

Guardian NetSecure

User Guide

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

Copyright & License Information

Copyright © 2017 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.

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

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 NetSecure is subject to user's unconditional acceptance of the Guardian NetSecure end-user license terms and conditions.

To read the license terms, visit www.quickheal.com/eula and check the End-User License Agreement for your product.

About This Document

This user guide covers all the information required to install and use Guardian NetSecure products on Windows operating systems. The following table lists the conventions that we have followed to prepare this guide.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down box, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights reservation 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 the task related to the topic being discussed.
	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

1. Getting started.....	1
Prerequisites	1
System requirements.....	1
Installing Guardian NetSecure	3
Uninstalling Guardian NetSecure.....	4
2. Registration, reactivation, and renewal	5
Registration.....	5
Registering online	5
Registering offline	6
<i>Obtaining Product Key and Installation Number</i>	<i>6</i>
<i>Generating Activation Key for offline activation.....</i>	<i>6</i>
<i>Activating Guardian NetSecure with offline Activation Key</i>	<i>7</i>
Registering through SMS	7
Reactivation	8
Renewal.....	9
Renewing online	9
Renewing offline	10
<i>Getting the details of Guardian NetSecure</i>	<i>10</i>
<i>Generating Activation Key for offline activation.....</i>	<i>10</i>
<i>Renewing Guardian NetSecure with <license>.key file</i>	<i>11</i>
3. Guardian NetSecure Dashboard.....	12
About Guardian NetSecure Dashboard	12
<i>Right-click Menu Options</i>	<i>14</i>
4. Guardian NetSecure Protection Center.....	15
Files & Folders.....	16
Scan Settings	16
<i>Scan archive files</i>	<i>17</i>
<i>Select the type of archive that should be scanned.....</i>	<i>18</i>
<i>Scan packed files</i>	<i>18</i>
<i>Scan mailboxes.....</i>	<i>18</i>
Virus Protection	19
Advance DNAScan.....	20
Block Suspicious Packed Files	22
Automatic Rogueware Scan.....	23

Anti-Keylogger.....	23
<i>Configuring Anti-Keylogger</i>	23
Screen Locker Protection.....	23
<i>Configuring Screen Locker Protection</i>	23
Scan Schedule.....	24
<i>Configuring Scan Schedule</i>	24
Exclude Files & Folders.....	26
<i>Configuring Exclude Files & Folders</i>	26
Quarantine & Backup.....	27
<i>Configuring Quarantine & Backup</i>	27
Emails.....	28
Email Protection.....	28
<i>Configuring Email Protection</i>	28
Trusted Email Clients Protection.....	30
<i>Configuring Trusted Email Clients Protection</i>	30
Internet & Network.....	30
Firewall Protection.....	30
<i>Configuring Firewall Protection</i>	30
Browsing Protection.....	33
<i>Configuring Browsing Protection</i>	34
Malware Protection.....	34
<i>Configuring Malware Protection</i>	34
News Alert.....	35
<i>Turning News Alert off</i>	35
IDS/IPS.....	35
<i>Turning IDS/IPS ON</i>	35
External Drives & Devices.....	36
Autorun Protection.....	36
<i>Configuring Autorun Protection</i>	36
Scan External Drives.....	36
<i>Configuring Scan External Drives</i>	36
5. Quick Access Features.....	38
Scan.....	38
Performing Full System Scan.....	38
Performing Custom Scan.....	38
Performing Memory Scan.....	39

Performing Boot Time Scan	39
News.....	40
6. Guardian NetSecure Menus	41
Settings.....	41
Import and Export Settings.....	41
Automatic Update.....	42
<i>Configuring Automatic Update</i>	<i>42</i>
Internet Settings	43
<i>Configuring Internet Settings</i>	<i>43</i>
Registry Restore	44
<i>Configuring Registry Restore.....</i>	<i>44</i>
Self Protection.....	44
<i>Configuring Self Protection</i>	<i>45</i>
Password Protection	45
<i>Safe Mode Protection.....</i>	<i>45</i>
<i>Configuring Password Protection.....</i>	<i>45</i>
Report Settings.....	45
<i>Configuring Report Settings</i>	<i>46</i>
Report Virus Statistics.....	46
<i>Configuring Report Virus Statistics.....</i>	<i>46</i>
Restore Default Settings	46
<i>Restoring Default Settings.....</i>	<i>46</i>
Tools.....	47
Hijack Restore	47
<i>Using Hijack Restore.....</i>	<i>47</i>
Track Cleaner	48
<i>Using Track Cleaner.....</i>	<i>48</i>
Anti-Rootkit.....	49
<i>Using Guardian NetSecure Anti-Rootkit.....</i>	<i>49</i>
<i>Configuring Guardian NetSecure Anti-Rootkit Settings</i>	<i>50</i>
<i>Scanning Results and Cleaning Rootkits</i>	<i>51</i>
<i>Cleaning Rootkits through Guardian NetSecure Emergency Disk.....</i>	<i>52</i>
Creating Emergency Disk	53
Launch AntiMalware.....	54
<i>Launching Guardian NetSecure AntiMalware.....</i>	<i>54</i>
<i>Using Guardian NetSecure AntiMalware</i>	<i>54</i>
View Quarantine Files.....	55

<i>Launching Quarantine Files</i>	55
USB Drive Protection	56
System Explorer	56
Windows Spy.....	56
<i>Using Windows Spy</i>	57
Exclude File Extensions	57
<i>Creating Exclusion List for Virus Protection</i>	57
Reports.....	58
Viewing Reports	58
Help.....	59
7. Updating Guardian NetSecure & Cleaning Viruses	62
Updating Guardian NetSecure from Internet.....	62
Updating Guardian NetSecure with definition files.....	63
Update Guidelines for Network Environment	63
Cleaning Viruses.....	64
Cleaning viruses encountered during scanning	64
<i>Scanning Options</i>	64
Cleaning virus encountered in memory.....	65
8. Technical Support	66
9. Index.....	68

Getting started

Guardian NetSecure is simple to install and easy to use. During installation, read each installation screen carefully and follow the instructions.

Prerequisites

Remember the following guidelines before installing Guardian NetSecure on your system.

- Remove any other antivirus software program from your computer if you have any. Multiple antivirus software products installed on a single computer 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 NetSecure.

System requirements

To use Guardian NetSecure, your system must meet the following minimum requirements. However, we recommend that your system should have higher configuration to obtain better results.

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.

General requirements

- CD/DVD Drive
- Internet Explorer 6 or later
- Internet connection to receive updates
- Free disk space 1.5 GB

System requirements for various Microsoft Windows OS

Operating Systems (OS)	System Requirements
Windows 10	Processor: 1 gigahertz (GHz) or faster RAM: 1 gigabyte (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	Processor: 1 GHz or faster RAM: 1 GB for 32-bit or 2 GB for 64-bit
Windows Vista	Processor: 1 GHz or faster RAM: 1 GB
Windows XP (Service Pack 2 and later)	Processor: 300 Megahertz (MHz) Pentium or faster RAM: 512 MB
Windows 2000 (Service Pack 4)	Processor: 300 MHz Pentium or faster RAM: 512 MB

To check for the latest system requirements, visit our website at <http://www.guardianav.co.in>.

