

USER'S GUIDE

Thirtyseven4™ AntiVirus 2012

Thirtyseven4, L.L.C

<http://www.thirtyseven4.com>

END USER LICENSE AGREEMENT

By using or installing any software product created by Thirtyseven4, L.L.C. an Ohio limited liability company having a principal place of business at P.O. Box 1642, Medina, Ohio 44258 (hereafter referred to as "Company") including software components, source code, object code, and the corresponding documentation herein referred to as "Software"), you (herein referred to as "User"), are agreeing to be bound by the terms and conditions of this Agreement.

1. License Grant and Restrictions

In consideration for the license fee paid at time of purchase and subject to the conditions set forth in this Agreement, Company grants to User, a non-exclusive, non-sub licensable, non-assignable, non-transferable, worldwide right to use the Software. User may only use the Software on one single computer. User may install the Software on a network, provided User have a licensed copy of the Software for each and every computer that can access the Software on the network.

User may not resell, rent, lease, distribute or transfer the Software in any way.

2. Fees

In consideration for use of the Software, User has agreed to pay Company the amount set forth on www.thirtyseven4.com, Company's primary website, or the amount agreed to in writing between User and Company. **USER EXPRESSLY ACKNOWLEDGES THAT PRIOR TO SUBMITTING ANY PAYMENT TO COMPANY OR USING THE SOFTWARE, THAT USER HAS REVIEWED AND AGREED TO BE BOUND BY THE TERMS OF THIS AGREEMENT.**

3. Ownership

The Software and all intellectual property rights, including collateral and/or derivative rights associated therewith are the property of Company. Should any of rights relating to the forgoing become vested in User or a third party by User's use of the Software, User shall immediately transfer and/or take all steps necessary, and without compensation to Company, to insure that all right, title and interest in the same vest fully and completely in Company.

The Software and any accompanying materials are copyrighted and contain proprietary information. Unauthorized copying of the Software or accompanying materials even if modified, merged, or included with other software, or of any documentation or written materials, is expressly forbidden. However, User may make one (1) copy of the Software solely for backup purposes provided all proper legal notices are reproduced in their entirety on the backup copy. Company reserves all rights not specifically granted to User.

The Software and documentation are licensed, not sold, to User. User may not rent, lease, display or distribute copies of the Software to others except under the conditions of this Agreement.

4. Termination

This Agreement is effective until terminated. This Agreement will terminate immediately and automatically without notice from Company for failure to comply with any provision contained herein or if the funds paid for the license are refunded or are not received. Company also may terminate this Agreement with or without cause at any time by providing notice to User of its intent to Terminate. Should Company elect to terminate this Agreement under this provision and Customer has not violated any provision of this Agreement, Company shall refund any fees paid by User to Company during the twelve months that preceded the termination. User agrees that if User desire to terminate this Agreement, that Company shall determine in its sole and absolute discretion whether or not to refund part or all of any fee paid by User for the Software. Therefore, User expressly acknowledges that User has no right to any refund. Upon termination, User shall destroy the Software and all copies, in part and in whole, including modified copies, if any.

5. Warranties and Indemnities

Although efforts have been made to assure that the Software is date compliant, correct, reliable, and technically accurate, the Software is licensed to User "as is" and without warranties as to performance of merchantability, fitness for a particular purpose or use, or any other warranties whether expressed or implied. User assumes all risks when using it.

EXCEPT AS OTHERWISE EXPRESSLY STATED HEREIN, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, AS TO THE VALUE, CONDITION, DESIGN, FUNCTIONING OF THE SOFTWARE, OR ANY USE OF THE SOFTWARE, MERCHANTABILITY, FITNESS FOR ANY PURPOSE OR USE OF THE SOFTWARE, FREEDOM FROM INFRINGEMENT OR ANY OTHER REPRESENTATION OR WARRANTY WHATSOEVER WITH RESPECT TO THE SOFTWARE. COMPANY SHALL NOT BE LIABLE TO ANY USER OF THE SOFTWARE, FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, LIABILITY, LOSS OR DAMAGE CAUSED OR ALLEGED TO HAVE BEEN CAUSED BY THE SOFTWARE, EVEN IF COMPANY WAS AWARE OF THE POTENTIAL FOR SUCH DAMAGES AND LOSS TO OCCUR.

USER SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS COMPANY, ITS LICENSORS, DEALERS, INDEPENDENT CONTRACTORS, SHAREHOLDERS, DIRECTORS, EMPLOYEES, OFFICERS, AFFILIATES AND AGENTS, AND THE RESPECTIVE SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES AND AGENTS OF EACH OF THE FOREGOING, FROM AND AGAINST ANY AND ALL CLAIMS, ACTIONS, JUDGMENTS, LIABILITIES, COSTS AND EXPENSES (INCLUDING LEGAL FEES) RELATING TO OR ARISING FROM THE USE OR DISTRIBUTION OF USER APPLICATIONS OR SERVICES PROVIDED BY USER (INCLUDING, BUT NOT LIMITED TO, CLAIMS RELATING TO LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, INTELLECTUAL PROPERTY RIGHTS, U.S. EXPORT AND IMPORT LAWS, DEFECTIVE PRODUCTS, OR PRODUCT LIABILITY CLAIMS).

User expressly acknowledges that any modification of the Software, whether or not permitted, is beyond the control of Company, and as such, such modification shall void any warranties, express or implied, under this Agreement.

6. Controlling Law and Severability

This Agreement shall be governed by and construed in accordance with the laws of the United States and the State of Ohio, as applied to agreements entered into and to be performed entirely within Ohio between Ohio residents. The federal and state courts of the State of Ohio, County of Medina, shall have exclusive jurisdiction and venue over any dispute, proceeding or action arising out of or in connection with this Agreement or User's use of the Software. If venue is appropriate in federal court and that federal court is not located in Medina County, User and Company agree to litigate any disputes in a federal court located in Cuyahoga County, Ohio. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

7. Non-Binding Mediation

Company and User agree to submit the dispute to non-binding mediation before resorting to litigation. Mediation shall occur in Medina, Ohio before a single mediator jointly selected by the parties. The parties agree to each pay one-half of the mediator's fee.

Company and User agree to waive any possible arbitration claims unless Company and User later agree to arbitrate this dispute following mediation, wherein such arbitration shall be binding and incur in lieu of litigation.

8. Limitation of Liability and Fees

COMPANY'S TOTAL LIABILITY, INCLUDING ANY DAMAGES, SHALL NOT EXCEED THE TOTAL AMOUNT USER PAID TO COMPANY. SHOULD COMPANY BE FORCED TO MEDIATE, ARBITRATE, OR LITIGATE ANY DISPUTE AGAINST USER AND SHOULD COMPANY PREVAIL IN SUCH DISPUTE, USER SHALL REIMBURSE COMPANY FOR ALL OF ITS ATTORNEY FEES AND COSTS ASSOCIATED WITH THE ENTIRE DISPUTE, INCLUDING FEES OR COSTS INCURRED PRIOR TO ANY CLAIM BEING FILED AND ALL OF COMPANY'S COSTS, INCLUDING ATTORNEY'S FEES, ASSOCIATED WITH THE MEDIATION, ARBITRATION, OR LITIGATION.

9. Non-Waiver

The failure by Company at any time to enforce any of the provisions of this Agreement or any right or remedy available hereunder or at law or in equity, or to exercise any option herein provided, shall not constitute a waiver of such provision, right, remedy or option or in any way affect the validity of this Agreement. The waiver of any default by Company shall not be deemed a continuing waiver, but shall apply solely to the instance to which such waiver is directed.

10. Successors; Assigns

This Agreement shall be binding on and inure to the benefit of the parties and their respective successors and permitted assigns. Except as provided for herein, this Agreement may not be assigned by User without the prior written consent of Company.

11. Use of Site Image

User grants a perpetual, world-wide, royalty-free license to Company to use and publish one or more screen shot captures of any User web sites using the Software, User's trademarks, logos or names and/or otherwise list User as a licensee of Company; provided, however, no such license shall be granted to Company if User sends an e-mail to Company stating objecting to such license within ten (10) days of receiving the Software.

12. Complete Agreement

This Agreement constitutes the complete agreement between User and Company. No amendment or modification may be made to this Agreement except in writing signed by User and Company.

Please contact us with any questions or concerns regarding this Agreement.

Thirtyseven4™, L.L.C

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Thirtyseven4, L.L.C

Marketing, distribution or use by anyone barring the people authorized by Thirtyseven4, L.L.C is liable to legal prosecution.

Trademarks

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

Trademarks

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

About the Document

This user guide covers all the information needed to install and use Thirtyseven4 Antivirus on Windows desktop-based operating systems. You can use it as a handbook of Thirtyseven4 Antivirus. We have ensured that all the details provided in this guide are completely updated with the latest developments in the shipping.

We have followed a certain set of conventions to prepare this guide. The following are a list of conventions that are used in this document.


Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a Menu Title, Window Title, Checkbox, Drop-down Box, Dialog Box, Buttons, Hyperlinks, etc.
	This symbol indicates additional information or important information about the topic being discussed.
1. <Step 1> 2. <Step 2>	The numbered list and the instruction mentioned in each numbered list indicate actions that you need to perform.

Table of Contents

INSTALLING THIRTYSEVEN4 ANTIVIRUS	8
GETTING STARTED	8
SYSTEM REQUIREMENTS.....	9
HOW TO INSTALL THIRTYSEVEN4 ANTIVIRUS.....	11
UN-INSTALLING THIRTYSEVEN4 ANTIVIRUS.....	12
REGISTRATION, RE-ACTIVATION AND RENEWAL	13
REGISTRATION	13
REGISTERING ONLINE WITH INTERNET CONNECTION ON THE SAME PC	13
REGISTERING OFFLINE WITH INTERNET CONNECTION ON SOME OTHER PC	14
RE-ACTIVATION	15
RENEWAL	15
RENEWING ONLINE WITH INTERNET CONNECTION ON THE SAME PC.....	15
RENEWING OFFLINE USING INTERNET CONNECTION ON SOME OTHER PC.....	16
USING THIRTYSEVEN4 ANTIVIRUS	18
ABOUT THIRTYSEVEN4 DASHBOARD	18
RIGHT SHELL MENU OPTIONS.....	20
THIRTYSEVEN4 PROTECTION CENTER.....	21
FILES & FOLDERS.....	22
EMAILS	30
INTERNET & NETWORK.....	32
EXTERNAL DRIVES & DEVICES	33
QUICK ACCESS FEATURES	35
SCAN	35
PERFORMING A FULL SYSTEM SCAN	35
PERFORMING A CUSTOM SCAN.....	35
PERFORMING MEMORY SCAN.....	36
PERFORMING BOOT TIME SCAN	36
NEWS.....	36
THIRTYSEVEN4 MENUS.....	37
SETTINGS.....	37
AUTOMATIC UPDATE	37
INTERNET SETTINGS	38
REGISTRY RESTORE.....	39
SELF PROTECTION	39
PASSWORD PROTECTION.....	39
REPORT SETTINGS.....	40

REPORT VIRUS STATISTICS.....	40
RESTORE DEFAULT SETTINGS.....	40
TOOLS.....	41
HIJACK RESTORE	41
TRACK CLEANER.....	43
ANTI-ROOTKIT	43
CREATE EMERGENCY DISK	47
LAUNCH ANTIMALWARE	48
VIEW QUARANTINE FILES.....	49
USB DRIVE PROTECTION	49
SYSTEM EXPLORER	50
WINDOWS SPY	50
EXCLUDE FILE EXTENSIONS	50
REPORTS.....	51
HELP.....	52
HELP.....	52
SUPPORT.....	52
ABOUT.....	54
UPDATING THIRTYSEVEN4 ANTIVIRUS	55
UPDATING THIRTYSEVEN4 ANTIVIRUS FROM INTERNET	55
UPDATING THIRTYSEVEN4 ANTIVIRUS WITH DEFINITION FILES.....	56
UPDATE GUIDELINES FOR NETWORK ENVIRONMENT	56
CLEANING VIRUSES	57
CLEANING VIRUSES ENCOUNTERED DURING SCANS.....	57
CLEANING VIRUS ENCOUNTERED IN MEMORY	58
TECHNICAL SUPPORT	59
CONTACT US.....	59

Installing Thirtyseven4 Antivirus

Thirtyseven4 Antivirus has a simple installation procedure. During installation, read each installation screen, follow the instructions, and then click Next to continue.

