click the Guardian Total Security product icon in the Windows system tray and select Launch Antimalware.

## Using Guardian AntiMalware

On the Guardian AntiMalware screen, click **Scan Now** to initiate the malware scan process. During scanning, Guardian AntiMalware displays the files, folders, and registry entries infected by malwares. Once the scan is complete, a list will be displayed with all the detected malwares contained in malicious files, folders, and registry entries.

You can clear specific file, folder, or registry entries from the displayed list, but ensure that all cleared items are genuine applications and not malicious ones.

In a case a malware is detected, you can take any of the following actions:

Options	Description
Clean	Helps you clean the malwares and its remains from the system. If you clear the specific file, folder or registry entry, you are prompted whether you want to exclude those items in future scan. If you want to permanently exclude those items, click <b>Yes</b> , otherwise click <b>No</b> for temporary exclusion.
Skip	Helps you to skip taking any action against malwares in your system.
Stop Scan	Helps you stop the scan.
Set System Restore point before cleaning	Helps you create System Restore point before the cleaning process starts in your system. This helps you revert to the cleaning done by Guardian AntiMalware by using Windows System Restore facility.  Note: The feature <b>Set System Restore point before cleaning</b> is not available in Windows 2000 operating system.
Details	Helps you redirect to the website of <a href="#">Guardian</a> .

## Anti Rootkit

This feature helps you proactively detect and clean rootkits that are active in the system. This program scans objects such as running Processes, Windows Registry, and Files and Folders for any suspicious activity and detects the rootkits without any signatures. Anti-Rootkit detects most of the existing rootkits and is designed to detect the upcoming rootkits and also to provide the option to clean them.

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

## Using Guardian Anti-Rootkit

To use Anti-Rootkit, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Anti-Rootkit**.

A message appears that recommends you to close all other applications before launching Anti-Rootkit.

3. In the left pane on the Anti-Rootkit screen, click the **Start Scan** button.

Guardian Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry and Files and Folders.

After completion of the scan, the result is displayed in three tabs.

4. Select the appropriate action against each threat displayed. For example, you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.

After taking the action, you should restart your system so that rootkit cleaning takes place.

Buttons	Description
Stop Scanning	Helps you stop the scan while the scan is under way.
Close	Helps you close the Anti-Rootkit window. If you choose to close the Anti-Rootkit window while scanning is in progress, it will prompt you to stop the scan first.
Error Report Submission	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 the Settings feature available on the Anti-Rootkit screen, you can configure what items to scan.

## Configuring Guardian Anti-Rootkit Settings

1. Open **Guardian Total Security**.
2. On the left pane, click **Protection** and then click **Anti-Rootkit**.

Guardian Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.

Scan Options	Description
Auto Scan	Auto Scan is the default scan setting for Anti-Rootkit. Under Auto Scan, the Guardian Anti-Rootkit scans the predefined system areas such as: <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>
Custom Scan	Helps you customize the scan setting for Anti-Rootkit for the following options:
	<b>Detect Hidden Process</b> – scans the hidden processes running in the system.
	<b>Detect Hidden Registry Items</b> – scans the hidden items in Windows Registry.
	<b>Detect Hidden files and folders</b> – scans the hidden files and folders in the system and executable ADS (Alternate Data Streams). You can further choose from the following options: <ul style="list-style-type: none"> <li>• Scan drive on which Operating System is installed</li> <li>• Scan all fixed drives</li> <li>• ADS (Alternate Data Streams) to scan for executable ADS.</li> </ul>
Report File Path	Guardian Anti-Rootkit creates a scan report file at the location from which it is executed. However, you can specify a different location.

## Overview of Alternate Data Streams – ADS

Alternate Data Streams or ADS allows the data to be stored in hidden formats 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. ADS is a security risk because streams are almost completely hidden.

Trojan or virus author can take advantage of streams to spread malware so to hide the source of viruses.

## Scanning Results and Cleaning Rootkits

1. Open **Guardian Anti-Rootkit**.
2. In the left pane on the Guardian Anti-Rootkit screen, click the **Start Scan** button.
3. Guardian Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry and Files and Folders.

After completion of the scan, the result is displayed in three different tabs.

Take the appropriate action. You need to restart your system so that rootkit cleaning takes place.

### Tabs that appear on the Scan Results screen

Options	Description
Process	After the scan is complete, Guardian Anti-Rootkit will detect and display a list of hidden processes. You can select the Process tab for termination, but ensure that the list of processes does not include any known trusted process. Guardian Anti-Rootkit also displays a summary of total number of processes scanned and hidden processes detected.
Terminating Hidden Process	After selecting the list of processes to close, click the Terminate button. If a process is successfully terminated, then its PID (Process Identifier) field will show n/a and process name is appended by Terminated. All terminated Processes will be renamed after a restart.
Registry	Similar to the Process scan, Guardian Anti-Rootkit displays a list of hidden Registry keys. You can select keys for renaming, but ensure that the list of keys does not include any known trusted registry key. Guardian Anti-Rootkit also displays a summary of total number of items scanned and number of hidden items detected.
Renaming Hidden Registry Key	After selecting the list of keys for renaming, click the Rename button. Renaming of operation requires reboot hence Key name will be prefixed by Rename Queued.
Files and Folders	Similarly, Guardian Anti-Rootkit displays a list of hidden files and folders. You can select the Files and Folders tab for renaming, but ensure that the list of Files and Folders does not include any known trusted file.