POP3 email clients compatibility

Guardian NetSecure supports	Guardian NetSecure does not support
<ul style="list-style-type: none"> • Microsoft Outlook Express 5.5 and later • Microsoft Outlook 2000 and later • Netscape Messenger 4 and later • Eudora • Mozilla Thunderbird • IncrediMail • Windows Mail 	<ul style="list-style-type: none"> • IMAP • AOL • POP3s with Secure Sockets Layer (SSL) • Web-based email such as Hotmail and Yahoo! Mail • Lotus Notes

Note: The Email Protection feature of Guardian NetSecure is not supported on encrypted email connections that use Secure Sockets Layer (SSL).

The following features of Guardian NetSecure follow specific compatibility

Features	Conditions
Anti-Keylogger	<ul style="list-style-type: none"> • Is not supported on Microsoft Windows 2000, Windows XP 32-bit with Service Pack 1 or previous, and Windows XP 64-bit.
Emergency Disk	<ul style="list-style-type: none"> • 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.
Firewall	<ul style="list-style-type: none"> The Monitor Wi-Fi Networks feature is not supported on Microsoft Windows 2000 and Windows XP 64-bit.
Self-Protection	<ul style="list-style-type: none"> Is not supported on Microsoft Windows 2000 OS. For Microsoft Windows XP operating system, this feature is supported only if Service Pack 2 or later is installed. For Microsoft Windows Server 2003 operating system, this feature is supported only if Service Pack 1 or later is installed. Process protection functionality of Self-Protection is supported on Microsoft Windows Vista Service Pack 1 and later.
Anti-Rootkit	<ul style="list-style-type: none"> Is supported on 32-bit OS only.

Installing Guardian NetSecure

To install Guardian NetSecure, follow these steps:

1. Insert the Guardian NetSecure CD/DVD in the DVD drive.

The autorun feature of the CD/DVD is enabled and it will automatically open a screen with a list of options.

If the DVD drive does not start the CD/DVD automatically, follow these steps:

- i. Go to the folder where you can access the CD/DVD.
- ii. Right-click the DVD drive and select **Explore**.
- iii. Double-click **Autorun.exe**.

2. Click **Install** to initiate the installation process.

The installation wizard performs a pre-install virus scan of the system. If a virus is found active in memory, then:

- The installer automatically sets the boot time scanner to scan and disinfect the system on the next boot.
- After disinfection of your computer, the computer restarts and you need to re-initiate the installation. For more details, see [Performing Boot Time Scan](#).

If no virus is found in the system memory, the installation proceeds.

The End-User License Agreement screen appears. Read the license agreement carefully.

3. At the end of the license agreement, there are two options **Submit suspicious files** and **Submit statistics** which are selected by default. If you do not want to submit the suspicious files or statistics or both, clear these options.

4. Select **I Agree** if you accept the terms and then click **Next**.

The Install Location screen appears. The default location where Guardian NetSecure is to be installed is displayed. The disk space required for the installation is also mentioned on the screen.

5. If the default location has insufficient space, or if you want to install Guardian NetSecure on another location, click **Browse** to change the location or click **Next** to continue.

The installation is initiated. When installation is complete, a message appears.

6. Click **Register Now** to initiate the activation process or click **Register Later** to perform activation later.

Uninstalling Guardian NetSecure

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

1. Select **Start > Programs > Guardian NetSecure > Uninstall Guardian NetSecure**.

- **Remove Guardian NetSecure and keep update definitions files** - If you select this option, Guardian NetSecure 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 NetSecure completely** - If you select this option, Guardian NetSecure 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 NetSecure, 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 NetSecure by clicking **Write to us the reason of un-installing Guardian NetSecure**. Your feedback is valuable to us and it helps us improve the product quality.



Please 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 NetSecure uninstallation. To restart click **Restart Now**, or click **Restart Later** to continue working on the system and restart after some time.

Registration, reactivation, and renewal

You should register your product immediately after installing it. Unless you register the product, it will be considered as a trial version. Also, a subscriber with registered license can use all the features without any interruptions, take the updates regularly, and get technical support whenever required. If your product is not regularly updated, it cannot protect your system against the latest threats.

Registration

You can register Guardian NetSecure in any of the following ways.

[Registering online](#)

[Registering offline](#)

[Registering through SMS](#)

Registering online

If you are connected to the Internet you can register your product online. To register Guardian NetSecure online, follow these steps:

1. Select **Start > Programs > Guardian NetSecure > Activate Guardian NetSecure**.
2. On the Registration Wizard, enter the 20-digit Product Key and click **Next**.
The Registration Information appears.
3. Enter relevant information in the **Purchased From** and **Register for** text boxes, and then click **Next**.
4. Provide your **Name**, **Email Address**, and **Contact Number**. Select your **Country**, **State**, and **City**.

If your State/Province and City are not available in the list, you can type your locations in the respective boxes.

5. Click **Next** to continue.

A confirmation screen appears with the details you entered.

If any modifications are needed, click **Back** to go to the previous screen and make the required changes.

6. Click **Next** to continue.

Your product is activated successfully. The expiry date of your license is displayed.

7. Click **Finish** to close the Registration Wizard.

Registering offline

You can register Guardian NetSecure offline also if your system is not connected to the Internet.

You need to visit the offline activation page on the website of Guardian NetSecure at <http://www.guardianav.co.in/guardian-support> and complete the registration form. After the registration is complete, a new key is generated which you have to use to activate your product on your system that is not connected to the Internet.

You can register Guardian NetSecure offline in the following way.

Obtaining Product Key and Installation Number

Before visiting the offline activation page, ensure that you have the Product Key and the Installation Number with you. You can obtain the key and installation number in the following way.

- **Product Key:** The Product Key is found in your product packaging. The Product Key is sent to your email address if you have purchased it online.
- **Installation Number:** You can obtain the Installation Number from the Activation Wizard in the following way:
 - i. Select **Start > Programs > Guardian NetSecure > Activate Guardian NetSecure**.
 - ii. On the Registration Wizard, click **Register Offline**.

The offline activation screen appears with the offline activation URL and Installation Number.

You can note down the URL for offline activation and 12-digit Installation Number or click **Save to file** to save the details.

Generating Activation Key for offline activation

To activate your license offline, you need to generate a key in the following way:

1. Visit the offline activation page at <http://www.guardianav.co.in/guardian-support>.
An Off-Line Registration page appears.
2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.
Ensure that you have the [Product Key](#) and [Installation Number](#) (as described in the preceding section) with you.