Getting Started

Remember the following guidelines before installing Thirtyseven4 Antivirus on the system:

- A system with multiple anti-virus software installed, can be hazardous for the system. If any other anti-virus software is installed on the system, it needs to be un-installed before proceeding with Thirtyseven4 Antivirus installation.
- Close all open programs before proceeding with Thirtyseven4 Antivirus installation.
- We recommend you to keep a backup of your data in case your system is infected with viruses.
- Thirtyseven4 Antivirus must be installed with administrative rights.

System Requirements

To use Thirtyseven4 Antivirus, the system should meet the following minimum requirements:

- 850 MB of free Hard Disk Space
- DVD-ROM or CD-ROM drive
- Internet connection to receive updates
- Internet Explorer 6 or the latest browser

Operating Systems	Minimum Requirements
Windows 2000	<ul style="list-style-type: none">• 300 MHz Pentium (or compatible) processor• 256 MB RAM• Service Pack 4
Windows XP	<ul style="list-style-type: none">• 300 MHz Pentium (or compatible) processor• 256 MB RAM• Service Pack 2
Windows Vista	<ul style="list-style-type: none">• 1 GHz Pentium (or compatible) processor• 512 MB RAM
Windows 7	<ul style="list-style-type: none">• 1 GHz Pentium (or compatible) processor• For 32-bit: 512 MB RAM; For 64-bit: 1 GB RAM



- The requirement is applicable to both 32-bit and 64-bit operating systems unless specifically mentioned.
- The requirement is applicable to all flavors of the operating system.
- The requirements provided are minimum system requirements. Thirtyseven4 recommends system with higher configuration than the minimum requirements to obtain best results.
- To check the latest system requirements, visit www.thirtyseven4.com.

Clients that support email scan

The POP3 email clients that support the email scanning feature are as follows:

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

Clients that do not support email scan

The POP3 email clients and network protocols that do not support the email scanning feature are as follows:

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

SSL connections not supported

Email Protection does not support encrypted email connections that use Secure Sockets Layer (SSL). If SSL connections are being used then the emails are not protected by Email Protection.

Thirtyseven4 Anti-Rootkit Requirements

- This feature is not supported on 64-bit operating systems.
- It requires minimum 256 MB RAM installed on system.

Thirtyseven4 Self-Protection

- This feature is not supported on Microsoft Windows 2000 Operating System.

How to install Thirtyseven4 Antivirus

To begin installation, insert the Thirtyseven4 Antivirus CD in the CD or DVD drive. The autorun feature of the CD is enabled and it will automatically open a screen and provide a list of options. Sometimes the CD or DVD Drive does not automatically start a CD when it is inserted. In such case, to start the installation, please perform the following steps:

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

Please perform the following steps for a successful installation of Thirtyseven4 Antivirus:

1. Click **Install Thirtyseven4 Antivirus** to initiate the installation process.
2. The installation wizard will perform a pre-install virus scan of the system. This pre-install scan will scan the system memory for viruses. During the pre-install scan, if a virus is found active in memory, then:
 - a. The installer automatically sets the boot time scanner to scan and disinfect the system on next boot.
 - b. After disinfection of the system, the system will start and you need to re-initiate the installation. For more details refer to Boot Time Scan in User Guide.During the pre-install virus scan if viruses are not found in the in the system memory, then the installation will proceed further.
3. The End User License Agreement screen appears. Read the license agreement carefully. At the end of the license agreement there are two checkboxes: **Submit suspicious files** and **Submit statistics**. By default these two options are checked. If you do not wish to submit suspicious files or statistics or both, then uncheck these options. If you do not agree with the terms mentioned in the license agreement, click **Cancel** to discontinue the installation. If you agree with the terms mentioned, then check **I Agree** and click **Next** to continue the installation.
4. The Install Location screen appears. The default location where Thirtyseven4 Antivirus will be installed is displayed. The disk space required during installation is mentioned on the screen. If the default location has insufficient space, or to install Thirtyseven4 Antivirus on another location, click **Browse** to change the installation location otherwise click **Next** to continue the installation.
5. The installation progress screen appears. This screen displays the status of installation in the progress bar.
6. Upon completion, a screen appears that indicates Thirtyseven4 Antivirus was successfully installed on the system. Click **Register Now** to initiate the activation process or click **Register Later** to perform activation at some other time.

Un-installing Thirtyseven4 Antivirus

If due to any reasons you wish to uninstall Thirtyseven4 Antivirus, please perform the following steps:

1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Uninstall Thirtyseven4 Antivirus** to initiate the un-installation process.
2. The screen appears with the prompt **Do you want to Remove Thirtyseven4 Antivirus completely from your computer?** Click **No** to abort the un-installation. Click **Yes** to continue with the un-installation.
3. If the Password Protection is enabled for Thirtyseven4 Antivirus, then a screen appears which requires the password to proceed further. Enter the password and click **OK** to continue.
4. Thirtyseven4 Antivirus maintains a repository of Report Files, Quarantine Files and Backup Files. You have the option to retain or delete this repository during un-installation. By default the **Remove Report Files** and **Remove Quarantine/Backup Files** options are checked. Click **Next** to continue un-installation without saving the repository. If the repository is to be retained, uncheck the required options, or all the options, and click **Next** to continue with the un-installation.
5. The un-installation progress screen appears. This screen displays the status of un-installation in the progress bar.
6. Upon completion, a screen appears that indicates Thirtyseven4 Antivirus was successfully un-installed from the system. You can provide feedback and reasons for un-installing Thirtyseven4 Antivirus by clicking **Write to us the reason of un-installing Thirtyseven4 Antivirus**. Your feedback will help us to improve the product. Please note the product key for future reference. You can also click **Copy to clipboard**. Upon clicking Copy to clipboard, the Product Key will be copied to the windows clipboard. You can open a document and directly paste this information into the document. Restart is recommended after un-installation. To restart click **Restart Now**, or click **Restart Later** to continue working on the system and restart after some time.

Chapter 2

Registration, Re-activation and Renewal

Registration

Thirtyseven4 Antivirus needs to be registered upon installation to activate the copy. It is strongly recommended that you register the copy immediately after installation; otherwise without activation it cannot be further updated. If the product is not regularly updated it will not protect your system against the latest threats. Registered users will also get technical support through email.

You can register Thirtyseven4 Antivirus by any of the following methods:

- [Online with Internet connection on the same PC](#)
- [Offline with Internet connection on some other PC](#)

Registering online with Internet connection on the same PC

1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Activate Thirtyseven4 Antivirus**.
2. The Registration Wizard opens. Enter the 20-digit Product Key and click **Next** to continue.
3. The Registration Information appears. Enter details like **Purchased From** and **Register for**. Click **Next** to continue.
4. Provide personal details like **Name**, **Email Address**, **Contact Number**, **Country**, **State** and **City**. You can select the Country, State and City in the drop-down. In case your State/Province and City are not available in the list you can type the same in the respective boxes. Click **Next** to continue.
5. The entered details will be displayed. If any modifications are needed, click **Back** and modify the concerned fields or click **Next** to continue.
6. The activation progress screen appears displaying the progress of the activation.
7. The activation will be successfully completed. The expiry date is displayed. Click **Finish** to close the Registration Wizard.

Registering offline with Internet connection on some other PC

If you do not have an Internet connection on the system, then Thirtyseven4 Antivirus can be registered by filling the registration form on Thirtyseven4 website by visiting the offline activation page <http://173.192.146.76/useract/act2011> with any system having Internet connection. For example: Cyber cafe.

Offline registration involves the following steps:

- [Getting the details of Thirtyseven4 Antivirus installation.](#)
- [Visiting and filling offline registration form on Thirtyseven4 website using some other PC having Internet connection.](#)
- [Receiving <license>.key file.](#)
- [Activating Thirtyseven4 Antivirus installation using the <license>.key file.](#)

Getting the details of Thirtyseven4 Antivirus installation

Before visiting the offline activation page, as mentioned earlier, you should have the following details ready:

- Product Key: It will be pasted on the User Guide and/or inside the box. If the product is purchased online, then the product key can be obtained from the e-mail confirming the order.
- Installation Number: It can be obtained from the Activation Wizard by performing the following steps:
 1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Activate Thirtyseven4 Antivirus**.
 2. The Internet connection required screen appears. Click **Register Offline**.
 3. The offline activation screen appears. You can note down the offline activation URL and Installation Number or click **Copy to clipboard**. Upon clicking Copy to clipboard, the offline activation URL and the 12-digit Installation Number will be copied to the windows clipboard. You can open a document and directly paste this information into the document.
- A valid email address: A <license>.key file will be generated upon successful completion of offline activation. This file will be sent to the email address provided by you. You should ensure the correctness of the email address provided.

Visiting and filling offline registration web form using some other PC having Internet connection

You must visit the offline activation page <http://173.192.146.76/useract/act2011> and perform the following steps:

1. Click the hyperlink **Click here to proceed to Step 1**.
2. Enter the Product Key and Installation Number and click **Submit**.
3. Enter the details requested on the screen. The fields with a * are mandatory fields. Click **Submit** upon completion.

Receiving <license>.key file

You can download the <license>.key from the Acknowledgement screen upon successful completion of offline activation. The downloaded <license>.key file can be transferred to the PC, on which Thirtyseven4 Antivirus is installed, using a removable media.

The <license>.key file is also sent as an attachment to the email address provided. You can download the file from the email to a removable media and transfer it to the PC on which Thirtyseven4 Antivirus is installed.

Activating the Thirtyseven4 Antivirus installation using newly obtained <license>.key file

Once the <license>.key file is transferred to the PC having Thirtyseven4 Antivirus, please perform the following steps:

1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Activate Thirtyseven4 Antivirus**.
2. The Internet connection required screen appears. Click **Register Offline**.
3. The offline activation screen appears. Click **Browse** to locate the path where the <license>.key is stored and click **Next** to continue.
4. The activation will be successfully completed. Click **Finish** to close the Registration Wizard.

Re-activation

During the product validity period, you might need to format the system, or you might need to discontinue using Thirtyseven4 Antivirus on the existing system, to continue using it on another system. In such cases you are advised to re-activate Thirtyseven4 Antivirus upon re-installation.