Options	Description
	Guardian Anti-Rootkit also displays a list of executable Alternate Data Streams. Guardian Anti-Rootkit also displays a summary of total number of files scanned and number of hidden files detected.
Renaming Hidden Files and Folders	After selecting the list of files and folders for renaming, click the Rename button. Renaming of operation requires reboot hence Files and Folders name will be prefixed by Rename Queued.

## Cleaning Rootkits through Guardian Emergency Disk

Sometimes rootkits are not cleaned properly and they reappear even after Guardian Anti-Rootkit scan. In such cases, you can also use Guardian Emergency Disk for complete cleaning. For cleaning this way, create Guardian Emergency Disk and boot your system through it.

To create Guardian Emergency Disk and clean your system through it, follow these steps:

### Step 1

To create Guardian Emergency Disk, follow the link [Create Emergency Disk](#), p - 75.

### Step 2

1. Open **Guardian Anti-Rootkit**.
2. In the left pane on the Guardian Anti-Rootkit screen, click the **Start Scan** button.  
  
Guardian Anti-Rootkit starts scanning your system for suspicious rootkit activity in the running Processes, Windows Registry, and Files and Folders. After the scan is complete, the scan result is displayed in three different tabs.
3. Take the appropriate action against each threat displayed. For example, you can terminate the rootkit process or rename the rootkit registry entry or files.

### Step 3

1. Boot your system using **Guardian Emergency Disk**.
2. Guardian Emergency Disk will automatically scan and clean the rootkits from your system.

## 5. Privacy

---

In the age of digital environment, privacy of data and personal identity has become most important for everyone. There are various sources from where hackers and fraudsters can steal valuable data and manipulate the things.

Privacy section includes those features that allow you to secure data, personal information, and privacy. Privacy includes the following features.

[Data Backup](#)

[Manage Backup](#)

[Restore Backup](#)

[Registry Restore](#)

[Data Theft Protection](#)

[Screen Locker Protection](#)

[Anti-Keylogger](#)

### Data Backup

#### Take a backup of your data to avoid data loss

Using Data Backup, you can take a backup of any kind of data you prefer. Taking a backup of the data is required for protection against [ransomware attacks](#). If any ransomware attacks happen, you can restore the backed up data.

### Turning Data Backup on

To turn Data Backup on, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Data Backup**. Turn **Data Backup** on. Data Backup is turned on by default.

3. To configure what data you should save and where, click anywhere on the **Data Backup** feature. Specify the location to save data and select the types of files you want to save under **Select types of files to back up**.
4. To change the backup location, click **Change Location**.

A message appears that cautions that the data backed up till date will be moved to the changed location and the new backup of the data will be saved on this new location from now.

5. Click **Select Location** and then browse a location. Click **OK**.
6. Click **Move**.

The data is moved successfully.

Under [Select types of files to backup](#), you can enlist the file extensions that you want to back up or even add the file extensions in the exclusion list not to take their backup.

## Select types of files to backup

The backup files list includes three file categories: default, custom, and user specified. Data of the default file category is saved without fail. In order to back up the data from the custom category, you need to keep the file categories selected.

In user specified category, you can add the file extensions for which you want backup or exclude certain file extensions of which you do not need backup. Be careful while excluding any file extensions as these data will not be backed up.

To add or exclude file extensions, follow these steps.

1. On the [Data Backup](#) screen, select **Select types of files to backup > Advanced**.
2. Click **Configure**.

The file categories list appears. This list includes the following file categories.

**Default file type:** You cannot edit the default file types. Data of these files are backed up without fail.

**Custom file type:** In order to back up the data, you must keep the file categories selected. If you do not select the file categories, the data will not be saved.

**User specified file type:** Displays the file extensions that have been added or excluded.

3. To exclude file extensions, select **User Excluded Files** and click **Exclude Extension**. Enter the file extensions and click **OK** to save the entries.

The entries will be displayed under **User specified file type**. After enlisting the entries, you must select the **User Excluded Files** to exclude saving the backup of the listed extensions.

4. To include file extensions, select **User Specified Files** and click **Add Extension**. Enter the file extensions and click **OK** to save the entries.

The entries will be displayed under **User specified file type**. After enlisting the entries, you must select the **User Specified Files** to back up the data of the listed extensions.

## Manage Backup

Using Manage Backup, you can delete the [backed up data](#) or copy the backed up data from the current backup location to a different location. You may change the backup location if you do not have enough space on the current location.

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Data Backup**. To configure backup, click **Manage Backup**.

If you do not need the backed up data, you may delete the backup to free the disk space.

3. To delete the backup, click **Delete**. A warning message appears. Read the message carefully. To confirm deletion, click **Yes**.
4. To copy the backed up data, click **Select Location** and then browse a location. Click **OK**.

A message appears. The data that is copied from the protected location to another location will not be protected. The new data will continue to be backed up at the protected location.