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

All asterisk (*) fields are mandatory to fill.

5. A new key is generated. Save this key for future reference.

This key is also sent to your email address that you provided during registration of the product.

Activating Guardian NetSecure with offline Activation Key

After the offline activation key is generated, you can proceed with activating Guardian NetSecure on your system that is not connected to the Internet in the following way:

1. Select **Start > Programs > Guardian NetSecure > Activate Guardian NetSecure**.
2. On the Registration Wizard, click **Register Offline**.

The offline activation screen appears.

3. Click **Browse** to locate the path where the **<license>.key** is stored and click **Next**.

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

4. Click **Finish** to close the Registration Wizard.

Registering through SMS

Guardian NetSecure may also be activated through SMS. If your system is not connected to the Internet, you can register your product through SMS Registration process.



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

Guardian NetSecure can be registered through the SMS Registration facility in the following way:

1. Select **Start > Programs > Guardian NetSecure > Activate Guardian NetSecure**.
2. On the Registration Wizard, click **SMS Registration**.

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

3. Click **Next**.
4. Enter the 20-digit **Product Key** and click **Next**.

The Registration Information appears.

5. Enter relevant information in the **Purchased From** and **Register for** text boxes, and then click **Next**.

6. Provide your **Name, Email Address, and Contact Number**. Select your **Country, State, and City**.

If your State/Province and City are not available in the list, you can type your locations in the respective boxes.

7. Click **Next** to continue.

A confirmation screen appears with the information that you entered.

If any modifications are needed, click **Back** to go to the previous page and make the required changes.

8. Click **Next** to continue.

A unique code along with a mobile number is displayed.

9. Type the code and send it as an SMS to the number displayed.

10. After successful registration at the Guardian NetSecure Registration Center, you will receive an SMS on your registered mobile which contains an alphanumeric activation code. Type this activation code in the text box provided and click **Next**.

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

11. Click **Finish** to close the Registration Wizard.

Reactivation

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 NetSecure on another computer. In such cases, you need to re-install and reactivate Guardian NetSecure on your system.

The reactivation process is similar to the activation process, with the exception that you do not need to enter the complete personal details again. Upon submitting the Product Key (and Installation Number in case of offline reactivation), the details are displayed. You can just verify the details and complete the process.

If you have saved the license backup using the [Remove Guardian NetSecure and keep update definitions files](#) option during uninstallation on your computer, and initiate reactivation, the Product Key is displayed on the Guardian NetSecure registration dialog box. You can proceed with the found Product Key and the updates you saved. Moreover, you can also use another Product Key if you prefer.

Upon submitting the Product Key (and Installation Number in case of offline reactivation), the user details are displayed. You can verify the details and complete the process.



If you prefer to reactivate your license through SMS, you have to fill in the user information again.

Renewal

You can renew your product license as soon as it expires by purchasing a renewal code. However, you are recommended to renew your product before your product license expires so that your computer remains protected. You can buy the renewal code from the website of Guardian NetSecure, or from the nearest distributor or reseller.

You can renew Guardian NetSecure in any of the following ways.

[Renewing online](#)

[Renewing offline](#)

Renewing online

If your computer is connected to the Internet, you can renew Guardian NetSecure online in the following way:

1. Select **Start > Programs > Guardian NetSecure > Guardian NetSecure**.
2. Click the **Help** menu and then select **About > Renew Now**.

If your product license has expired the **Renew Now** button is displayed on the Guardian NetSecure Dashboard. To renew your license, click **Renew Now**.

The Registration Wizard appears.

3. Select the option **I want to renew with renewal code. I already have renewal code with me** and click **Next**.

The Registration Information appears.

Note: If you do not have a renewal key and want to renew your license, select **I do not have renewal code with me** and then make the purchase.

4. Relevant information in the **Purchased From**, **Email Address**, and **Contact Number** text boxes appears pre-filled. However, you can modify your contact details if required and then click **Next**.

The license information such as **Current expiry date** and **New expiry date** is displayed for your confirmation.

5. Click **Next**.

The license of Guardian NetSecure is renewed successfully.

6. Click **Finish** to complete the renewal process.



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

Renewing offline

Guardian NetSecure can be renewed offline if your system is not connected to the Internet.

Visit the offline renewal page on the website of Guardian NetSecure at <http://www.guardianav.co.in/guardian-support> and complete the registration form. After the offline renewal registration is complete, a new key will be generated. You have to use this new key to renew your product on the computer that is not connected to the Internet.

You can renew Guardian NetSecure offline in the following way:

Getting the details of Guardian NetSecure

Before visiting the offline renewal page, keep the following details ready:

- Product Key and Installation Number – You can get the Product Key and Installation Number by filling in the renewal form in the following way :
 - i. Select **Start > Programs > Guardian NetSecure > Guardian NetSecure**.
 - ii. If your copy of Guardian NetSecure has expired, a button Renew Now is displayed on the Guardian NetSecure Dashboard. You can renew your license using this button. If your copy of Guardian NetSecure has not expired yet, then go to the Help menu, and select **About > Renew Now**.
 - iii. Click **Renew Offline**.

The offline renewal details screen appears.

You can either note down the offline renewal URL, Product Key and 12-digit Installation Number or click **Save to file** to save these details.

Generating Activation Key for offline activation

To renew your license offline, you need to generate a key in the following way:

1. Visit the offline renewal page at <http://www.guardianav.co.in/guardian-support>.
An Off-Line Renewal page appears.
2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.
Ensure that you have the [Product Key](#) and Installation Number (as described in the preceding section), and renewal code with you.
3. Enter the Product Key, Installation Number, Purchased Renewal Code and Purchased From details and click **Submit**.
4. 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**.
5. A new key is generated. Save this key for future reference.

This key is also sent to your email address that you provided during registration of the product.

Renewing Guardian NetSecure with <license>.key file

After the offline renewal key is generated, you can proceed with renewing Guardian NetSecure on your system that is not connected to the Internet in the following way:

1. Select **Start > Programs > Guardian NetSecure > Guardian NetSecure**.
2. If your copy of Guardian NetSecure has expired, a button **Renew Now** is displayed on the Guardian NetSecure Dashboard. You can renew your license using this button. If your copy of Guardian NetSecure has not expired yet, then go to the Help menu and select **About > Renew Now**.
3. Click **Renew Offline**.
The offline renewal details screen appears.
4. Click **Browse** to locate the path where the <license>.key is stored and click **Next** to continue.
The copy of Guardian NetSecure is renewed and the license validity is displayed.
5. Click **Finish** to close the Registration Wizard.

Guardian NetSecure Dashboard

The Guardian NetSecure Dashboard serves as the main interface to all the features of Guardian NetSecure. Guardian NetSecure protects your system even with the default settings. You can open Guardian NetSecure to check the status of protection, to manually scan the system, view reports, and update the product.