The re-activation process is similar to the activation process, with just one exception: You do not have to enter the complete personal details again. Upon submitting the Product Key (and Installation Number in case of offline re-activation), the details will be displayed. You can just verify the details and complete the process.

Renewal

Once Thirtyseven4 Antivirus is activated, it displays the expiry date. This date indicates the period of validity of Thirtyseven4 Antivirus. Till this date, your system will be constantly protected from all the latest malware. Upon expiry, you need to renew Thirtyseven4 Antivirus by purchasing a renewal code. You can renew Thirtyseven4 Antivirus from Thirtyseven4 website, or from the nearest distributor or reseller.

You can renew Thirtyseven4 Antivirus by any of the following methods:

- [Online with Internet connection on the same PC](#)
- [Offline with Internet connection on some other PC](#)

Renewing online with Internet connection on the same PC

If your system has Internet connection then Thirtyseven4 Antivirus can be renewed by performing the following steps:

1. Click **Start -> Programs -> Thirtyseven4 Antivirus -> Thirtyseven4 Antivirus.**
2. If your copy of Thirtyseven4 Antivirus has expired then click **Renew Now** on the Thirtyseven4 dashboard. If your copy of Thirtyseven4 Antivirus has not expired, then click **About** under **Help** menu, and click **Renew Now.**
3. The Renewal wizard opens. Select **I want to renew using renewal code. I already have renewal code with me** option and click **Next.**
4. The Registration Information appears. Enter details like **Purchased From, Email Address** and **Contact Number.** Click **Next** to continue.
5. The license information such as **Current expiry date** and **New expiry date** will be displayed for your confirmation.
6. Click **Next** to proceed with renewal.
7. The copy of Thirtyseven4 Antivirus will be renewed. Click **Finish** to complete the renewal process.



- In case you do not have renewal code please select **I do not have renewal code with me. I want to purchase renewal code online** option and click **Buy Now.**
- In case your license is already renewed on Thirtyseven4 Activation Server to extend the license validity of your copy, please select **I have already renewed my license. Please update my license from server** and click **Next.**
- If you have purchased an additional renewal code, then the renewal can be performed only after 10 days of the current renewal.

Renewing offline using Internet connection on some other PC

If you do not have Internet connection on the system, then Thirtyseven4 Antivirus can be renewed by filling the renewal form on Thirtyseven4 website by visiting the offline renewal page <http://173.192.146.76/useract/renew> with any system having Internet connection. For example: Cyber cafe.

Offline renewal involves the following steps:

- [Getting the details of Thirtyseven4 Antivirus installation.](#)
- [Visiting and filling offline renewal web form using some other PC having Internet connection.](#)
- [Receiving <license>.key file.](#)
- [Renewing Thirtyseven4 Antivirus using the newly obtained <license>.key file.](#)

Getting the details of Thirtyseven4 Antivirus installation

Before visiting the offline renewal page, as mentioned earlier, you should have the following details ready:

- Product Key and Installation Number: These can be obtained from the Renewal form by performing the following steps:
 1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Thirtyseven4 Antivirus**.
 2. If Thirtyseven4 Antivirus has expired then click **Renew Now** on the main window. If Thirtyseven4 Antivirus has not expired, then click **Help** -> **About** and click **Renew Now**.
 3. Click **Renew Offline**.
 4. The offline renewal details screen appears. You can note down the offline renewal URL, Product Key and Installation Number or click **Copy to clipboard**. Upon clicking Copy to clipboard, the offline renewal URL, the 12-digit Installation Number and the 20-digit Product Key will be copied to the windows clipboard. You can open a document and directly paste this information into the document.
- A valid email address: A <license>.key file will be generated upon successful completion of offline renewal. This file will be sent to the email address provided. You should ensure the correctness of the email address provided.

Visiting and filling offline renewal web form using some other PC having Internet connection

You can visit the offline renewal page <http://173.192.146.76/useract/renew> with perform the following steps:

1. Click the hyperlink **Click here to proceed to Step 1**.
2. Enter the **Product Key**, **Installation Number**, **Purchased Renewal Code** and **Purchased From** details and click **Submit**.
3. Upon verification of the provided data, the next screen will display the user name, registered email address & contact number. If your email address and contact number has changed, then you have the option to update it in this form. Click **Submit**.

Receiving <license>.key file

You can download the <license>.key from the Acknowledgement screen upon successful completion of offline renewal. The downloaded <license>.key file can be transferred to the PC, on which Thirtyseven4 Antivirus is installed, using a removable media.

The <license>.key file is also sent as an attachment to the email address. You can download the file from the email to a removable media and transfer it to the PC on which Thirtyseven4 Antivirus is installed.

Renewing Thirtyseven4 Antivirus using the newly obtained <license>.key file

Once the <license>.key file is transferred to the PC having Thirtyseven4 Antivirus, please perform the following steps:

1. Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Thirtyseven4 Antivirus**.
2. If Thirtyseven4 Antivirus has expired then click **Renew Now** on the Thirtyseven4 dashboard. If Thirtyseven4 Antivirus has not expired, then click **Help** -> **About** and click **Renew Now**.
3. Click **Renew Offline**.
4. The offline renewal details screen appears. Click **Browse** to locate the path where the <license>.key is stored and click **Next** to continue.
5. The copy of Thirtyseven4 Antivirus will be renewed and the renewed validity of Thirtyseven4 Antivirus will be displayed. Click **Finish** to close the Registration Wizard.
6. The copy of Thirtyseven4 Antivirus will be renewed and the renewed validity of Thirtyseven4 Antivirus will be displayed. Click **Finish** to close the Registration Wizard.

Chapter 3

Using Thirtyseven4 Antivirus

Thirtyseven4 Antivirus can be accessed from the desktop in any of the following ways:

- By clicking **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Thirtyseven4 Antivirus** from the desktop.
- By double-clicking the **Virus Protection** icon on the system tray.
- By right-clicking the **Virus Protection** icon on the system tray and clicking **Thirtyseven4 Antivirus**.
- By clicking **Start** -> **Run**, typing **Scanner** and pressing the **Enter** key.

Thirtyseven4 Antivirus, with its unique **Graphical User Interface (GUI)**, is designed with the focus to simplify the task of securing your PC.

The Main Window or the Dashboard will serve as the interface to all the features of Thirtyseven4 Antivirus. You can also access the Dashboard and certain features of Thirtyseven4 Antivirus from the Windows system tray. Thirtyseven4 protects the entire system even with the default settings. You can start Thirtyseven4 Antivirus to check the status of Thirtyseven4 protection, to manually scan, to view reports and update the product.

About Thirtyseven4 Dashboard

The dashboard is split into three sections. They are:

- Thirtyseven4 Protection Center
- Quick Access Features
- Thirtyseven4 Menus

Thirtyseven4 Protection Center provides indication of the security status of Thirtyseven4 Antivirus with the help of colored icons. The colored icons and their specific meaning are as follows:

Green	This indicates that Thirtyseven4 Antivirus is configured with optimal settings and your system is protected.
Red	This indicates that Thirtyseven4 Antivirus is not configured with optimal settings and your immediate attention is needed. The action corresponding to the message needs to be executed immediately to keep your system protected.
Orange	This indicates that a feature of Thirtyseven4 Antivirus needs your attention, if not immediately, but at the earliest.

There are four categories of protection offered by Thirtyseven4 Antivirus. These four categories are the areas or medium through which a malware can gain access and infect your system. Each category has many options of protection. The categories and their description are provided in the following table:

Files & Folders	Allows you to configure settings to protect your files and folders against malwares. Also allows you to customize scan options and actions.
Emails	Allows you to configure settings that protect your system against malicious threats that try to sneak into your system through emails.
Internet & Network	Allows you to configure settings that protect your system against malicious threats that try to sneak into your system when you are browsing the Internet, or when you are perform to-and-fro transfer of files in the network.
External Drives & Devices	Allows you to configure settings that protect your system against malicious threats from external drives like CDs, DVDs and USB-based drives.

Quick Access Features deals with the frequently used features. Quick Access Features are as follows:

News	Provides you the latest bytes of information from Thirtyseven4 Labs.
Scan	Launches the scanner that scans the entire system, user-defined locations, system memory and to perform boot time scan.

Thirtyseven4 Menus deals with configuring the general settings of Thirtyseven4, tools for preventing virus infection and diagnosing the system, reports of the activities of the features and access help and license details. The following menus are available:

Settings	Allows you to customize important settings of Thirtyseven4 Antivirus.
Tools	Provides access to important tools that can help you keep the system and its software protected.
Reports	Provides detailed logs of important activity performed by Thirtyseven4 Antivirus.
Help	Provides vital information related to software and licensing information. Also provides support related details.

The features of the following buttons and settings are common irrespective of where they are placed:

Cancel	Exit from the feature being accessed.
Default	Configures default settings.
Save Changes / OK	Saves changes made to settings. If changes are made and if you try to exit from the screen, then a prompt will appear saying Do you want to continue without saving? Click Yes if you do not want to save the changes, else click No if you want to save the changes.
ON/OFF	Click the button to keep the setting to ON or OFF . ON means the feature is enabled and OFF means the feature is disabled.
Help	Displays Help for the feature or the dialog box opened.

Right Shell Menu Options

You can right-click the Virus Protection icon on the Windows System Tray and access the following features:

Open Thirtyseven4	Click this to launch Thirtyseven4 Antivirus.
Launch AntiMalware	Click this to launch Thirtyseven4 AntiMalware.
Enable / Disable Entertainment Mode	Click this to enable / disable all Thirtyseven4 prompts and notifications.
Enable / Disable Virus Protection	Click this to enable / disable Thirtyseven4 Virus Protection.
Update Now	Click this to update Thirtyseven4 Antivirus.
Scan Memory	Click this to scan system memory for viruses.




You can also scan specific files and folders for malicious behavior and activity by right-clicking the desired file and folder and selecting **Thirtyseven4 Antivirus Scan**.

Chapter 4

Thirtyseven4 Protection Center

Thirtyseven4 Protection Center is your instant interface to vital protection settings that can affect files, folders, emails, etc. It also allows users to configure protection against viruses that try to gain entry through Internet, external drives and emails. Thirtyseven4 Protection Center is split into two sections.

The top strip of the Protection Center acts as a security status indicator which displays color coded icons that indicates the security status at any moment. The icons and the description of their status are as follows:

	If the icon is red, it indicates that Thirtyseven4 Antivirus requires your immediate attention. The icon turns red if your copy is not activated, if your license has expired or if some vital settings have been disabled.
	If the icon is green, it indicates that Thirtyseven4 Antivirus is safe and the settings maintained are optimal to protect your system.
	If the icon is Orange, it indicates that Thirtyseven4 Antivirus is providing you with a warning that might not require your immediate attention, but might require your attention at the earliest.

Each colored icon has an action associated with it which needs to be executed by the user.