5. Click **Copy**.

The data is copied successfully.

## Restore Backup

Using Restore Data, you can restore the backed up data in case any [ransomware attacks](#) happen. It is important that you [back up your data](#) to avoid any ransomware attacks.

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Restore Backup**.
3. To restore backup, click **Restore Backup**.

Two options **From System** and **From Other Sources** appear. With **From System**, you can restore data from current backup location on your computer while with **From Other Sources**, you can restore data from any other location where the backup is available.

4. Select **From System**, if you want to restore data from current backup location and then select a version. Click **Next**.
5. Click **Select Location** and browse a location on your computer. Click **OK** and then click **Next**.
6. Select **From Other Sources**, if you want to restore data from any other location where the backup is available. Click **Select Location** and then browse a location on your computer. Click **OK** and then click **Next**.

The data is restored successfully.

## Registry Restore

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 the Control Panel settings, or File Associations, System Policies, or install new software, the changes are reflected and stored in the Registry. Malware usually targets the system Registry to restrict specific features of the operating systems or other applications. It may modify the system registry so that it behaves in a manner beneficial to malware creating problem to the system.

The Registry Restore feature restores the critical system registry area and other areas from the changes made by malware. It also repairs the system registry.

## Configuring Registry Restore

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Registry Restore**.
3. Select **Restore critical system registry areas** to restore the critical system registry during the scan. Critical System Registry areas are generally changed by malware to perform certain task automatically or to avoid detection or modification by system applications such as Disabling Task Manager, and Disabling Registry Editor.
4. Select **Repair malicious registry entries** to scan system registry for malware related entries. Malware and its remains are repaired automatically during the scan.

## Data Theft Protection

### Prevent copying of data from your computer to a drive

With Data Theft Protection, you can block transfer of the data between the system and USB drives and CD/DVD devices. Data Theft Protection ensures no files or data can be copied from your system to any external drives or devices. Similarly no files or data can be transferred from the USB drives and CD/DVD devices to your system. Hence neither your information can be theft nor can any harmful files be implanted in your system.

This feature allows you to block transfer of the data between the system and external devices such as USB drives and CD/DVD devices. Data Theft Protection ensures no files or data can be copied from your system to any external devices or vice versa. It ensures data security and also eliminates the possibility of transfer of any harmful files.

## Configuring Data Theft Protection

To configure Data Theft Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Data Theft Protection**.

3. Turn **Data Theft Protection** on.

Data Theft Protection is activated.

4. Click **Data Theft Protection** and do any of the following options:

- **Read only and no write access to external drives:** Allows transfer of data from the USB drives and CD/DVD devices to the system but not vice versa. By default, this option is selected.
- **Block complete access to external drives:** Blocks transfer of data between the system and all external devices.
- **Authorize USB drive and Mobile devices:** Select this option if you want to allow access only to the authorized USB drives and mobile devices. If this option is selected, and you connect a USB drive or a mobile device to your system, you are prompted for password to access them. Hence access is granted only to the authorized devices.

This option will work only if Data Theft Protection and [Password Protection](#) are turned on.

- **Block Mobile devices:** Blocks complete access to mobile devices.

5. To save your settings, click **Save Changes**.

## Screen Locker Protection

Malicious programs that lock the screen preventing access to your computer are known as screen lockers. With Screen Locker Protection, you can create a short-cut key combination to initiate a clean-up of your computer and remove such malicious programs. By pressing the short-cut key, you can initiate cleaning up of your computer and remove the malicious program.

## Configuring Screen Locker Protection

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Screen Locker Protection**.
3. To enable Screen Locker Protection, select **Protect from screen lockers**. By default, this option is selected.
4. Select an alphabet from the drop-down list to create a short-cut combination with **Ctrl+Alt+Shift**. Here **A** is selected by default.

5. Click **Save Changes**.



---

Note: You have to restart your computer at least once after you install the product to activate this feature.

---

## Anti-Keylogger

Keyloggers are malicious programs that record all information typed by you on the keyboard of your computer or laptop and share that information with the hackers. You may lose confidential information such as usernames, passwords, or PIN to the hackers. Anti-Keylogger helps you prevent information getting recorded by keystroke logger malware.

### Configuring Anti-Keylogger

1. Open **Guardian Total Security**.
2. On the left pane, click **Privacy** and then click **Anti-Keylogger**.
3. Turn **Anti-Keylogger** on or off as you prefer.

## 6. Performance

---

When you work on your computer, you may be busy in serious activities and you wish not to be distracted by notifications for various functions in your computer system. For example, when you are playing any game, you want all processes to be suppressed so the speed is not compromised. You can take advantage of Auto Silent Mode or Game Booster.

Performance section includes those features that help you to improve performance of your computer, clean browsing history, and boost gaming experience.

Performance includes the following features.

[Auto Silent Mode](#)

[Track Cleaner](#)

[Hijack Restore](#)

[System Explorer](#)

### Auto Silent Mode

With Auto Silent Mode, you can keep your antivirus running in the background but no notifications or pop-ups are displayed. Any scheduled scan is also deferred to the next schedule until Auto Silent Mode is turned off, if any application is running in full screen mode.