You can manually start Guardian NetSecure in any one of the following ways:

- Select **Start > Programs > Guardian NetSecure > Guardian NetSecure**.
- On the taskbar, double-click the **Guardian NetSecure** icon or right-click the **Guardian NetSecure** icon and select **Open Guardian NetSecure**.
- Select **Start > Run**, type Scanner and press the **Enter** key.

About Guardian NetSecure Dashboard

The Guardian NetSecure Dashboard is divided into various sections. The top section includes the product menus, the middle section the protection options, and the bottom section the latest news from Guardian NetSecure and scan options.

Top section

The top section includes the product menus that help you configure the general settings of Guardian NetSecure and use tools for preventing virus infection. You can diagnose the system and view the reports of various activities of the features, access the Help and see the license details.

The following table describes the menus and their usage.

Menus	Description
Settings	Helps you customize features such as Automatic Update, Internet Settings, Registry Restore, Self Protection, Password Protection, Reports Settings, Report Virus Statistics, and Restore Default Settings.
Tools	Helps you diagnose the system in case of virus attacks, clean application and Internet activities, restore the Internet Explorer settings modified by malwares, isolate the infected and suspicious files, remove rogeware and

Reports	prevent USB drives against autorun malware infection. You can also exclude files from virus protection. Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Scan Scheduler, Behavior Detection, Quick Update, Memory Scan, Registry Restore, Boot Time Scanner, AntiMalware Scan, Firewall Protection, IDS & IPS, Browsing Protection, and Anti-Keylogger.
Help	Helps you access the Help tool for Guardian NetSecure, see details about product version, virus database, validity details, license details, and seek technical support.

To know more about this section, see [Guardian NetSecure Menus](#).

Middle section

The middle section includes the protection options that help you configure various features for the security that your computer needs.

The following table describes the options and their usage.

Options	Description
Files & Folders	Helps you protect files and folders against malicious threats. With this option, you can configure Scan Settings, Virus Protection, Advance DNAScan, Block Suspicious Packed Files, Automatic Rogueware Scan, Anti-Keylogger, Screen Locker Protection, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Helps you configure Email Protection, and Trusted Email Clients Protection.
Internet & Network	Helps you configure the settings for Internet & Network protection. With this option, you can configure Firewall Protection, Browsing Protection, Malware Protection, News Alert, and IDS/IPS.
External Drives & Devices	Helps you configure protection for external drives. With this option, you can configure Autorun Protection, and Scan External Drives.

To know more about this section, see [Guardian NetSecure Protection Center](#).

Bottom section

The following table describes the options and their usage.

Miscellanies	Description
News	Displays the latest news from Guardian NetSecure. You can see all the news by clicking <i>See All</i> .
Scan	Provides you with various scan options such as Full System Scan, Custom Scan, Memory Scan, and Boot Time Scan.

Support Facebook Like	<p>Helps you get to various support options available in the Support menu.</p> <p>With this link, you can like the Guardian NetSecure page on Facebook. Guardian's corporate Facebook page has a vibrant community of users and a host of regular posts on cyber security and virus threats and alerts. You can follow the Guardian Facebook page by clicking the 'Facebook Like' link available on Dashboard.</p> <p>Alternately, if you are logged on to Facebook but you are not a part of the Guardian users' community on Facebook, you will get a prompt to like and follow the Guardian page.</p>
--	--

To know more about this section, see [Quick Access Features](#).

Right-click Menu Options

These options provide you quick access to some of the important features of your Guardian NetSecure. To access any of these options, right-click the Guardian NetSecure icon in the taskbar and then select an option.

Right-click Menus	Description
Open Guardian NetSecure	Helps you launch Guardian NetSecure.
Launch AntiMalware	Helps you launch Guardian NetSecure AntiMalware, an integrated tool that helps you scan registry, files, and folders at a very high speed. It helps you to thoroughly detect and clean Spywares, Adware, Rogueware, Dialers, Riskware and a number of other potential threats in your system.
Enable / Disable Silent Mode	Helps you enable / disable all Guardian NetSecure prompts and notifications.
Enable / Disable Virus Protection	Helps you enable / disable Guardian NetSecure Virus Protection.
Update Now	Helps you update Guardian NetSecure virus database.
Scan Memory	Helps you scan system memory for viruses.




To know more about this section, see [Guardian NetSecure Protection Center](#).

Guardian NetSecure Protection Center

While working with computer system, you are connected to the Internet, external drives, and send and receive email communications. This makes your system exposed to viruses that try to infiltrate into your system. Guardian NetSecure Protection Center 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.

Just above the features current status about your Guardian NetSecure product is displayed. If the antivirus detects any threat in your system, it is indicated through color coded icons.

The following table describes the icons and their meanings.

Green		Indicates that Guardian NetSecure is configured with optimal settings and your system is protected.
Orange		Indicates that a feature of Guardian NetSecure needs your attention at your earliest convenience, but not immediately.
Red		Indicates that Guardian NetSecure is not configured with optimal settings and your immediate attention is needed. The action corresponding to the message needs to be carried out immediately to keep your system protected.

Guardian NetSecure Protection Center includes the following features.

Features	Description
Files & Folders	Includes Scan Settings, Virus Protection, Advance DNAScan, Block Suspicious Packed Files, Automatic Rogueware Scan, Anti-Keylogger, Screen Locker Protection, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Includes Email Protection and Trusted Email Clients Protection.
Internet & Network	Includes Firewall Protection, Browsing Protection, Malware Protection, News Alert, and IDS/IPS.
External Drives & Devices	Includes Autorun Protection, and Scan External Drives.

Files & Folders

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

Files & Folders includes the following protection settings.

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. However, the default settings are optimal that ensures the required protection to your system.

To configure Scan Settings, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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**.

Select scan mode

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

Various actions and their description are as follows:

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 NetSecure 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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.
However, the Scan executable files option is selected by default.
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 **Thorough scan of mailboxes** to scan thoroughly.
8. Click **OK**.
9. Click **Save Changes** to save your settings.

Scan archive files

This feature helps you further set 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 till you want to scan the files and folders.
The default scan level is set to level 2. However, 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. Click **OK** to save your settings.

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.

Select the type of archive that should 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.

Scan packed files

This feature helps you scan packers. 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.

Scan 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. It 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. However, this may affect the speed as the size of the mailbox increases.

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 for viruses. Importantly, this feature does not re-scan the files that have not changed since the previous scan. This helps in maintaining lower resource usage.

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

To configure Virus Protection, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Virus Protection** on.
4. Click **Virus Protection**.
The Virus Protection details screen appears.
5. Set the following options as per requirement:
 - **Display alert messages** – Select this option if you want to get the alerts on various events such as when malware is detected. However, this option is selected by default.
 - **Select action to be performed when virus is detected** – Select an appropriate action 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.
6. Click **Save Changes** to save your setting.