Thirtyseven4 Protection Center also provides four categories of protection and customizable settings. These four categories are the areas or medium through which a malware can gain access and infect your system. The four categories of protection are as follows:

- [Files & Folders](#)
- [Emails](#)
- [Internet & Network](#)
- [External Drives & Devices](#)

Each of these categories displays vital features of that particular category, below the category icon. These features have to be enabled all the time. If you want to disable these features, for some reasons, then the corresponding category icons will turn red. The categories and their corresponding features displayed on the Dashboard are as follows:

Files & Folders	Virus Protection, DNA Scan
Emails	Email Protection
Internet & Network	Firewall Protection, Browsing Protection
External Drives and Devices	Autorun Protection, Scan External Drives

Files & Folders

Files & Folders option in the Protection Center of the Dashboard allows you to customize the settings that concern the protection of files and folders on your system. It allows you to configure the following settings:

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

Scan Settings

Scan Settings lets you customize the way a scan is to be performed and the action that needs to be taken when a virus is detected. The default settings are optimal and can provide the required protection a system needs.

Scan Settings feature in Thirtyseven4 Antivirus can be accessed by clicking **Files & Folders** -> **Scan Settings** from the *Dashboard*. The following options are available:

Select Scan Mode	
Automatic (Recommended)	Select Automatic (Recommended) scan mode which is the default scan mode configured to provide complete protection for the system. This setting is recommended for achieving best results from the scan and is the ideal option for novice users.
Advanced	Select Advanced mode if you want to customize the scanning behavior. This is ideal for experienced users only. Selecting this option activates the Configure button. To know more about configuring the scanner, refer Configuring the scanner .

Select action to be performed when virus is found	
Repair	During a scan if a virus is found, then it will repair the file or automatically quarantine it, if it cannot be repaired. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. If the infectious file is a Backdoor, Worm, Trojan, or Malware then Thirtyseven4 Antivirus automatically deletes the file.
Delete	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing details about all the actions taken and other scan details. Files deleted in such a manner cannot be recovered.
Skip	In this mode the scanner scans for viruses, skips them, when the scan is over a summary window (report) appears providing all the scan details.
Backup before taking action	Scanner will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

After making the selection click **Save Changes** to apply the settings.

Configuring Advanced Scan Mode

If you select *Advanced* scan mode, it activates the **Configure** button. Clicking the **Configure** button will provide you with the following options:

Scan executable files	Select Scan executable files if you want the scanner to scan only executable files.
Scan all files (Takes longer time)	Select Scan all files if you want the scanner to scan all files and types. If this option is selected, then the scanning process slows down considerably.

Scan archive files

If **Scan archive files** feature is checked then the scanner will also scan archived files like zip files, archive files, etc. If **Scan archive files** feature is un-checked then the scanner will skip archive files during the scan. It will also de-activate the **Configure** button. By default, this feature is checked. If this feature is checked, then the **Configure** button is active and allows you to configure the way scanner should treat malicious archive files. Clicking the Configure button gives you the following option:

Select action to be performed when virus is found	
Delete	Deletes an archive containing virus-infected file without notifying you.
Quarantine	During scan if a virus is found in an archive file, then the archive will be moved to Quarantine.
Skip	In this mode the scanner scans for viruses under archive, skips the virus and archive file without taking any action.

Archive Scan level	Set the level to scan inside an archive. By default it is set to level 2. Increasing the default Archive Scan Level may affect the scanning speed.
---------------------------	--

Select the type of archive that should be scanned

The list of archive file types that can be scanned during the scanning process is available in this section. A few important archive file types are checked by default. You can customize the same.

Select All	Click Select All to check all the archive file types displayed in the list.
Deselect All	Click Deselect All to un-check all the archive file types displayed in the list.

Scan packed files

If **Scan packed files** feature is checked then the scanner will also scan packers. Packers are files that pack together many files, or compress a single file to reduce file size. These files do not need a third party application to get unpacked. They have an inbuilt functionality of packing and unpacking. Packers can also be used as tools to spread malware by packing a malicious file along with a set of files. When such packers are unpacked it can cause harm to your PC. If **Scan packed files** feature is un-checked then the scanner will skip packers during the scan.

List files while scanning

If **List files while scanning** is checked then the entire list of files scanned, along with their scanned status (i.e. Clean or Infected), will be displayed in the **Actions** tab of the particular scan and also in the Scanner Reports.

Scan mailboxes

If **Scan mailboxes** feature is checked then the scanner will scan the mail box of Outlook Express 5.0 and higher versions (inside the **DBX** files). Viruses like KAK, JS.Flea.B etc, remain inside 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). If Scan mailboxes feature is un-checked then the scanner will skip mailboxes during the scan. By default, **Scan mailboxes** feature is checked which activates the following two options:

Quick scan of mailboxes	Select Quick scan of mailboxes if you want to skip all previously scanned messages and to scan only new messages. By default, this option is selected.
Thorough scan of mailboxes	Select Thorough scan of mailboxes if you want to scan all the mails in the mailbox all the time. Selecting this option will considerably affect the speed as the size of the mailbox increases.



The options **Quick scan of mailboxes** and **Thorough scan of mailboxes** are activated only if the **Scan mailboxes** feature is checked.

Virus Protection

Virus Protection continuously monitors the system by working in the background and trapping any malicious files that have tried to sneak from email attachments, Internet downloads, network file transfer, file execution, etc.

Virus Protection feature in Thirtyseven4 Antivirus can be accessed by clicking **Files & Folders** from the *Dashboard*. By default Virus Protection is enabled and is set to **ON**. You can disable Virus Protection by clicking the button. Thirtyseven4 recommends that you keep it enabled to secure your system from any potential threats at any point of time.

ON	The ON state indicates that Virus Protection feature is enabled.
OFF	<p>The OFF state indicates that Virus Protection feature is disabled. If you click the ON/OFF button when Virus Protection is set to ON, then a prompt is displayed that recommends against turning off Virus Protection. You can select one of the following options from the Select Action drop-down box:</p> <ul style="list-style-type: none">• Turn on after 15 minutes• Turn on after 30 minutes• Turn on after 1 hour• Turn on after next reboot• Permanently disable <p>Select an option and click OK button. You will see that Virus Protection icon's color has changed from Green to Red in Windows System Tray. It means that Virus Protection has been disabled temporarily or permanently based on your selection. If you have selected Turn on after 15 minutes / 30 minutes / 1 hour then the icon's color will change back from Red to Green, based on the time frame selected, to indicate that Virus Protection has been enabled. If you have selected Turn on after next reboot, then the icon's color will change back to Green at the next reboot. If you have selected Permanently disable then the icon's color will remain Red until you enable Virus Protection manually.</p>

You can customize Virus Protection by clicking **Files & Folders** -> **Virus Protection** from the *Dashboard*. The following options are available:

Display alert messages	Display alert messages feature, if checked or enabled, displays an alert message whenever a malware is detected. If un-checked, it will not display an alert message whenever a malware is detected. By default this feature is checked.
-------------------------------	--

Select action to be performed when virus is found

You can configure the action that needs to be carried out when a malware is detected by Virus Protection. The following actions are available:

Repair	Attempts to repair the file and quarantines it automatically in case if it cannot be repaired.
Delete	Deletes a virus-infected file without notifying you. Files deleted in such a manner cannot be recovered.
Deny access	Prevents you from using a virus-infected file.
Backup before taking action	Virus Protection will keep a copy of infected file before disinfecting it. (Files that are stored in backup can be restored from Quarantine menu.)

After making the selection click **Save Changes** to apply the settings.

DNAScan

DNAScan is Thirtyseven4's indigenous technology to detect and eliminate new and unknown malicious threats in the system. Additionally it copies the suspected file in the Quarantine directory before taking any action. Quarantined suspicious files can be submitted to our research lab for further analysis. This submission is important to curb the wild spread of new malicious threats. Suspicious file submission ensures the detailed analysis of the file in our research lab. After the detailed analysis it can be added in the known threat signature database which will be provided in updates to all the users. This can be only possible if they are detected and eliminated before their wild spread. DNAScan technology successfully traps suspected files with very less false alarms.

Whenever DNAScan detects a new malicious threat in your system it informs you, or asks for your action during memory scanning if the scanning is set with Prompt settings. One copy of DNAScan suspected files will always be quarantined which can later be submitted to research lab for further detailed analysis. The submission can be done automatically or manually through email. The submission takes place whenever Thirtyseven4 Antivirus updates itself and finds new DNAScan suspected files in the Quarantine folder. It sends new DNAScan suspicious quarantined files in an encrypted file format to Thirtyseven4 research lab.

DNAScan feature in Thirtyseven4 Antivirus can be accessed by clicking **Files & Folders** from the *Dashboard*. By default DNAScan is enabled and is set to **ON**. You can disable DNAScan by clicking the button. Thirtyseven4 recommends that you keep it enabled to secure your system from any potential threats at any point of time.

IF DNAScan Protection is disabled then it will remain disabled during Scan, Virus Protection and Email Scans.

Configuring the submission settings

DNAScan suspected files can be submitted to research lab of Thirtyseven4 through email. Submission of the suspected files is at your liberty. Submission of the DNAScan suspected files depend on the below mentioned settings:

Do not submit files	This option does not let DNAScan submit the suspected files to Thirtyseven4 research lab.
Submit files	DNAScan suspected files can be submitted to Thirtyseven4 research lab. If Show notification while submitting files option is checked, then Thirtyseven4 prompts for permission before submission of samples to Thirtyseven4 Research Lab. If Show notification while submitting files option is not checked, then Thirtyseven4 submits the suspicious files without notifying you.



Manual submission can be done through the Quarantine tool.

Block Suspicious Packed Files

Suspicious Packed Files are files that are packed using pre-defined list of suspicious packers. These packers are mostly used to pack malicious files, and when unpacked can cause a lot of harm to the computer.

Block Suspicious Packed Files feature in Thirtyseven4 Antivirus can be accessed by clicking **Files & Folders** from the *Dashboard*. Click the button to either enable or disable Block Suspicious Packed Files feature. By default, Block Suspicious Packed Files feature is enabled and set to **ON**.

Automatic Rogueware Scan

The Automatic Rogueware Scan feature in Thirtyseven4 Antivirus automatically scans and removes critical level rogueware and fake anti-virus software.

Automatic Rogueware Scan feature in Thirtyseven4 Antivirus can be accessed by clicking **Files & Folders** from the *Dashboard*. Click the button to either enable or disable Automatic Rogueware Scan files feature. By default, Automatic Rogueware Scan feature is enabled and set to **ON**.

Scan Schedule

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

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

To create a new schedule scan

1. Click **Files & Folder** -> **Schedule Scan** from the *Dashboard*.
2. The Schedule Scan wizard opens. Click **New**.
3. Name your custom schedule scan under **Scan Name**. For example: *My Scan*.
4. Select **Start at First Boot** to schedule the scanner to scan at first boot of the day. When you select Start at First Boot, you don't have to specify the time of the day to start the scan. Scan will take place only during the first boot no matter at what time you start the system. Otherwise set the frequency and time at which you want to scan the system. Most of the frequency options include additional options (Every day (s) and Repeat scan after every) that let you further refine your schedule scan. Select the schedule scan priority from **Low** or **High**. Set the additional options as necessary.
5. Provide **User Name** and **Password**.
6. Under **Scan Settings**, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advance options while scanning. By default, setting has been set for adequate options for scanning.
7. When you are done, press **Next**.
8. Click **Add Folders**.
9. Select the Drives, folder or multiple folders to be scanned and press **OK**. You can configure **Exclude Subfolder** while scanning of a specific folder. This will ignore scanning inside the subfolders while scanning. e.g. If you select C:\ drive for scan along with selecting Exclude Subfolder option, this will initiate scan for files available at the root of C:\ drive only.
10. Click **Next**.
11. Review the summary of your custom scheduled scan.
12. When you are done, click **Finish**.