#### Turning Auto Silent Mode on

To turn Auto Silent Mode, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Performance** and then click **Auto Silent Mode**. Turn **Auto Silent Mode** on.

By default, Auto Silent Mode is turned on.

## Track Cleaner

Most of the programs store the list of recently opened files in their internal format to help you open them again for quick access. If a system is used by more than one user, the user's privacy may be compromised. Track Cleaner helps you remove all the tracks of such most recently used (MRU) programs and prevent privacy breach.

### Using Track Cleaner

To use Track Cleaner, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Performance** and then click **Track Cleaner**.

The Track Cleaner screen appears. This displays a list of all the programs opened recently.

3. Select the programs whose traces you want to remove or select **Check All** to select all the programs in the list.
4. To initiate cleaning, click **Start Cleaning**.
5. To close the Track Cleaner window, click **Close**.

## Hijack Restore

If you have modified the default settings of Internet Explorer or if the settings have been modified by malwares, spywares, and sometimes genuine applications, you can restore the default settings. This feature helps you restore the settings of Internet Explorer browser, and also of critical operating system settings such as Registry Editor and Task Manager.

### Using Hijack Restore

To use Hijack Restore, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Performance** and then click **Hijack Restore**.
3. On the Hijack Restore screen, select **Check All** to select all the browser settings in the list.
4. Select **Restore default host file** to restore the default host file.

5. Select **Restore important system settings** to restore important system settings.
6. To initiate restoring your settings, click **Restore Now**.

## Restore Default Host File

The default host file includes the following options.

Fields	Description
IP Address	Enter the IP Address of the host.
Host Name	Enter the host name.
Add	Click <b>Add</b> to add the host details in the list.
Edit	Select the host in the list and click <b>Edit</b> to make the changes.
Delete	Select the host in the list and click <b>Delete</b> to remove the host.
OK	Click <b>OK</b> to save your setting for the host files and exit from the Host Specification window.
Close	Click <b>Close</b> to exit without saving your settings from the Host Specification window.

## Restore important system settings

The restore important system settings option includes the following options.

Options	Description
Check All	Helps you restore all the system settings in the list.
OK	Helps you save all the modified settings and exit from the Important System Settings window.
Close	Helps you exit without saving the settings, from the Important System Settings window.

The buttons on the Hijack Restore screen are as follows.

Buttons	Description
Restore Now	Helps you initiate restoring the settings that you selected.
Undo	Helps you undo your settings done on the current screen. If you click the <b>Undo</b> button, it opens a window Undo Operations. The settings which have been restored to default settings will be listed. Select your settings or <b>Check All</b> to select all the settings. Click <b>OK</b> to revert to the existing settings.

Close	Helps you exit from the Hijack Restore window without saving your settings.
-------	---

## System Explorer

This tool provides you all the important information related to your computer such as running process, installed BHOs, toolbars installed in Internet Explorer, installed ActiveX, Hosts, LSPs, Startup Programs, Internet Explorer settings and Active network connection. This helps you diagnose the system for any new malware or riskware.

## Using System Explorer

To use system explorer, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Performance** and then click **System Explorer**.

On the System Explorer screen, you can select a process, tool, program or any other processes that you want to analyze. Based on the selection, you can select a process and view its description. You can terminate any process that you think so.

## 7. Settings

---

Settings section includes those features that allow you to configure Internet connection, create emergency disk, and other settings.

### Configure these settings to ensure enhanced security

Settings includes the following features.

[Automatic Update](#)

[View Quarantine Files](#)

[Report Settings](#)

[Report Virus Statistics](#)

[Restore Default Settings](#)

[Password Protection](#)

[Security Updates](#)

[Internet Settings](#)

[Self Protection](#)

[Create Emergency Disk](#)

[Import/Export Settings](#)

### Automatic Update

This feature helps you take the updates of the latest virus signatures automatically. It is advisable that you keep your Guardian Total Security up-to-date for protection against new and unknown malwares and viruses.

To take the updates regularly, ensure the following conditions.

1. You must always keep the **Automatic Update** turned on.
2. You must set an update mode to take the updates.

## Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Automatic Update**. Turn **Automatic Update** on.  
  
By default, Automatic Update is turned on.
3. To configure about how to take the updates, click the setting icon of **Automatic Update**.
4. Select **Show update notification window**, if you want to get notified about the update of Guardian Total Security. By default, this option is turned on.
5. Select the update mode from the following options:
  - **Download from Internet** – Helps you download the updates to your computer from the Internet.
  - [Pick update files from specified path](#) –Helps you pick the updates from a local folder or a network folder.
6. Select other options.
  - [Copy update files to specified location](#) – Helps you save a copy of the updates on a local drive of your computer.
  - Check for the latest version of Guardian Total Security:
    - **Notify me when upgrade is available**: Select this option if you want to be notified when there is a new upgrade available.
    - **Automatically download the upgrade**: Select this option if you want a new upgrade when available get downloaded automatically on your system. Then you need to install it to upgrade your current version.
7. To save your settings, click **Save Changes**.

## Selecting Update Mode

Guardian Total Security provides multiple update modes that you can select according to your convenience.