Action to be taken when a virus is detected

Action	Description
Repair	If a virus is found during a scan, it repairs the file. If the file cannot be

Delete	repaired, it is quarantined automatically.
Deny Access	Deletes a virus-infected file without notifying you. 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. However, you can turn Virus Protection off when absolutely necessary. While you turn Virus Protection off, you have a number of options to turn the feature only temporarily, so that it turns on automatically after the select time interval passes.

To turn off Virus Protection,

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Virus Protection** off.
4. 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
5. Click **OK** to save your settings.

After you turn Virus Protection off, the icon color of the Files & Folders option on Dashboard changes from green to red and a message “System is not secure” is displayed.

Advance DNAScan

DNAScan is an indigenous technology of Guardian NetSecure to detect and eliminate new and unknown malicious threats in the 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 NetSecure 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.

To configure Advance DNAScan, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.

3. On the Files & Folders 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 NetSecure 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 NetSecure will send alert if any suspicious activity of a running application is noticed.
 - Low: If you select this security level, Guardian NetSecure 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 NetSecure research labs.
 - **Submit files:** Select this option if you want to submit the suspicious files to the Guardian NetSecure Research labs for further analysis. You can also select **Show notification while submitting files** to get prompts for permission before submitting the files.



If the option **Show notification while submitting files** is not selected, Guardian NetSecure 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. However, 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 NetSecure updates itself and finds new quarantined DNAScan-suspected files. This file is sent in an encrypted file format to the Guardian NetSecure 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
3. Under Cleaning & Restore Tools, click **View Quarantine Files**.
The Quarantine dialogue appears.
A list of the files that have been quarantined is displayed.
4. Select the files that you want to submit to the Guardian NetSecure labs and then click **Send**.
5. Click **Close** to close the Quarantine dialogue.

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.

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Block Suspicious Packed Files** on.

However, Block Suspicious Packed Files is turned on by default.

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.

To configure Automatic Rogueware Scan, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Automatic Rogueware Scan** on.

However, Automatic Rogueware Scan is turned on by default.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, turn **Anti-Keylogger** on or off as you prefer.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders screen, click **Screen Locker Protection**.
4. To enable Screen Locker Protection, select **Protect from screen lockers**. However, this option is selected by default.
5. Select an alphabet from the drop-down list to create a short-cut combination with **Ctrl+Alt+Shift**. Here **A** is selected by default.
6. Click **Save Changes**.



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

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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. However, this option is selected by default.

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 . However, this option is selected by default.

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. However, 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 Vista 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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.

Deleting a scan schedule

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

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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. Click **Close** to close the Scan Schedule screen.

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

Exclude Files & Folders

With this feature, you can decide which files and folders should not be included during scanning for known viruses, DNAScan, Suspicious Packed files, and Behavior Detection. This helps you avoid unnecessarily scanning files which have already been scanned or that you are sure should not be scanned.

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

- Scanner
- Virus Protection
- Memory Scanner
- DNAScan

Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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 options.

7. Click **OK**.

8. Click **Save Changes** to save your settings.



- 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Files & Folders**.
3. On the Files & Folders 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. However, 30 days is set by default.
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:

- **Add:** Helps you add new files from the folders and drives to be quarantined manually.
- **Remove:** Helps you remove any of the quarantine files from the Quarantine list. To remove a file, select the file and then click the **Remove** button.
- **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. To restore a file, select the files and then click the **Restore** button.
- **Remove All:** Helps you remove all the quarantined files from the Quarantine list. To remove all the files, click the **Remove All** button. On the confirmation message, click **Yes** to remove all the files.
- **Send:** Helps you send the quarantined files to our research labs. To send a file, select the file and then click the **Send** button.

6. To close the Quarantine dialog, click the **Close** button.

Emails

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

This feature is turned on by default which provides the optimal protection to the mailbox 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Emails**.
3. On the Emails screen, turn **Email Protection** on.

However, Email Protection is turned on by default.

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.



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

- 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.



If the attachment cannot be repaired then it is deleted.

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

Attachment Control Settings

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. Emails such as MIME, IFRAME contain vulnerability.
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>Block all attachments: Helps you block all types of attachments in emails.</p> <p>Block user specified attachments:</p> <p>Helps you block email attachments with certain extensions. If you select this option, the Configure button is activated. For further settings, click Configure and set the following options:</p> <ul style="list-style-type: none"> 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. 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. Click OK to save changes.

Trusted Email Clients Protection

Since 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Emails**.
3. On the Emails 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. Click **Save Changes** to save your settings.

Internet & Network

This feature allows you to set the protection rules to protect your system from malicious files that can sneak into your system during online activities such as banking, shopping, and surfing.

Internet & Network includes the following features.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Internet & Network**.
3. Turn **Firewall Protection** on or off by using the toggle button.
However, Firewall Protection is turned on by default.
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 NetSecure will be blocked. For example, Guardian NetSecure 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	<p>Home: All incoming and outgoing connections are allowed except exceptions.</p> <p>Work: All incoming and outgoing connections are allowed except exceptions.</p> <p>Public: All incoming and outgoing connections are allowed except exceptions.</p> <p>Restricted: All incoming and outgoing connections are blocked except exceptions.</p> <p>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 file and printer. However, default setting is ideal for required security.</p>
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 & printer between other users and you. However, with sharing of files 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 Delete .
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.

Browsing Protection

While 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **Browsing Protection** on.

Browsing Protection is activated.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **Malware Protection** on.

Malware Protection is enabled.

4. 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, actions to be performed option is activated.
 - **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	<p>If you select this option, a message will appear when an adware is detected. The message will display the following options:</p> <ul style="list-style-type: none"> • Allow: Click this button to allow the adware to execute. • Remove: 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. • Close: Click this button to close the message. However, the same message will keep appearing until you take an action.
Repair	<p>Select this option if you want to repair a file.</p> <p>If an adware is found in a file during scan, it repairs the file. If the file cannot be repaired, it is quarantined and will be cleaned in the next Boot Time Scan.</p>
Skip	Select this option if you want to take no action on a file.

News Alert

With this feature, you get the latest news about cyber security, virus threats and alerts and other important information related to the computer protection. The latest news is also available on the Guardian NetSecure Dashboard. If you do not want to get the news alert, turn News Alert off.

Turning News Alert off

To turn News Alert off, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **News Alert** off.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Internet & Network**.
3. On the Internet & Network screen, turn **IDS/IPS** on.

External Drives & Devices

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them.

This feature allows you to set protection rules for external devices such as CDs, DVDs, and USB-based 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices screen, turn **Autorun Protection** on.

Autorun Protection is activated.

Scan External Drives

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

Configuring Scan External Drives

To configure Scan External Drives, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **External Drives & Devices**.
3. On the External Drives & Devices 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. However, this option is selected by default.
 - **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.