To edit a scheduled scan

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

1. Click **Files & Folders** -> **Scan Schedule** from the *Dashboard*.
2. Highlight the desired Schedule Item from the list and click **Edit**.
3. Change the schedule as desired.
4. When you are done, click **Next**.
5. Change the scan area as desired.
6. Click **Next**.
7. Review the summary of your custom scheduled scan.
8. When you are done, click **Finish**.

To delete a scan schedule

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

1. Click **Files & Folders** -> **Scan Schedule** from the *Dashboard*.
2. Highlight the desired Schedule Item from the list and click **Remove**.
3. The following prompt appears: **Do you want to remove the Schedule Scan?** Click **Yes** to delete the Schedule Item.

Exclude Files & Folders

You can configure Thirtyseven4 Antivirus to skip scanning of certain files or folders. Scanning can be excluded in the cases, of known virus detection, DNAScan and packer identification.

Following scanning modules can be excluded

- Scanner
- Virus Protection
- Memory Scanner
- DNAScan

To exclude Files or Folders from scanning, please perform the following steps:

1. Click **Files & Folders** -> **Exclude Files & Folders** from the *Dashboard*.
2. The Exclude Files & Folders screen opens. Click **Add**.
3. Click File Icon or Folder icon for the exclusion.
4. Select the desired file or folder for exclusion from scanning.
5. Check **Include Subfolder** option to exclude subfolders from the scan as well. Click **OK** to complete the process.

The following are a few guidelines:

- If you are getting a 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 for scanning of **DNAScan**.

Quarantine & Backup

Quarantine & Backup feature allows you to configure the number of days to retain the quarantined or backup files. To access this feature click **Files & Folders** -> **Quarantine & Backup** from the *Dashboard*.

The following can be configured in Quarantine & Backup:

Delete quarantine/backup files after	If this feature is checked then it enables deletion of quarantine/backup files after the selected option in the drop-down box. By default the value is 30 days. If this feature is un-checked then it disables deletion of quarantine/backup files and retains all the files. The list of files in Quarantine will be listed below this feature.
View Files	Click this button to view the files under Quarantine and Backup. To know more refer View Quarantine Files .

Emails

Emails option in the Protection Center of the Dashboard allows you to customize the settings that concern the protection of emails entering your mailbox. It allows you to configure the following settings:

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

Email Protection

Email Protection feature allows you to customize the action that needs to be taken when a malware is detected in mail. The default settings are optimal and can provide the required protection to the mailbox from malicious mails.

Email Protection feature in Thirtyseven4 Antivirus can be accessed by clicking **Emails** from the *Dashboard*. By default Email Protection is enabled and is set to **ON**. You can disable Email Protection by clicking the button. Thirtyseven4 recommends that you keep it enabled to secure your mailbox from any potential threats at any point of time.

You can customize Email Protection by clicking **Emails** -> **Email Protection** from the *Dashboard*. The following options are available:

Display alert message	<p>Virus found alert will be shown in case a virus is found in an email or attachment. Display Alert Message will contain following information:</p> <ul style="list-style-type: none">• Virus Name• Sender Email Address• Email Subject• Attachment Name• Action Taken
Select action to be performed when virus is found	
Repair	Attempts to repair the malicious attachment. If the attachment cannot be repaired then it will be deleted.
Delete	Selecting this option will delete the infected attachment while downloading mails.
Backup before taking action	Email Protection will keep a copy of infected email before disinfecting it. (Files that are stored in backup can be restored by clicking Tools -> View Quarantine Files from the <i>Dashboard</i> .)

Attachment Control Settings

Block attachments with multiple extensions	Checking this feature enables blocking of attachment in emails with multiple extensions. Worms commonly use multiple extensions. Enabling this option will block multiple extension attachments in incoming e-mails. It prevents infection from new worms, and thus protects your system. Un-checking of this feature disables blocking of attachment in emails with multiple extensions. By default this feature is checked or enabled.
Block emails crafted to exploit vulnerability	Checking this feature enables blocking of emails whose sole purpose is to exploit vulnerabilities of mail clients. Enabling this option will block emails, which contain vulnerability like MIME, IFRAME, etc. Un-checking of this feature disables the blocking of emails that are crafted to exploit vulnerability. By default this feature is checked or enabled.
Enable attachment control	<p>Checking this feature enables attachment control that allows you to customize blocking of email attachments with specific extensions or all extensions. Un-checking this feature does not provide you with the option to customize the type of mail attachments that can enter your mailbox. By default this feature is disabled. When enabled it provides the following options:</p> <p>Block all attachments</p> <p>Selecting this option blocks all types of attachments in emails.</p> <p>Block user specified attachments</p> <p>Selecting this option allows you to customize the type of email attachments you can receive and block. If this option is selected, Configure button is activated. Click Configure and configuration dialog appears. Perform the following steps to block specific extensions:</p> <ol style="list-style-type: none">1. If you wish to block the extensions mentioned in the list just retain the ones you want to block and delete all other extensions using the Delete button. If you wish to configure default extensions for blocking then click Default button.2. If the desired extension is not in the list, enter the extension and click Add button. Perform the previous step again to configure.3. Click OK to save changes.

Trusted Email Clients Protection

Trusted Email Clients Protection is, by default, configured to support most of the popularly used email clients like Eudora. If your email client is different from the ones provided in the list, then you can simply add the same in the trusted email client list.

Trusted Email Clients Protection feature in Thirtyseven4 Antivirus can be accessed by clicking **Emails** from the *Dashboard*. By default Trusted Email Clients Protection is enabled and is set to **ON**. You can disable Trusted Email Clients Protection by clicking the button.

To add email client, perform the following steps:

1. Click **Emails** -> **Trusted Email Clients Protection** from the *Dashboard*.
2. Click **Browse** and select the trusted client.
3. Click **Add** to add the email client into trusted email client list.
4. Click **Save Changes**.

Internet & Network

Internet & Network option in the Protection Center of the Dashboard allows you to customize the settings that concern the protection of your system from malicious files that can sneak into your system during online activities like banking, shopping, surfing etc. It allows you to configure the following settings:

- [Firewall Protection](#)
- [Browsing Protection](#)
- [Malware Protection](#)

Firewall Protection

Firewall Protection feature works silently in the background and monitors network activity for malicious behavior to ensure their elimination before the malwares can reach the system. The method of detecting malicious network activity is done by Intrusion Detection System and the method of elimination of malicious network activity is done by Intrusion Prevention System.

Firewall Protection in Thirtyseven4 Antivirus can be accessed by clicking **Internet & Network** from the *Dashboard*. Click the button to either enable or disable Firewall Protection feature. By default, Firewall Protection feature is enabled and set to **ON**.

Browsing Protection

Browsing Protection feature blocks malicious websites. Browsing Protection in Thirtyseven4 Antivirus can be accessed by clicking **Internet & Network** from the *Dashboard*. Click the button to either enable or disable Browsing Protection feature. By default, Browsing Protection feature is enabled and set to **ON**.

Malware Protection

Malware Protection feature safeguards your PC from Internet related threats like spywares, adwares, keyloggers, riskwares etc. Malware Protection in Thirtyseven4 Antivirus can be accessed by clicking **Internet & Network** from the *Dashboard*. Click the button to either enable or disable Malware Protection feature. By default, Malware Protection feature is enabled and set to **ON**.

External Drives & Devices

External Drives & Devices option in the Protection Center of the Dashboard allows you customize the settings that concern protection of your system against malware that may try to sneak in through external devices or drives like CDs, DVDs, USB-based drives, etc. External Drives & Devices option allows you to configure the following settings:

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

Autorun Protection

Autorun Protection feature protects your system from autorun malware that tries to sneak into your system from USB-based devices or CDs / DVDs using the autorun feature of the installed operating system.

Autorun Protection feature in Thirtyseven4 Antivirus can be accessed by clicking **External Drives and Devices** from the *Dashboard*. Click the button to either enable or disable Autorun Protection feature. By default, Autorun Protection feature is enabled and set to **ON**.

Scan External Drives

USB-based drives should always be scanned for viruses before accessing it from your system, as these devices have become the medium for quick transfer of malware from one system to another. The Scan External Drives feature, if enabled, always prompts you to scan USB-based drives as soon as they are attached to your system. By default, this feature is enabled.

Scan External Drives feature in Thirtyseven4 Antivirus can be accessed by clicking **External Drives and Devices** from the *Dashboard*. Click the button to either enable or disable Scan External Drives feature. By default, Scan External Drives feature is enabled and set to **ON**.

You can customize the scanning of USB-based drives by clicking **Scan External Drives**. The following two options will be available:

Scan files on the root of the drive only	Selecting this option ensures that only the files on the root drive are scanned. The files within the folders on the root drive are skipped. This option is quick but less safe. By default, this option is selected.
Scan full drive	Selecting this option ensures that all the files on the USB-based drive are scanned. This option is slow but safe.

After making the selection click **Save Changes** to apply the settings.



Scan External Drives feature will not be performed if the feature **Data Theft Protection** is enabled, and its option **Block complete access to external drives** is selected.

Data Theft Protection

Data Theft Protection is used to block to-and-fro transfer of data between the system and USB drives. This feature ensures protection of confidential information on your system by blocking transfer of data from the system to these drives. It also blocks transfer of data from the USB drives to the system protecting your system from malware that can infect your system.

Data Theft Protection feature in Thirtyseven4 can be accessed by clicking **External Drives and Devices** from the *Dashboard*. Click the button to either enable or disable Data Theft Protection feature. By default, Data Theft Protection is **OFF**.

You can customize the protection provided by the feature by clicking **Data Theft Protection**. The following two options will be available:

Read only and no write access to external drives	Selecting this option allows transfer of data from the USB drives to the system but not from the system to the USB drives. By default this option is selected.
Block complete access to external drives	Selecting this option blocks to-and-fro transfer of data between the system and the USB drive.

After making the selection click **Save Changes** to apply the settings.

Chapter 5

Quick Access Features

Quick Access Features provides you with quick access to important features like Scan and also provides latest news about Thirtyseven4.

Scan

If virus protection is enabled with default setting, a manual scan will not be needed as the system will be continuously monitored and protected. However, you can manually scan the entire computer, drives, network drives (mapped drives), USB data storage drives, folders, or files as per your wish. Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan by clicking **Files & Folders** -> **Scan Settings** from the dashboard.

Performing a Full System Scan

A full system scan scans all boot records, drives, folders and files on your computer (excluding mapped network drives). To perform a full system scan, please perform the following steps:

1. Start **Thirtyseven4 Antivirus**.
2. In the Thirtyseven4 Antivirus main window, click **Scan** on the lower side of right pane.
3. Click **Scan** -> **Full System Scan** on the Thirtyseven4 Dashboard.
4. The scan will begin. Upon completion of the scan, you can view the scan report under **Reports**.

Performing a Custom Scan

To perform a scan of specific files or folders, please perform the following steps:

1. Start **Thirtyseven4 Antivirus**.
2. In the Thirtyseven4 Antivirus main window, click **Scan** on the lower side of right pane.
3. Click **Scan** -> **Custom Scan** on the Thirtyseven4 Dashboard.
4. Click **Add** to locate the path of the desired Folder that is to be scanned. You can select multiple folders for scan.
5. Once the selection is made, click **Start Scan**.
6. The scan will begin. Upon completion of the scan, you can view the scan report under **Reports**.