### Pick update files from specified path

Picking the updates is helpful in two ways.

1. Single computer: If your computer where Guardian Total Security is installed is not connected to the Internet.
2. Multiple computers: You can download the updates on a single computer to save the Internet bandwidth and pick up the updates for all computers in the network.

To pick the updates automatically, ensure the following things.

1. Select **Pick update files from specified**.
2. Browse a path to the drive on your computer or any other computer in the network.
3. To save your setting, click **Save Changes**.

### Copy update files to specified location

Whenever Guardian Total Security is updated with new virus database signatures, one version of the update is saved at the location that you specify here. This is helpful in case there is any technical issue or the antivirus crashes because of new update. You can roll back to the previous version easily.



---

Note: To save the update at this location, you must keep this option selected.

---

## View Quarantine Files

This feature helps you safely isolate the infected or suspected files. When a file is quarantined, Guardian Total Security encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted format, these files cannot be executed and hence are safe. Quarantine also keeps a copy of the infected file before repairing. You can take a backup of the files also before taking an action.

### Launching Quarantine Files

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **View Quarantine**.

A list of all quarantined and backed up files is displayed.

You can perform the following tasks on the Quarantine dialog:

Buttons	Description
Submit for Analysis	Helps you send a quarantined file to the Guardian research labs for analysis. We will analyze the file and create an appropriate solution in future.
Add	Helps you quarantine a file manually.
Restore	Helps you restore a quarantined file to its original location. When you find a quarantined file trustworthy and try to restore it, an option for adding the file to the exclusion list appears. You can add the file to the exclusion list so that the same file is not treated as suspected and quarantined again.
Delete	Helps you delete a quarantined file. Select a quarantined file and click <b>Delete</b> .
Delete All	Helps you delete all the quarantined files at one go.

## Report Settings

Reports on all activities of the Guardian Total Security product are generated. You can use these reports to verify what all activities are going on such as whether your computer has been scanned, any malware has been detected, or any blocked website has been visited.

Such reports keep on adding up in the report list. You can set the rule when these reports should be removed automatically. The default setting for deleting reports is 30 days. You can also retain the reports if you need them.

### Configuring Report Settings

To configure Report Settings, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Report Settings**.

The Report Settings screen appears.

3. Select **Delete reports after**, and then select the number of days after which the reports should be removed automatically.

If you clear **Delete reports after**, no reports will be removed.

4. To apply the settings, click **Save Changes**.

## Report Virus Statistics

This feature helps you submit the virus detection statistics report generated during scans to the Guardian Research Center automatically.

### Configuring Report Virus Statistics

To configure Report Virus Statistics, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Report Virus Statistics**. Turn **Report Virus Statistics** on.

The Report Virus Statistics is activated.

## Restore Default Settings

This feature allows you to revert the settings customized by you to the default settings. This is very helpful when you change the default settings but you are not satisfied with the protection or you feel your protection is being compromised. You can restore the system default settings.

### Restoring Default Settings

To restore default settings, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Restore Default Settings**.
3. On the Restore Default Settings, click the **Default All** button.

Your Guardian Total Security is reverted to the default settings.

## Password Protection

This feature allows you to restrict unauthorized people from modifying the Guardian Total Security settings so that your security is not compromised. It is recommended that you always keep Password Protection turned on.

## Safe Mode Protection

If you run Windows in Safe Mode, your computer starts with only basic files and drivers and the security features of Guardian Total Security are disabled by default. In such a situation, unauthorized users may take advantage and steal data or modify the settings of the Guardian Total Security features.

To prevent access to your system by any unauthorized users, you can configure Safe Mode Protection. Once you configure it, you need to provide a password to work in Safe Mode.

## Configuring Password Protection

To configure Password Protection, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Password Protection**. Turn **Password Protection** on.

The Password Protection feature is turned off by default.

3. In **Enter password**, enter a new password if you are setting the password for the first time, and then enter the same password in **Confirm password**.

If you are setting the password for the first time, then **Enter old password** will not be available.

4. To enable safe mode protection, select [Enable Safe mode protection](#).
5. Click **Save Changes**.

## Security Updates

With this feature, you get the latest updates about cyber security, virus threats and alerts and other important information related to the computer protection. The latest news is also available on the dashboard of Guardian Total Security. If you do not want to get the security updates, turn Security Updates off.

## Turning Security Updates off

To turn Security Updates off, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Security Updates**.

3. Turn **Security Updates** off.

## Internet Settings

This feature helps you turn proxy support on, set proxy type, configure IP address, and port of the proxy for using Internet connection. If you are using a proxy server on your network, or Socks Version 4 & 5 network, you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Internet settings. If you configure the Internet Settings, you have to enter your user name and password credentials.

The following Guardian Total Security modules require access to the Internet and may depend on the settings configured.

- Registration Wizard
- Quick Update
- Messenger

## Configuring Internet Settings

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Internet Settings**.
3. Click **Internet Settings** and select **Enable proxy settings**.

The proxy type, server, port, and user credentials text boxes are activated.