Quick Access Features

Quick Access Features provides quick access to some of the important features such as Scan options on Dashboard itself. It also displays latest news from Guardian NetSecure.

Scan

The Scan options available on the Guardian NetSecure Dashboard provide you with various options of scanning your system based on your requirements.

You can initiate scanning of your entire system, drives, network drives, USB drives, folders or files, certain 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.

Performing 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).

To initiate a full system scan, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, select **Scan > Full System Scan**.

The scan starts.

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

Performing 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, select **Scan > Custom Scan**.

- 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**.

- 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.

Performing Memory Scan

To perform a memory scan, follow these steps:

- Open **Guardian NetSecure**.
- On the Guardian NetSecure Dashboard, select **Scan > 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:

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.
I/O errors	Displays the number of I/O errors occurred during the scan.
Scanning status	Displays the current status of the scan being performed.

Performing Boot Time Scan

Boot Time Scan is very useful to clean the highly infected systems. Some viruses tend to be active if the system is running and they cannot be cleaned. However, 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, select **Scan > 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.

News

The News section displays the latest news about cyber security, virus threats and alerts and other important information related to the computer protection. However, to get the latest information, you must own a licensed version of the product.

Guardian NetSecure Menus

These menus help you configure the general settings for taking the updates automatically, and password-protect your Guardian NetSecure settings so that unauthorized persons cannot change them. It also provides settings for proxy support and for setting rules for automatic removal of reports from the list.

Settings

This feature allows you to apply various protection rules such as receiving updates from Guardian NetSecure as and when released, and password-protect your settings. It also allows you to set the rule when the reports generated on all the incidents should be removed. However, the default settings are optimum and can provide complete security to your system. We recommend that you change the settings only when absolutely necessary.

Settings includes the following features.

Import and Export Settings

This feature allows you to import and export the settings of Guardian NetSecure 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 computer(s). Both the default settings and the settings made by you can be exported.

Importing and Exporting the Guardian NetSecure Settings

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

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, click the **Import/Export** tab.
4. On the Import/Export Settings dialog, select either of the following options.
 - **Export settings to a file:** Helps you export the current settings to a .dat file.
 - **Import settings from a file:** 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**.

5. Upon successful export or import, a message appears. Click **OK** to close the Import/Export dialogue.



- The settings can be imported from the same product flavor and the same version only. For example, the settings of Guardian NetSecure version 17.00 can be imported to Guardian NetSecure version 17.00 only.
- The settings of the following features cannot be exported or imported:
 - Scheduled Scans
 - Password Protection

Automatic Update

This feature helps you take automatic updates of latest virus signatures. This protects your system from the latest malware. To take the updates regularly it is recommended that you always keep Automatic Update turned on. However, Automatic Update is turned off by default.

Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, turn **Automatic Update** on.
Automatic Update is activated.
4. Click **Automatic Update**.
5. Select **Show update notification window**, if you want to get notified about the update of Guardian NetSecure. However, this option is turned on by default.
6. Select the update mode from the following options:
 - **Download from Internet** – Helps you download the updates to your system from the Internet.
 - [Pick update files from the specified path](#) – Helps you pick the updates from a local folder or a network folder.
 - [Copy update files to specified location](#) – Helps you save a copy of the updates to your local folder or network folder.
 - Check for the latest version of Guardian NetSecure:
 - **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. Click **Save Changes** to save your settings.

Selecting Update Mode

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

Pick update files from specified path

This option is best suitable if Guardian NetSecure is installed on multiple computers. You can download the updates on a single computer and set a path on other computers to pick the updates from the destination computer. The other computers will take the updates from the specified path as the new updates are available automatically. This helps you save the Internet bandwidth.

Copy update files to specified location

This option is suitable if you are working offline. You can download the updates at a specific location or on other computer and share the updates with pen drive or other multimedia. If this option is selected and the location of the system is specified, the complete update process takes place automatically.

Note: Automatic Update works on compatible systems. Your computers should have the same Guardian NetSecure product name, product version, and architecture such as 32-bit or 64-bit operating system installed to process the update successfully.

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. However, if you configure Internet Settings, you have to enter your user name and password credentials.

The following Guardian NetSecure modules require these changes.

- Registration Wizard
- Quick Update
- Messenger

Configuring Internet Settings

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, click **Internet Settings**.

4. Select **Enable proxy settings**.

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

5. In **Type** list, select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.

6. In the **Server** text box, enter the IP address of the proxy server or domain.

7. 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.

8. Enter your user name and password credentials.

9. Click **Save Changes** to save your settings.

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 Guardian NetSecure 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 NetSecure**.

2. On the Guardian NetSecure Dashboard, click **Settings**.

3. On the Settings screen, click **Registry Restore**.

4. 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.

5. Select **Repair malicious registry entries** to scan system registry for malware related entries. Malware and its remains are repaired automatically during the scan.

Self Protection

This feature helps you protect Guardian NetSecure 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 NetSecure. It is recommended that you always keep Self Protection on. However, this option is turned on by default.

Configuring Self Protection

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, turn **Self Protection** on.

However, Self Protection is turned on by default.

Password Protection

This feature allows you to restrict unauthorized people from modifying the Guardian NetSecure 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 NetSecure are disabled by default. In such a situation, unauthorized users may take advantage and steal data or modify the settings of the Guardian NetSecure 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, turn **Password Protection** on.

The Password Protection settings screen appears.

4. 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.

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

Report Settings

Reports on all activities of the Guardian NetSecure 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, click **Report Settings**.

The Report Settings screen appears.

4. 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.

5. Click **Save Changes** to apply the settings.

Report Virus Statistics

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

Configuring Report Virus Statistics

To configure Report Virus Statistics, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.
3. On the Settings screen, 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Settings**.

The Settings details screen appears.

3. On the Restore Default Settings, click the **Default All** button.
Your Guardian NetSecure is reverted to the default settings.

Tools

This feature allows you to carry out various activities such as you can clean and restore your system to its original settings, prevent access to certain drives, and diagnose the system.

Tools includes the following features.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Hijack Restore**.
4. On the Hijack Restore screen, select **Check All** to select all the browser settings in the list.
5. Select **Restore default host file** to restore the default host file.
6. Select **Restore important system settings** to restore important system settings.
7. To initiate restoring your settings, click **Restore Now**.

Restore Default Host File

The default host file includes the following options:

IP Address	Enter the IP Address of the host.
Host Name	Enter the host name.
Add	Click Add to add the host details in the list.
Edit	Select the host in the list and click Edit to make the changes.
Delete	Select the host in the list and click Delete to remove the host.
OK	Click OK to save your setting for the host files and exit from the Host Specification window.

Close	Click Close to exit without saving your settings from the Host Specification window.
--------------	---

Restore Important System Settings

This feature includes the following options.