Performing Memory Scan

To perform a memory scan, please perform the following steps:

1. Start **Thirtyseven4 Antivirus**.
2. In the Thirtyseven4 Antivirus main window, click **Scan** on the lower side of right pane.
3. Click **Scan -> Memory Scan** on the Thirtyseven4 Dashboard.
4. The scan will begin. Upon completion of the scan, you can view the scan report under **Reports**.

The following fields will be displayed in the Status tab during a scan:

Files scanned	Displays the total number of files scanned.
Archive/Packed	Displays the number of scanned archive or packed files among the total number of files.
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 detected that were repaired.
Files quarantined	Displays the number of malicious files detected that were quarantined.
Files deleted	Displays the number of malicious files detected that were deleted.
I/O errors	Displays the number of I/O errors occurred during the scan.
Scanning status	Displays the status of the scan being performed.

Performing Boot Time Scan

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

1. Start **Thirtyseven4 Antivirus**.
2. In the Thirtyseven4 Antivirus main window, click **Scan** on the lower side of right pane.
3. Click **Scan -> Boot Time Scan** on the Thirtyseven4 Dashboard.
4. A confirmation prompt will be displayed to set boot time scanner on next boot. Click **Yes**.
5. To scan the system immediately, click **Yes** to restart the system. To scan the system later at next boot click **No**.

News

The News section displays the latest bytes of information and developments from Thirtyseven4, L.L.C.

Chapter 6

Thirtyseven4 Menus

Thirtyseven4 Menu gives you instant access to tools, settings, reports and help topics. Thirtyseven4 Menus are on the top right corner of the dashboard and are always available irrespective of the feature being accessed. Thirtyseven4 Menus are as follows:

- [Settings](#)
- [Tools](#)
- [Reports](#)
- [Help](#)

Settings

Thirtyseven4 Antivirus provides you the option to customize the functioning of certain settings of Thirtyseven4 Antivirus. The settings that can be customized are as follows:

- [Automatic Update](#)
- [Internet Settings](#)
- [Registry Restore](#)
- [Self Protection](#)
- [Password Protection](#)
- [Report Settings](#)
- [Report Virus Statistics](#)
- [Restore Default Settings](#)



The default settings that are configured are enough to provide complete security to your PC. We recommend that you keep the default settings intact and not change the settings unless absolutely required.

Automatic Update

Automatic Update ensures that Thirtyseven4 Antivirus is updated with the latest virus signatures to protect your system from the latest malwares. Automatic Updates requires an Internet connection to download the updates from the Thirtyseven4 server. By default the Automatic Update is enabled or is set to **ON**. Although it is not recommended, you can disable Automatic Update by clicking the **ON/OFF** button.

Configuring Automatic Update

Show update notification window	By default this feature is enabled. This ensures that a notification pops-up after each update of Thirtyseven4 Antivirus. To disable this feature, just uncheck the checkbox and click Save Changes .
--	--

Select the update mode

Download from Internet	By default this option is selected. This option downloads the updates to your system from Thirtyseven4 server.
Pick update files from the specified location	Select this option if you want to pick the updates from a local folder or a network folder.
Copy update files to specified location	Select this option if you want to save a copy of the updates downloaded to your local folder or network folder.

Internet Settings

If you are using a proxy server on your network, or using Socks Version 4 & 5 network then you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in Internet settings. Username & Password credentials are mandatory for login. Following Thirtyseven4 modules requires these changes:

- Registration Wizard
- Quick Update
- Messenger

To enable and configure HTTP proxy settings

1. Click **Settings** -> **Internet Settings** on the *Dashboard*.
2. Choose HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings and then perform the following steps:
 - In **Server**, type IP address of the proxy server or domain name (For example: proxy.yourcompany.com).
 - In **Port**, type the port number of the proxy server (For example: 80).
 - In **User Name** and **Password**, type your server login credentials, when required.
3. Click **Save Changes** to save the settings.

Registry Restore

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

Thirtyseven4 Registry Restore feature restores the critical system registry area and other areas from the changes made by malwares. It also repairs the system registry.

Registry Restore settings

Restore critical system registry areas	Selecting this option allows Thirtyseven4 Antivirus to restore the critical system registry during scan. Critical System Registry areas are generally changed by malwares to perform certain task automatically or to avoid detection or modification by system applications. e.g. Disabling Task Manager, Disabling Registry Editor etc.
Repair malicious registry entries	Selecting this option allows Thirtyseven4 Antivirus to scan system registry for malware related entries. Malwares and their remains will be repaired automatically during scan.

Self Protection

Self Protection feature, when enabled, will protect Thirtyseven4 Antivirus, by safeguarding its files, folders, configurations and registry entries against malwares and also against tamper from other applications.

Self Protection feature in Thirtyseven4 Antivirus can be accessed by clicking **Settings** from the *Dashboard*. Click the button to either enable or disable Self Protection feature. By default, Self Protection feature is enabled and set to **ON**.

Password Protection

You can protect the settings configured for Thirtyseven4 Antivirus by enabling Password Protection. Enabling Password Protection ensures that Thirtyseven4 Antivirus configurations and settings are protected from modification by other users. Once Password Protection is enabled, Protection Center features of Thirtyseven4 Antivirus like Files & Folders, Emails, Internet & Network, and External Drives & Devices along with the Settings menu will be accessible to users only on authentication of password.

To enable Password Protection please perform the following steps:

1. Click **Settings** on the Dashboard.
2. By default the Password Protection feature will be set to **OFF**. Click **OFF** to open Password Protection window.
3. If you are setting the password for the first time, then **Enter old password** will be de-activated. Type the desired password in **Enter new password** and re-type the same in **Confirm new password**.
4. Click **Save Changes**.

Report Settings

Report Settings lets you specify the number of days to retain the reports generated by Thirtyseven4 Antivirus. You can also retain all the reports without deleting any of the reports generated. By default, the setting has been configured to retain reports for 30 days.

Configuring Report Settings

To configure report settings, please perform the following steps:

1. Click **Settings** on the *Dashboard*.
2. The Settings screen is displayed. Click **Report Settings**.
3. The **Report Settings** screen is displayed. By default, the **Delete reports after** checkbox is checked and the value is set to **30 days**. If you want to retain all the reports generated then uncheck the **Delete reports after** checkbox. If you want to change the value of number of days for retaining the reports, then click the drop-down menu and select from the choices.
4. Click **Save Changes** to apply the settings.

Report Virus Statistics

Report Virus Statistics feature in Thirtyseven4 Antivirus submits the virus detection statistics report, generated during scans, to Thirtyseven4 Research Center.

Report Virus Statistics feature in Thirtyseven4 Antivirus can be accessed by clicking **Settings** from the *Dashboard*. Click the button to either enable or disable Report Virus Statistics feature. By default, Report Virus Statistics feature is enabled and set to **ON**.

Restore Default Settings

Restore Default Settings changes all the modifications to settings and restores the default settings. If you have customized the settings of Thirtyseven4 Antivirus and feel that the protection of the system may have been compromised, then you can bring back the protection to its default settings with the click of a single button. This single click restores all default settings so that you don't have to remember all the configurations made. To restore default settings, please perform the following steps:

1. Click **Settings** on the Dashboard.
2. In the **Restore Default Settings** row click **Default All**.

Tools

The tools available with Thirtyseven4 Antivirus are as follows:

- [Hijack Restore](#)
- [Track Cleaner](#)
- [Anti-Rootkit](#)
- [Create Emergency Disk](#)
- [Launch AntiMalware](#)
- [View Quarantine Files](#)
- [USB Drive Protection](#)
- [System Explorer](#)
- [Windows Spy](#)
- [Exclude File Extensions](#)

Hijack Restore

The Hijack Restore feature restores the modified settings of Internet Explorer browser to default settings. If you have modified the default settings of Internet Explorer or if the settings have been modified by malwares, spywares, and sometimes genuine applications, then you can restore the default settings of Internet Explorer browser by using the Hijack Restore feature. This feature also helps to restore critical operating system settings like Registry Editor and Task Manager.

Using Hijack Restore

1. Click **Tools** Menu from the *Dashboard*.
2. Click **Hijack Restore** under *Cleaning & Restore Tools*.

The following actions can be performed:

Check All	Checking this option checks all the options displayed in the <i>Internet Explorer Browser Settings</i> frame. This is useful if you want to restore all the browser settings and you can avoid manually checking all options one after the other. If all the options are checked and you want to uncheck all of them then unchecking Check All feature will un-check all the options displayed in the <i>Internet Explorer Browser Settings</i> frame.
------------------	--

Restore default host file

Check this option if you wish to restore the default host file. If you check **Restore default host file** option, it enables **Default Host file** button. Click **Default Host file** button to open the *Host Specification* window.

IP Address	Enter the IP Address of the host.
Host Name	Enter the host name of the host.
Add	Click Add to add the host details in the frame.
Edit	Highlight the added host in the frame and click Edit to make any modifications, if required, to the host details.
Delete	Highlight the added host in the frame and click Delete to remove the added host details.
OK	Click OK to save the added host and exit from the <i>Host Specification</i> window.
Close	Click Close to exit without saving, from the <i>Host Specification</i> window.

Restore important system settings

Check this option if you wish to restore critical system settings. If you check **Restore important system settings** option, it enables **Settings** button. Click **Default Host file** button to open the *Important System Settings* window.

Check All	Checking this option checks all the options displayed in the <i>Settings to restore</i> frame. This is useful if you want to restore all the system settings and you can avoid manually checking all options one after the other. If all the options are checked and you want to uncheck all of them then un-checking Check All feature will un-check all the options displayed in the <i>Settings to restore</i> frame.
OK	Click OK to save all modified settings and exit from the <i>Important System Settings</i> window.
Close	Click Close to exit without saving, from the <i>Important System Settings</i> window.

The buttons on the Hijack Restore function and their feature are as follows:

Restore Now	Once the required settings are checked, click Restore Now button to restore default settings.
Undo	If you wish to revert to the existing settings rather than the restored default settings, click Undo button. It opens a window called <i>Undo Operations</i> . The settings which have been restored to default settings will be listed. Check the required settings or check the option Check All to check all the settings displayed. Click OK to revert to the existing settings or click Close to exit without reverting.
Close	Click Close to exit from the <i>Hijack Restore</i> window.

Track Cleaner

Track Cleaner removes the **Most Recently Used** (MRU) from popular and daily-used applications to ensure that your privacy is not breached. Many applications store the list of recently opened files in their internal format to help you open them again for quick access. This feature of Windows is good but at the same time, on the systems which is used by more than one user it may happen that the user's privacy is compromised. Track Cleaner helps delete all the tracks of such applications and prevent privacy breach.

Using Track Cleaner

1. Click **Tools** -> **Track Cleaner** from Thirtyseven4 dashboard.
2. Select applications whose traces need to be removed by checking them. In case you want to remove traces of all the applications, check the **Check All** feature.
3. Click **Start Cleaning** to remove traces from the applications selected. Upon completion click **Close** to exit.