4. In **Type** list, select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.
5. In the **Server** text box, enter the IP address of the proxy server or domain.
6. In the **Port** text box, enter the port number of the proxy server.

Port number is set as 80 for HTTP and 1080 for SOCKS V4, SOCKS V5 by default.

7. Enter your user name and password credentials.
8. To save your settings, click **Save Changes**.

## Self Protection

This feature helps you protect Guardian Total Security so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way. It also protects the processes and services of Guardian Total Security. It is recommended that you always keep Self Protection on. By default, this option is turned on.

### Configuring Self Protection

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then **Self Protection**.
3. Turn **Self Protection** on.

By default, Self Protection is turned on.

## Create Emergency Disk

You can create your own emergency bootable Disk that will help you boot your Windows computer system and scan and clean all the drives including NTFS partitions. This Disk helps in cleaning badly infected system from the files infecting viruses that cannot be cleaned from inside Windows.

The Emergency Disk will be created with the latest virus signature pattern file used by Guardian Total Security on your system.

To create an Emergency Disk, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click **Create Emergency Disk**.
3. On the Create Emergency Disk screen, click the link and download the required package for emergency tool.
4. Extract the downloaded package on your system. For example: `c:\my documents\qhemgpkg`.
5. Provide the extracted package path, and click **Next**.
6. To create Emergency Disk, select any one of the options that are displayed on the screen. For example, select either Create Emergency USB disk or Create Emergency CD/DVD.

Note: Creating Emergency Disk using CD/DVD is not supported on Microsoft Windows 2003 and earlier versions. However, you can create Emergency Disk on USB drives.

7. Select the disk drive to be converted to an Emergency Disk and click Next.

On successful creation of an Emergency Disk, a message is displayed.

### Things to remember while creating an Emergency Disk

- It is recommended that you retain a copy of the extracted package on your system.
- While using a USB device, rewritable CD/DVD, take a backup as the device will be formatted.
- To boot the system from either USB or CD/DVD, you have to set Boot sequence in BIOS.
- Once the scan is complete, you must remove the Emergency USB disk or CD/DVD before restarting the computer, otherwise it will again boot in the boot shell.

### Using Emergency Disk

1. Insert **Emergency Disk** in your CD/DVD/USB drive.
2. Restart your system.
3. Emergency Disk starts scanning all the drives automatically. It will disinfect the infection, if found.
4. Restart your system.

## Import/Export Settings

This feature allows you to import and export the settings of Guardian Total Security features. If you need re-installation or have multiple computers and want the same settings, you can simply export the settings configured on your current computer and easily import them on the computers. Both the default settings and the settings made by you can be exported.

### Importing and Exporting the Guardian Total Security Settings

To import or export the Guardian Total Security settings, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click **Settings** and then click the **Import** or **Export** tab.
  - **Import:** Helps you import the settings from a .dat file.  
While you import the settings, a caution **This will overwrite all settings that you have configured.** appears. To confirm importing, click **Yes**.
  - **Export:** Helps you export the current settings to a .dat file.
3. Upon successful export or import, a message appears. Click **OK** to close the Import or Export dialogue.



---

### Note:

---

- The settings can be imported from the same product flavor and the same version only. For example, the settings of Guardian Total Security Pro version 19.00 can be imported to Guardian Total Security Pro version 19.00 only.
  - The settings of Scheduled Scans and Password Protection cannot be exported or imported:
-

## 8. More option

---

The More section includes the following options.

Options	Description
Product Guide	You can access to our complete user manual to know about all the features that are present in our product and how to configure them.
<a href="#">Reports</a>	Helps you to view reports on various incidents.
<a href="#">Submit System Information</a>	Helps you submit technical issue that your computer faces for which you could not find a solution. Guardian Total Security will analyze the issue and share the solution with you.
<a href="#">Support</a>	Includes all sources of support that Guardian Total Security provides.
<a href="#">About</a>	Includes the information related to the antivirus product license.
Help option	<p>Includes a Help guide to know about all the features that are present in our product and how to configure them.</p> <p>Our Help is context sensitive that means you can open Help by pressing <b>F1</b> for quick access wherever you are in the antivirus product.</p>

## 9. Help & Other Recommendations

---

Updates for Guardian Total Security are released regularly. These updates may include enhancements or security features against new malwares and viruses. To prevent your computer from new viruses, you must always keep Guardian Total Security up-to-date.

### Keep Guardian Total Security updated to be safe from new viruses

The default setting of Guardian Total Security is configured to take the updates automatically from the Internet, without the intervention of the user. However, your system must be connected to the Internet to get the updates regularly.



---

Note:

---

- The updates may include enhancements and new virus database signatures against new malwares and viruses.
  - The updates may upgrade your current version of Guardian Total Security to the new version.
- 

You can update Guardian Total Security [online](#) and [offline](#) as per your preference.

### Updating Guardian Total Security online

Although, the default setting of Guardian Total Security is configured to take the updates automatically from the Internet. With Update Now, you can update Guardian Total Security manually whenever you prefer.

To update Guardian Total Security online, follow these steps.

1. Right-click the Guardian Total Security icon on the system tray and select **Update Now**.

Alternatively, open **Guardian Total Security**. On the left pane, click the **More** option and then select **About**. On the About screen, click the **Update Now** button.