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:

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 Undo button, it opens a window Undo Operations. The settings which have been restored to default settings will be listed. Select your settings or Check All to select all the settings. Click OK to revert to the existing settings.
Close	Helps you exit from the Hijack Restore window without saving your settings.

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. However, 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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Track Cleaner**.
The Track Cleaner screen appears. This displays a list of all the programs opened recently.
4. Select the programs whose traces you want to remove or select **Check All** to select all the programs in the list.
5. To initiate cleaning, click **Start Cleaning**.

6. To close the Track Cleaner window, click **Close**.

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.

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

Using Guardian NetSecure Anti-Rootkit

To use Anti-Rootkit, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Anti-Rootkit**.
A message appears that recommends you to close all other applications before launching Anti-Rootkit.
4. In the left pane on the Anti-Rootkit screen, click the **Start Scan** button.
Guardian NetSecure 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.
5. 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.

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 NetSecure Anti-Rootkit may fail. On failure, you will be asked to re-scan your system and submit error report to Guardian NetSecure 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 NetSecure Anti-Rootkit Settings

1. Open **Guardian NetSecure Anti-Rootkit**.
2. On the Guardian NetSecure Anti-Rootkit screen, click **Tools**.
The Tools details screen appears.
3. Guardian NetSecure Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.

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

<p>Process</p>	<p>After the scan is complete, Guardian NetSecure 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.</p> <p>Guardian NetSecure Anti-Rootkit also displays a summary of total number of processes scanned and hidden processes detected.</p>
<p>Terminating Hidden Process</p>	<p>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.</p>

<p>Registry</p>	<p>Similar to the Process scan, Guardian NetSecure 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.</p> <p>Guardian NetSecure Anti-Rootkit also displays a summary of total number of items scanned and number of hidden items detected.</p>
<p>Renaming Hidden Registry Key</p>	<p>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.</p>

Files and Folders	<p>Similarly, Guardian NetSecure 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.</p> <p>Guardian NetSecure Anti-Rootkit also displays a list of executable Alternate Data Streams.</p> <p>Guardian NetSecure Anti-Rootkit also displays a summary of total number of files scanned and number of hidden files detected.</p>
Renaming Hidden Files and Folders	<p>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.</p>

Cleaning Rootkits through Guardian NetSecure Emergency Disk

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

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

Step 1

To create Guardian NetSecure Emergency Disk, follow the link [Create Emergency Disk](#), p - 53.

Step 2

1. Open **Guardian NetSecure Anti-Rootkit**.
2. In the left pane on the Guardian NetSecure Anti-Rootkit screen, click the **Start Scan** button.

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

Creating 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 NetSecure on your system.

To create an Emergency Disk, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Create Emergency Disk**.
4. On the Create Emergency Disk screen, click the link and download the required package for emergency tool.
5. Extract the downloaded package on your system. For example: `c:\my documents\qhemgpkg`.
6. Provide the extracted package path, and click **Next**.
7. 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.
8. 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.

Launch AntiMalware

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

Launching Guardian NetSecure AntiMalware

Guardian NetSecure AntiMalware can be launched in any of the following ways:


- Select **Start > Programs > Guardian NetSecure > Guardian NetSecure AntiMalware**.
- Right-click the Guardian NetSecure Virus Protection icon in the Windows system tray and select Launch Antimalware.
- Open **Guardian NetSecure** and click **Tools**. Under **Cleaning & Restore Tools**, click **Launch AntiMalware**.

Using Guardian NetSecure AntiMalware

On the Guardian NetSecure AntiMalware screen, click **Scan Now** to initiate the malware scan process. During scanning, Guardian NetSecure 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:

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 Yes , otherwise click No 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 NetSecure AntiMalware by using Windows System Restore facility.
	 The feature Set System Restore point before cleaning is not available in Windows 2000 operating

Details	system. Helps you redirect to the Web site of Guardian NetSecure.
----------------	--

View Quarantine Files

This feature helps you safely isolate the infected or suspected files. When a file is quarantined, Guardian NetSecure 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. However, you can take a backup of the files also before taking an action.

Launching Quarantine Files

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **View Quarantine**.
A list of all quarantined files is displayed.

You can perform the following tasks on the Quarantine dialog:

Add	Helps you quarantine a file manually.
Remove	Helps you remove a quarantined file.
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.
Remove All	Helps you remove all the quarantined files.
Send	Helps you send the quarantined file to our research labs for further analysis. Select the file that you want to submit and click Send .

When you send a quarantined file to the Guardian NetSecure research labs, you are prompted to provide your email address and a reason for submitting the file. The reasons include the following ones:

Suspicious File	Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
File is un-repairable	Select this reason if Guardian NetSecure has been able to detect the malicious file on your system during its scans, but

False positive	has not been able to repair the infection of the file. Select this reason if a non-malicious data file that you have been using and are aware of its function, has been detected by Guardian NetSecure as a malicious file.
-----------------------	--

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Preventive Tools, click **USB Drive Protection**.
4. 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.



Guardian NetSecure recommends that you keep the autorun feature of your USB drive turned off, however, if you may turn on the Autorun feature of the USB drive following the same process as mentioned in here.

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.

To use system explorer, follow these steps:

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Diagnostic Tools, click **System Explorer**.

Windows Spy

This feature helps you find more information about an application or process. Sometimes we keep getting dialog boxes or messages that are actually shown by spyware or some malware

that we are unable to locate. In such a case, this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

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

Using Windows Spy

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Diagnostic Tools, click **Windows Spy**.
4. Drag the mouse pointer on the application.
A window will be opened displaying the above mentioned information.
5. If you want to terminate that application or window, click **Kill Process**.

Exclude File Extensions

This feature helps you create an exclusion list of file types or extensions for Virus Protection. This helps Virus Protection concentrate only on those files that are prone to malicious behavior.

Creating Exclusion List for Virus Protection

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Tools**.
The Tools details screen appears.
3. Under Diagnostic Tools, click **Exclude File Extensions**.
4. Enter the file extension that needs to be excluded from the Virus Protection scan and click **Add**.
5. If the added extension is incorrect, then select the extension added in the list and click **Remove** to delete it.
6. Click **OK** to save the list.

Reports

Guardian NetSecure 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.

The reports on the following features of Guardian NetSecure can be viewed:

- Scanner
- Virus Protection
- Email Protection
- Scan Scheduler
- Behavior Detection
- Quick Update
- Memory Scan
- Registry Restore
- Boot Time Scanner
- AntiMalware Scan
- Firewall Protection
- IDS & IPS
- Browsing Protection
- Anti-Keylogger

Viewing Reports

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

1. Open **Guardian NetSecure**.
2. On the Guardian NetSecure Dashboard, click **Reports**.
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.

Button	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.

For more details about Reports, see [Reports](#).