Anti-Rootkit

Thirtyseven4 Anti-Rootkit is a program that proactively detects and cleans rootkits that are active in the system. This program scans objects like running Processes, Windows Registry and Files and Folders for any suspicious activity and detects the rootkits without any signatures. It detects most of the existing rootkits and is designed to detect the upcoming rootkits and also provides the option to clean them.

It is recommended that Thirtyseven4 Anti-Rootkit should be used by person having certain knowledge of the operating system or with the help of Thirtyseven4 Technical Support engineer. Improper usage of this program could result in unstable system.

To Start Thirtyseven4 Anti-Rootkit from Thirtyseven4 Antivirus

1. Click **Tools** -> **Anti-Rootkit** from the Dashboard.
2. A pop-up appears that recommends closing all other applications before launching Anti-Rootkit.

Using Thirtyseven4 Anti-Rootkit

1. Start **Thirtyseven4 Anti-Rootkit**.
2. In the left side of the main window click **Start Scan**.
3. Thirtyseven4 Anti-Rootkit will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry, Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

Stop Scanning	During scan you can select Stop Scan to stop the scan; Thirtyseven4 Anti-Rootkit will prompt before stopping the scan.
Close	Click Close to quit Thirtyseven4 Anti-Rootkit. If you choose to close the application while scanning is in progress, it will prompt to stop the scan.

Error Report Submission	Due to infection or some unexpected conditions in system, scanning of Thirtyseven4 Anti-Rootkit may fail. On failure you will be asked to re-scan your system and submit error report to Thirtyseven4 Team for further analysis.
--------------------------------	--

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

Configuring Thirtyseven4 Anti-Rootkit for Scan

1. Start **Thirtyseven4 Anti-Rootkit**.
2. Click on the **Settings** button on top bar of Thirtyseven4 Anti-Rootkit.
3. Settings dialog box will appear.
4. By default Thirtyseven4 Anti-Rootkit is configured for Auto Scan where it scans appropriate predefined system areas.

Auto Scan	<p>Auto Scan is default scan option provided by Thirtyseven4 Anti-Rootkit. Under Auto Scan Thirtyseven4 Anti-Rootkit scans appropriate predefined system areas. During Auto Scan, scanning is performed for:</p> <ul style="list-style-type: none"> • Hidden Processes. • Hidden Registry entries. • Hidden Files and Folders. • Executable ADS.
------------------	--

Custom Scan	By selecting Custom Scan radio button, you can configure following options:
Detect Hidden Process	To scan for running hidden processes in the system.
Detect Hidden Registry Items	To scan for hidden items in Windows Registry.
Detect Hidden files and folders	To scan for hidden files and folders in the system and executable ADS (Alternate Data Streams). You can choose option: <ol style="list-style-type: none"> 1. Scan drive on which Operating System is installed. 2. Scan All Drives to perform scanning in all fixed drives. 3. Alternate Data Streams (ADS) to scan for executable ADS.
Scan drive on which operating system is installed	Will scan for hidden files and folders on the drive on which operating system is installed.
Scan all fixed drives	Will scan for hidden files and folders on all the fixed drives of the system.
Alternate Data Streams (ADS)	To scan for suspicious items in Alternate Data Streams of NTFS File system.

Report File Path	Thirtyseven4 Anti-Rootkit creates a scan report file at the location from which it is executed. You can specify different location by specifying report file path.
-------------------------	--

Overview of Alternate Data Streams - ADS

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

Scanning Results and Cleaning Rootkits

Thirtyseven4 Anti-Rootkit Scanning

1. Start **Thirtyseven4 Anti-Rootkit**.
2. In the left side of the main window click on **Start Scan**.
3. **Thirtyseven4 Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit Process or rename the rootkit Registry entry or Files.
6. After taking the appropriate action you need to restart your system so that rootkit cleaning take place.

Action to be taken on Scan Results

Process	<p>After scanning Thirtyseven4 Anti-Rootkit will detect and display a list of hidden Processes. You can select process or process for termination, but make sure that list of Processes for termination doesn't include any know trusted process.</p> <p>Thirtyseven4 Anti-Rootkit also displays summary of process scanning as total number of Processes scanned and number of hidden Processes detected.</p>
Terminating Hidden Process	<p>After selecting list of Processes for termination click on Terminate button. If a process is successfully terminated then its PID (Process Identifier) field will show n/a and process name will be appended by Terminated. All terminated Processes will be renamed after a restart.</p>
Registry	<p>Similar to process scan Thirtyseven4 Anti-Rootkit will display a list of hidden Registry keys. You can select keys for renaming, but make sure that list of keys for renaming doesn't include any known trusted registry key.</p> <p>Thirtyseven4 Anti-Rootkit also displays summary of Registry scanning as total number of items scanned and number of hidden items detected.</p>
Renaming Hidden Registry Key	<p>After selecting list of keys for renaming click on Rename button. Renaming operation requires reboot hence Key name will be prefixed by Rename Queued.</p>

Files and Folders	<p>Similar to process and Registry Thirtyseven4 Anti-Rootkit will display a list of hidden Files and Folders. You can select Files and Folders for renaming, but make sure that list of Files and Folders for renaming doesn't include any know trusted file.</p> <p>Thirtyseven4 Anti-Rootkit also displays list of executable Alternate Data Streams.</p> <p>Thirtyseven4 Anti-Rootkit also displays summary of File scanning as total number of files scanned and number of hidden files detected.</p>
Renaming Hidden Files and Folders	<p>After selecting list of Files and Folders for renaming click on Rename button. Renaming operation requires reboot hence Files and Folders name will be prefixed by Rename Queued.</p>

Cleaning Rootkits through Thirtyseven4 Emergency Disk

In some cases it may happen that rootkits are not being cleaned. They are reappearing during Thirtyseven4 Anti-Rootkit scan. In such case you can also use Thirtyseven4 Emergency Disk for proper cleaning. All you have to do is create a Thirtyseven4 Emergency Disk and boot your system through it. To create a Thirtyseven4 Emergency Disk and clean your system through it, please follow the below given steps:

Step 1

Step 1 consists of creating a Thirtyseven4 Emergency Disk. To create a Thirtyseven4 Emergency Disk, please use the following link. [Create Emergency Disk](#)

Step 2

1. Start **Thirtyseven4 Anti-Rootkit**.
2. In the left side of the main window click on **Start Scan**.
3. **Thirtyseven4 Anti-Rootkit** will start scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.
4. After completing the scan result is displayed in three different tabs that will display hidden items in running Processes, Windows Registry and Files and Folders.
5. You can now select and take appropriate action against each displayed threat. Like you can terminate the rootkit process or rename the rootkit registry entry or files.

Step 3

1. Boot your system using **Thirtyseven4 Emergency Disk**.
2. Thirtyseven4 Emergency Disk will automatically scan and clean the rootkits from your system.

Create Emergency Disk

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

The Emergency Disk will be created with the latest virus signature pattern file used by Thirtyseven4 Antivirus on your system.

To create an Emergency Disk please perform following steps:

1. Click **Tools** -> **Create Emergency Disk** from the *Dashboard*.
2. Click the link displayed on the screen and download the required package.
3. Extract the downloaded package on your system. e.g. c:\my documents\qhemgpkg.
4. Provide the extracted package path, and click **Next**.
5. To create Emergency Disk, select any one of the options that are displayed on screen i.e. either select **Create Emergency USB disk** or **Create Emergency CD/DVD**.
6. Select the disk drive to be converted to an Emergency Disk and, click **Next**.
7. On successful creation of an Emergency Disk a message confirming the same will be displayed.

Things to remember while creating an Emergency Disk:

- It is always advisable to retain a copy of the extracted package on your system.
- On Windows XP and Windows 2003 Operating Systems you need to install **Imaging API version 2.0 patch**.
- While using an USB device, rewritable CD/DVD, please 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 scanning 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 the **Emergency Disk** into your CD/DVD/USB drive.
2. Restart your system.
3. Emergency Disk will automatically start scanning all the drives. It will automatically disinfect the infection, if found.
4. Restart your system.

Launch AntiMalware

Thirtyseven4 AntiMalware, with its improved malware scanning engine, scans registry, files and folders at lightning speed to thoroughly detect and clean Spywares, Adwares, Roguewares, Dialers, Riskwares and lots of other potential threats in your system.

Launching Thirtyseven4 AntiMalware


Thirtyseven4 AntiMalware can be launched from any of the following ways:

- Click **Start** -> **Programs** -> **Thirtyseven4 Antivirus** -> **Thirtyseven4 AntiMalware**.
- Right-clicking the Virus Protection icon on the Windows system tray and selecting **Launch AntiMalware**.
- Clicking **Tools** -> **Launch AntiMalware** from the Thirtyseven4 dashboard.

Using Thirtyseven4 AntiMalware

Click Scan Now on the Thirtyseven4 AntiMalware screen to initiate the malware scan process. While scanning for malwares Thirtyseven4 AntiMalware displays malicious files, folders and registry entries related to various malwares. Once the scanning is complete and in case a malware is found, a list will be displayed for detected malwares contained in malicious files, folders and registry. You can un-check specific file, folder or registry entries within the displayed list, but ensure that all un-checked items are genuine applications and not malicious ones.

In a case a malware is detected, the following actions can be taken:

Clean	Clicking this button will clean the malwares and its remains from the system. If you have un-checked specific file, folder or registry entry then you will be prompted whether you wish to exclude those items in future scan. If you wish to permanently exclude those items then click Yes , otherwise click No for temporary exclusion.
Skip	Clicking this button will not take any action against malwares in your system.
Stop Scan	Selecting
Set System Restore point before cleaning	Selecting this option will create System Restore point before the cleaning process starts in your system. This enables you to revert to the cleaning done by Thirtyseven4 AntiMalware by using Windows System Restore facility.  Set System Restore point before cleaning feature is not available on Windows 2000 operating system.
Details	Clicking this button redirects you to http://www.thirtyseven4.com

View Quarantine Files

Quarantine helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Thirtyseven4 Antivirus encrypts the file and keeps it inside the Quarantine directory. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of infected file before repairing. Backup functionality is available by selecting Backup before repairing option under Scanner's settings.

How to launch Quarantine Files

1. Click **Tools** -> **View Quarantine Files** from the *Dashboard*.

You can perform the following tasks with the Quarantine feature:

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

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

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 Thirtyseven4 has been able to detect the malicious file on your system during its scans, but has not been able to repair the infection of the file.
False positive	Select this reason if a non-malicious data file that you have been using and are aware of its function, has been detected by Thirtyseven4 as a malicious file.

USB Drive Protection

Thirtyseven4 Antivirus safeguards your USB devices from autorun malwares. Autorun feature of the removable drive is one of the mediums for malwares to gain access into the system. The USB Drive Protection feature prevents autorun malwares from using your removable device as an infection spreading medium. Securing the removable drive also ensures that the drive, if connected to an infected system, cannot be used for spreading autorun malwares on other system.

To safeguard removable drives please perform the following steps:

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



Although Thirtyseven4 recommends that you keep the autorun feature of your USB drive disabled but if you wish to enable the Autorun feature of the USB drive, just follow the steps mentioned earlier and in Step 2 click the **Un-secure Removable Drive** button to enable autorun on your USB drive. Insert the same removable drive for un-secure that has been secured using Thirtyseven4 Antivirus.