Quick Update starts updating.

2. On completion of updating, click **Finish**.

Note: Quick Update connects to the website of [Guardian](#), downloads the appropriate updates, and applies the updates.

## Updating Guardian Total Security offline

You can update Guardian Total Security without connecting to the Internet. Updating offline is useful if your computer where Guardian Total Security is installed is not connected to the Internet or you have several computers. You do not need to download the update on all the computers in the network.

To update Guardian Total Security offline, follow these steps.

1. Go to <http://www.guardianav.co.in/update>.
2. On the Guardian Total Security Offline Product Updates portal, enter the required information about your product version, operating system architecture, and the type of updates.
3. Click the **Download** button.
4. Double-click the downloaded file.

The Guardian Total Security Updater wizard appears.

5. Click **Update Now**.

Alternatively, you can click the **Extract the updates** link and browse to the folder where you want to save the update. Once the update is saved, you can go to the folder and apply the update manually.

You can select **Install Updates after extraction** and then click **Continue** to apply the update automatically.

Your antivirus is updated successfully.

## Update Guidelines for Network Environment

If you are using multiple computers with Guardian Total Security installed, you can configure a server to provide hassle free updates to all computers in your network. You are suggested to follow these guidelines for best results.

1. Set up one computer (may be the server) as the master update machine. Suppose server name is SERVER.
2. Make a folder named as **GTSUPD** on a local drive in your computer. For example: **C:\GTSUPD**. Assign Read-only sharing right to this folder.
3. Open **Guardian Total Security**.
4. On the left pane, click **Settings** and then click **Automatic Update**. Turn **Automatic Update** on.  
Automatic Update is activated.
5. Click the setting icon for Automatic Update.
6. Select **Copy update files to specified location**.
7. Browse the **GTSUPD** folder and click **OK**.
8. To save your settings, click **Save Changes**.
9. On all user computers within the network launch **Guardian Total Security**.
10. Under **Settings**, go to the **Automatic Update** page.
11. Select **Pick update files from specified path** and click **Browse**.
12. Locate the `SERVER\GTSUPD` folder from Network Neighborhood.  
Alternatively, you can type the path as `\\SERVER\GTSUPD`.
13. To save your settings, click **Save Changes**.

## Cleaning Viruses

Guardian Total Security warns you of a virus infection when:

- A virus is encountered during a manual scan.
- A virus is encountered by Guardian Virus Protection/Email Protection.

### Cleaning viruses encountered during scanning

The default settings of Guardian Total Security are adequately configured and are optimum to protect your system. If a virus is detected during scanning, Guardian Total Security tries to repair the virus. If it fails in repairing the infected files, such files are quarantined. In case you have customized the default scanner settings, take an appropriate action when a virus is found.

### Scanning Options

During scan, you can take any of the following actions as per requirement.

Buttons	Description
Action Tab	Displays the action taken on the files.
Skip Folder	Helps you avoid scanning the current folder. Scanning moves to other location. This option is useful while scanning a folder that contains non-suspicious items.
Skip File	Helps you avoid scanning the current file. This option is useful while scanning an archive of a large number of files.
Stop	Helps you stop the scanning process.
Close	Helps you exit from the scanning process.
Shut down PC when finished	Helps you shut down your system after finishing the scan. This feature will work only when the scan is complete.

### Cleaning virus detected in memory

“Virus Active in memory” means that a virus is active, and is spreading to other files or computers (if connected to a network) and doing malicious activity.

Whenever a virus is detected during memory scan, a Boot Time Scan is automatically scheduled to run the next time you boot your system. Boot Time Scan will scan and clean all drives including NTFS partitions before the desktop is completely loaded. It will detect and clean even the most typical Rootkits, spywares, special purpose Trojans, and loggers.

### Restart required during cleaning for some malwares

Some malwares drop and inject their dynamic link libraries in the running processes of the system such as explorer.exe, Iexplore.exe, svchost.exe, etc. which cannot be disabled or cleaned. During memory scan when they are detected, they will be set

for deletion in the next boot automatically. Guardian Total Security memory scan will provide details or action recommendation for you in such cases.

### Cleaning of Boot/Partition viruses

If Guardian Total Security memory scanner detects a boot or partition virus in your system, it will recommend you to boot your system using a clean bootable disk. It will scan and clean the virus using the Guardian Emergency disk.

### Responding to virus found alerts from Virus Protection

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

## About antivirus license

The About section of Guardian Total Security includes the following information.

- Guardian Total Security Version
- License details
- License validity
- Update Now option

The following buttons are available in the About section.

Options	Description
Renew Now	Helps you renew your existing subscription.
License Details	<p>License Information and End-User License Agreement (EULA) are available under this section.</p> <p><b>Update License Details:</b> This feature is useful to synchronize your existing License information with Guardian Total Security Activation Server.</p> <p>To update your license information, follow these steps:</p> <ol style="list-style-type: none"><li>1. Open <b>Guardian Total Security</b>.</li><li>2. On the left pane, click the More option and select the <b>About</b> menu.</li><li>3. On the About screen, click <b>License Details</b>.</li><li>4. Click <b>Update License Details</b> and then click <b>Continue</b>.</li></ol> <p><b>Print License Details:</b> Click Print License Details to take the print of the existing subscription information.</p>

Options	Description
Update Now	Helps you update virus database of Guardian Total Security.