Help

This feature helps you access the Help topics whenever you want to know about how to use and configure the Guardian NetSecure features, how to seek support from the Guardian NetSecure Technical Support team, how to update the product, and see the license details of the product.

The Help feature includes the following options.

- **Help:** Helps you access the in-built Help topics. On the Guardian NetSecure Dashboard, select **Help > Help**, you are redirected to the Help page where you can find topics that describe the features of the product and how to use them. (Alternatively, press **F1** key, or click the **Help** button in a dialog to get to the Help page.)
- **Submit System Information:** Helps you submit information of your system to Guardian NetSecure for analysis.
For details on how to submit System Information, see [System Information](#).
- **Support:** Helps you seek support from the Customer Care of Guardian NetSecure whenever you face issues regarding the product or its features. Support has the options: Email Support and Phone Support. You can also submit your system information and ask the Guardian NetSecure technical executives to remotely access your system for solving an issue.
For more details on Support, see [Technical Support](#).
- **About:** The About section of Guardian NetSecure includes the following information:
 - Guardian NetSecure Version
 - License details
 - License validity
 - Update Now option

The following buttons are also available in the About section:

Renew Now	Helps you renew your existing subscription.
License Details	License Information and End-User License Agreement (EULA) are available under this section.
	Update License Details: This feature is useful to synchronize

Update Now	<p>your existing License information with Guardian NetSecure Activation Server. If you want to renew your existing subscription and you do not know how to renew it or you face the problem during renewal, you can call Guardian NetSecure Support team and provide your Product Key and Renewal Code.</p> <p>Guardian NetSecure Support team will renew your copy. However, you need to follow these steps:</p> <ol style="list-style-type: none"> 1. Be connected to the Internet. 2. Click Update License Details. 3. Click Continue to update your existing subscription. <p>Print License Details: Click Print License Details to take the print of the existing subscription information.</p> <p>Helps you update virus database of Guardian NetSecure.</p>
------------	--

System Information

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

To detect new Malwares	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.
To get Guardian NetSecure information	It gathers information of the installed version of Guardian NetSecure, its configuration settings and Quarantined file(s), if any.

Submitting System Information file

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



INFO.QHC file contains the critical system details and version details of Guardian NetSecure 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 NetSecure. The above information is used to provide better and adequate services to customers. 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.

Generating System Information

To generate system information, follow these steps:

1. On the Guardian NetSecure Dashboard, select **Help > Submit System Information**.

The System Information wizard opens.

2. Click **Next** to continue.
3. 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 NetSecure, select **I am having problem while using Guardian NetSecure**. Provide comments in the **Comments** text box and also enter your email address.
4. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Guardian NetSecure Technical Support.

Updating Guardian NetSecure & Cleaning Viruses

Updates for Guardian NetSecure are released regularly on the website of Guardian NetSecure. The updates include information pertaining to the detection and removal of newly discovered viruses. To prevent your system from new viruses, Guardian NetSecure must be updated regularly.

The default setting of Guardian NetSecure 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.

The updates can also be taken from a local or a network path, but that path should have the latest set of definitions. This is helpful if your computer on which Guardian NetSecure is installed is not connected to the Internet.

Some important facts about the Guardian NetSecure updates are:

- All the Guardian NetSecure updates are complete updates including Definition File Update and Engine Updates.
- All the Guardian NetSecure security updates also upgrade your version whenever required, thus making the new features and technology available for your protection.
- Guardian NetSecure Update is a single step upgrade process.

You can update Guardian NetSecure manually whenever necessary in any of the following ways:

Updating Guardian NetSecure from Internet

With Update Now, you may update Guardian NetSecure manually whenever you prefer. However, the default setting of Guardian NetSecure is configured to take the updates automatically through the Internet. Your system must be connected to the Internet to get updates regularly. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.).

To update Guardian NetSecure, follow these steps:

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

Updating Guardian NetSecure with definition files

If you have the update definition file with you, you can update Guardian NetSecure without connecting to the Internet. It is useful for Network environments with more than one system. You are not required to download the update file on all the computers within the network using Guardian NetSecure. You can download the latest definition files from the website of Guardian NetSecure from <http://www.guardianav.co.in/update>.

To update Guardian NetSecure through definition file, follow these steps:

1. Select **Start > Programs > Guardian NetSecure > Quick Update**.
2. Follow the instructions and click the **Next** button.
3. Select **Pick from specified path**.
4. Click **File** to locate the definition file. Select the update file.
5. Click **Next**.

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

Update Guidelines for Network Environment

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

1. Setup one computer (may be the server) as the master update machine. Suppose server name is SERVER.
2. Make **QHUPD** folder in any location. For example: **C:\QHUPD**. Assign Read-Only sharing rights to this folder.
3. Select **Start > Programs > Guardian NetSecure > Guardian NetSecure**.
4. On Dashboard, select **Settings > Automatic Update**.
5. Select **Copy update files to specified location**.

6. Click **Browse** and locate the **QHUPD** folder. Click **OK**.
7. Click **Save Changes** to save this setting.
8. On all user computers within the network launch **Guardian NetSecure**.
9. Under **Settings**, go to the **Automatic Update** page.
10. Select **Pick update files from specified path**.
11. Click **Browse**.
12. Locate the `SERVER\QHUPD` folder from Network Neighborhood. Alternatively you can type the path as `\\SERVER\QHUPD`.
13. Click **Save Changes** to save the settings.

Cleaning Viruses

Guardian NetSecure warns you of a virus infection when:

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

Cleaning viruses encountered during scanning

The default settings of Guardian NetSecure are adequately configured and are optimum to protect your system. If a virus is detected during scanning, Guardian NetSecure tries to repair the virus. However, 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.

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 which 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 encountered 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, lexplore.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 NetSecure memory scan will provide details or action recommendation for you in such cases.

Cleaning of Boot/Partition viruses

If Guardian NetSecure 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 NetSecure Emergency disk.

Responding to virus found alerts from Virus Protection

Virus Protection of Guardian NetSecure 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.

Technical Support

Guardian 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 support executives.

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 NetSecure**.
2. On the Guardian NetSecure Dashboard, select **Help > Support**.

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.

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

Other Sources of Support

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

Things to Do if the Product Key is Lost

Product Key serves as your identity to your Guardian NetSecure. If you lose the Product Key, please contact Guardian Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

Head Office Contact Details

Guardian NetSecure

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

E-mail: support@guardianav.co.in

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

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

Index

	B		R
Browsing Protection, 33		Registration	
	C	offline, 6	
Cleaning Viruses, 64		online, 5	
	D	product key, 6	
DNA Scan, 20		through SMS, 7	
	E	Renewal	
Email Protection, 28		offline, 10	
	P	online, 9	
Password Protection, 45			S
	Q	Scan	
Quarantine & Backup, 27		External Drives, 36	
		Scan Schedule, 24	
		Scan Settings, 16	
			V
		Virus Protection, 19	