System Explorer

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

Windows Spy

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

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

Using Windows Spy

1. Click **Tools** -> **Windows Spy** from the *Dashboard*.
2. Click **Drag** and move the mouse pointer on the application.
3. A window will be opened displaying above mentioned information.
4. If you wish to terminate that application or window then click **Kill Process**.

Exclude File Extensions

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

Creating exclusion list for virus protection

1. Click **Tools** -> **Exclude File Extensions** from the *Dashboard*.
2. Enter the file extension that needs to be excluded from the Virus Protection scan and click **Add**.
3. If the added extension is incorrect, then highlight the extension added in the list and click **Remove** to delete it from the list.
4. Click **OK** to save the list or click **Cancel** to exit without saving.

Reports

Thirtyseven4 Antivirus creates and maintains a detailed report of some important and frequently used features of Thirtyseven4. Reports such as virus scan details, update details, changes in settings of the features, etc, are maintained. The features of Thirtyseven4 Antivirus for which the reports can be viewed are as follows:

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

The Reports window consists of **Reports for** frame on the left side that contains the list of features for which reports can be viewed. To the right of the **Reports for** frame contains the list of records for a particular feature, where each record contains a detailed report for the respective feature of Thirtyseven4 Antivirus. There are three buttons present in the Reports window. The buttons and their functions are as follows:

Button	Action
Details	Click Details to display a detailed report of the highlighted record in the list.
Delete All	Click Delete All to delete all the records in the list.
Delete	Click Delete to delete the highlighted record in the list.

To view a detailed for a particular feature, please perform the following steps:

1. Click **Reports** on the Dashboard.
2. Click the desired feature, listed under the **Reports for** frame, for which the report is to be viewed.
3. Highlight the desired record on the right side of the **Reports for** frame and click **Details** button to view the Report.

Once the report window is opened, you can view the report. This window has five buttons in it. The buttons and their function are as follows:

Button	Action
Prev	Click Prev to display the detailed report of the previous record in the list. This button will be disabled if the record being accessed is the first record in the list.
Next	Click Next to display the detailed report of the next record in the list. This button will be disabled if the record being accessed is the last record in the list.
Print	Click Print to take a print-out of the detailed report.
Save As	Click Save As to save the detailed report in .txt format in the desired location of your system.
Close	Click Close to exit from the window.

Help

The Help menu provides you the required assistance to understand Thirtyseven4 Antivirus better. Assistance such as online documentation and license information can all be accessed from the Help menu. The following menu items are available under the Help menu:

- [Help](#)
- [Support](#)
- [About](#)

Help

Help system consists of extensive topics, index, commands and procedures with general FAQs. Thirtyseven4 provides online help for most of the message windows. You can get help on all the topics by any of the following ways:

- Launching Help by clicking **Help** -> **Help** from the Dashboard.
- Pressing **F1** key when help is needed.
- Clicking the **Help** button in a dialog box.

Support

Support menu item provides you with technical support details. The following features are available under Support menu item:

Thirtyseven4 Technical Support Details

The entire list of Thirtyseven4 branches and their contact information is available in this section.

System Information

Thirtyseven4 Antivirus System Information is an essential tool to gather critical information of a Windows based system for following cases:

To detect new Malwares	This tool gathers information to detect new Malwares from Running processes, Registry, System files like Config.Sys, Autoexec.bat etc.
To get Thirtyseven4 Antivirus information	It gathers information of the installed version of Thirtyseven4 Antivirus, its configuration settings and Quarantined file(s), if any.

Submitting System Information file

This tool generates an INFO.QHC file at C:\ and submits the same automatically to support@thirtyseven4.com



INFO.QHC file contains information in text and binary format. It contains critical system details and installed Thirtyseven4 Antivirus version details. Information contains automatic execution of files (through Registry, Autoexec.bat, System.ini and Win.ini) and Running processes along with their supported library details. These details are used to analyze the system for new Malwares and proper functioning of Thirtyseven4 Antivirus. The above information is used to provide better and adequate services to customers. This tool doesn't collect any other personally identifiable information, passwords etc. We respect your privacy; rest assured this information will not be shared or disclosed.

Generating System Information

To generate system information you need to perform the following steps:

1. Click **Help** -> **Support** from the *Dashboard*.
2. Click **Submit System Information**.
3. The System Information wizard opens. Click **Next** to continue.
4. Select the system information generating reason. If you are suspecting new Malwares in your system then select **I suspect my system is infected by new Malwares** or if you are facing problem while using Thirtyseven4 Antivirus then select **I am having problem while using Thirtyseven4**. Provide comments in the **Comments** text area and also enter your email address. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Thirtyseven4 Technical Support.

About

Thirtyseven4 Antivirus About section provides following information:

- Thirtyseven4 Antivirus Version
- License details
- License validity

Following buttons are also available in About Section:

Renew Now	Renew Now allows you to 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 pretty useful to synchronize your existing License information with Thirtyseven4 Activation Server. e.g. Suppose you wish to renew your existing subscription and you do not know how to renew it or facing problem during renewal. You can call Thirtyseven4 Support team; provide your Product key and Renewal Code. Thirtyseven4 Support team will renew your copy. You just need to follow the below given steps: <ol style="list-style-type: none">1. Be connected to Internet.2. Click Update License Details.3. Click Continue to update your existing subscription. Print License Details: Click Print License Details to print the existing subscription information.
Update Now	Update Now allows you to update virus database of Thirtyseven4 Antivirus.

Chapter 7

Updating Thirtyseven4 Antivirus

Updates for Thirtyseven4 Antivirus are posted regularly on its website containing detection and removal of newly discovered viruses. To prevent newly discovered viruses from infecting your computer, your system should have latest updated copy of Thirtyseven4 Antivirus. By default Thirtyseven4 Antivirus is set to update automatically from the Internet. This is done without user's intervention. Only basic requirement in this case, is the availability of a valid Internet connection for availing automatic updates. Automatic updates can also be applied from local or network path, but that path should have the latest set of definitions.

Some important facts about Thirtyseven4 Antivirus Updates

- All Thirtyseven4 Antivirus Updates are complete updates including Definition File Update and Engine Updates.
- All Thirtyseven4 Antivirus updates also provide you version up gradation, thus making available the new features and technology for your protection.
- Thirtyseven4 Quick Update is a single step upgrade.

Updating Thirtyseven4 Antivirus from Internet

Quick Update by default automatically updates your copy of Thirtyseven4 Antivirus through the Internet. For this, you only need to have a valid Internet Connection. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.)

To update Thirtyseven4 Antivirus manually through Internet

1. Click **Start -> Programs -> Thirtyseven4 Antivirus -> Quick Update.**
2. Follow the instructions and click **Next** button.
3. Check **Download from AntiVirus 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 Thirtyseven4 AntiVirus site, downloads the appropriate upgrade files for your copy of Thirtyseven4, and applies it thereafter to your copy, thus updating it to the latest available update file.

Updating Thirtyseven4 Antivirus with definition files

If you already have the upgraded definition file with you, you can upgrade Thirtyseven4 Antivirus without connecting to the Internet. It is specifically useful for Network environments with more than one PC. You are not required to download the upgrade file from the internet on all the PCs within the network using Thirtyseven4.

To update Thirtyseven4 Antivirus through definition file:

1. Click **Start -> Programs -> Thirtyseven4 Antivirus -> Quick Update.**
2. Follow the instructions and click Next button.
3. Click **Pick from specified path.**
4. Click **File** to locate the definition file. Select any .bin 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 Thirtyseven4 Antivirus accordingly.

Update Guidelines for Network Environment

Thirtyseven4 Antivirus can be configured to provide hassle free updates across the network. You are suggested to follow these guidelines for best results:

1. Setup one computer (may be the server) as the master update machine. Suppose server name is SERVER.
2. Make **QHUPD** folder in any location. For example: **C:\QHUPD.**
3. Assign Read-Only sharing rights to this folder.
4. Click **Start -> Programs -> Thirtyseven4 Antivirus -> Thirtyseven4 AntiVirus** to open **Thirtyseven4 Antivirus.**
5. Click **Settings -> Automatic Update** from the *Dashboard.*
6. Select **Copy update files to specified location.**
7. Click **Browse** and locate the **QHUPD** folder. Click **OK.**
8. Click **Save Changes** to save this setting.
9. On all user computers within the network launch **Thirtyseven4 Antivirus.**
10. Go to **Automatic Update** page under **Settings.**
11. Select **Pick update files from specified path.**
12. Click **Browse.**
13. Locate the **SERVER\QHUPD** folder from Network Neighborhood. Alternatively you can type the path as **\\SERVER\QHUPD.**
14. Click **Save Changes** to save the settings.

Chapter 8

Cleaning Viruses

Thirtyseven4 warns you for a virus infection when:

- A virus is encountered during a manual scan.
- A virus is encountered in the memory.
- A virus is encountered by Thirtyseven4 Antivirus Virus Protection/Email Protection.

Cleaning viruses encountered during scans

Thirtyseven4 Antivirus is adequately configured with the default installation to protect your system. If a virus is detected during scanning with default settings, Thirtyseven4 Antivirus tries to repair the virus and if it fails in doing so, it will quarantine the file. If you have changed the default scanner settings, then action will be taken accordingly when a virus is found.

Scanning Options

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

Action	Click this tab to view the action taken, if any, during the scan.
Skip Folder	During the scan if you want to avoid scanning the current folder, just press on Skip folder. Scanning will be moved to other location. This option can be used while scanning a folder which contains non-suspicious items.
Skip File	During the scan if you want to avoid scanning the current file, just press on Skip file. Scanning of the current file will be skipped. This option can be used while scanning a big archive of files.
Stop	To stop the scanning process.
Close	To exit from the scanning process.
Shut down PC when finished	Check this option when you to shut down your system after finishing the scan. This feature will work only if the scanning is completed.

Cleaning virus encountered in memory

"Virus Active in memory" means that virus is active, spreading to other files, computer (if connected to network) and doing malicious activity as per its payload.

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 at boot time before the desktop is completely loaded. It will detect and clean even the most cunning Rootkits, spywares, special purpose Trojans and loggers.

Restart required during cleaning for some malwares

Some malwares drop and inject their dynamic link libraries into system's running processes such as explorer.exe, Iexplore.exe, svchost.exe, etc. which cannot be disabled or cleaned. During memory scan when they will be detected, they will be set for deletion in the next boot automatically. Thirtyseven4 Antivirus memory scan will provide complete detail or action recommendation for you in such cases.

Cleaning of Boot/Partition viruses

In case if Thirtyseven4 Antivirus memory scanner detects a boot or partition virus in your system then it will recommend you to boot your system using a clean bootable disk and scan it using Thirtyseven4 Emergency disk to clean the virus.

Responding to virus found alerts from Virus Protection

Thirtyseven4 Antivirus Virus Protection 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 Thirtyseven4 Antivirus Virus Protection.

Technical Support

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

What should I be ready with, before calling?

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



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

Contact Us

SUPPORT CENTER

Thirtyseven4, L.L.C.

P.O. Box 1642,

Medina, Ohio 44258

United States

Phone number: 1-877-374-7581

Fax number: 1-866-561-4983

Email: support@thirtyseven4.com

Thirtyseven4 Support: <http://support.thirtyseven4.com>

Web: <http://www.thirtyseven4.com>

Sales: sales@thirtyseven4.com