## Submitting System Information

System Information is an essential tool to gather critical information of a Windows-based system for the following cases.

<b>To detect new Malwares</b>	This tool gathers information to detect new malwares from the Running processes, Registry, System files like Config.Sys, Autoexec.bat, and system and application event logs.
<b>To get Guardian information</b>	It gathers information of the installed version of Guardian Total Security, its configuration settings and Quarantined files, if any.

## Generating System Information

To generate system information, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click the More option and then select the **Submit System Information** option.  
  
The System Information wizard opens.
3. Click **Next** to continue.
4. Select a reason for submitting the system information. If you are suspecting new malware in your system, select **I suspect my system is infected by new Malwares** or if you are facing issues while using Guardian Total Security, select **I am having problem while using Guardian**. Provide comments in the **Comments** text box and also enter your email address.
5. Click **Finish**.

System Information (INFO.QHC) will be generated and sent to our Technical Support.

This tool generates an INFO.QHC file at C:\ and submits it automatically to [support@guardianav.co.in](mailto:support@guardianav.co.in).



Note: INFO.QHC file contains the critical system details and version details of Guardian Total Security installed on your system in the text and binary format.

The 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 malware and proper functioning of Guardian Total Security. This information is used to provide better and adequate services to customers.

Please note that this tool does not collect any other personally identifiable information such as passwords, nor do we share or disclose this information with anyone. We respect your privacy.

---

## Reports

Guardian Total Security creates and maintains a detailed report of all important activities such as virus scan, updates details, changes in settings of the features, and so on.

### Viewing Reports

To view reports and statistics of different features, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click the More option and then select the **Reports** option.  
A Reports list appears.
3. In the **Reports for** list, click a feature to view its report.

The report details list appears in the right pane. The report statistics on each feature includes Date and Time when the report was created and the reason for which the report was created.

Buttons	Action
Details	Helps you display a detailed report of the selected record in the list.
Delete All	Helps you delete all the records in the list.
Delete	Helps you delete the selected record in the list.
Close	Helps you close the Reports screen.

You can view further details of a report of a feature. In the right pane, click the report to view the details. The report details screen appears that includes the following options.

Button	Action
Prev	Helps you display the detailed report of the previous record in the list. This button is not available if the selected record is the first record in the list.
Next	Helps you display the detailed report of the next record in the list. This button is not available if the selected record is the last record in the list.
Print	Helps you take the print of the detailed report.
Save As	Helps you save the detailed report in .txt format in a location of your system.
Close	Helps you exit from the report details screen.

## Uninstalling antivirus software

Removing Guardian Total Security may expose your system to virus threats. However, you can uninstall Guardian Total Security in the following way:

1. Select **Start > Programs > Guardian Total Security<sup>#</sup> > Uninstall Guardian Total Security**.

- **Remove Guardian and keep update definitions files** - If you select this option, Guardian will save license information, all downloaded update definitions, reports, quarantined files, anti-spam whitelist/blacklist in a repository on your computer, so that these can be used during reinstallation.
- **Remove Guardian completely** - If you select this option, Guardian will be completely removed from your computer.

2. Select one of the options and click **Next** to continue with the uninstallation.

If you have password-protected Guardian Total Security, an authentication screen appears.

3. Enter your password and click **OK**.

The uninstallation process is initiated.

When uninstallation is complete, a message appears.

You may provide feedback and reasons for uninstalling Guardian Total Security by clicking **Write to us the reason of un-installing Guardian Total Security**. Your feedback is valuable to us and it helps us improve the product quality.



Note: Note down the product key for future reference. You can save your product key information by clicking **Save to file**. Restart of your computer is recommended after Guardian Total Security uninstallation. To restart click **Restart Now**, or click **Restart Later** to continue working on the system and restart after some time.

---

## 10. Support

---

Guardian Total Security provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the email or call to receive efficient support from the Guardian Total Security support executives.

### Technical Support

The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, submit your queries, send emails about your queries or call us directly.

To see the support options, follow these steps:

1. Open **Guardian Total Security**.
2. On the left pane, click the More option and then select the **Support** option.

Support includes the following options.

**Web Support:** Includes **Visit FAQ** (Frequently Asked Questions) and **Visit Forums** – where you can submit your queries to get an appropriate answer.

**Email Support:** Includes **Submit Ticket** that redirects you to our Support webpage. Here you can read some of the most common issues with answers. If you do not find an answer to your issue, you can submit a ticket.

**Remote Support:** This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.

**Live Chat Support:** Using this option, you can chat with our support executives.

**Phone Support:** Includes phone numbers. You can call our support team and get your issues resolved.

### Support by Phone

This feature helps you to call for instant support from the Guardian technical experts.

The following is the contact number for phone support: +91- 86696-67399.

---

## Other Sources of Support

To get other sources of support, please visit <http://www.guardianav.co.in/contact>.