User Guide

Thirtyseven4™ AntiVirus

Thirtyseven4, LLC
http://www.thirtyseven4.com

Copyright Information

All Rights Reserved.

Trademarks

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. 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-sublicensable, 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 A 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 arties, 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.

About the Document

This User Guide covers all the information about how to install and use Thirtyseven4 products on Windows operating systems in the easiest possible ways. We have ensured that the details provided in this guide are up-to-date with the latest developments in the software.

The following list describes the conventions that we have followed to prepare this document.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it may be a menu title, window title, check box, drop-down box, dialog, button names, and so on.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The numbered list and the instruction mentioned in each numbered list indicate actions that you need to perform.

Contents

Chapter 1 Getting Started

Thirtyseven4 AntiVirus is simple to install and easy to use. During installation, read each installation screen carefully and follow the instructions.

Prerequisites

Remember the following guidelines before installing Thirtyseven4 AntiVirus on your system.

- Multiple anti-virus software products installed on a single system may result in system malfunction. If any other anti-virus software program is installed on your system, you must remove it before proceeding with the Thirtyseven4 AntiVirus installation.
- Close all open programs before proceeding with the 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, your system should meet the following minimum requirements.

- Internet connection to receive updates
- CD/DVD Drive
- Free disk space required for is 1.30 GB.
- 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.
- Thirtyseven4 AntiVirus is not supported on Microsoft Windows Server operating systems.

Operating System Compatibility

Operating Systems	Minimum Requirements
Windows 2000	· 300 MHz Pentium (or compatible) processor · 256 MB of RAM · DVD or CD-ROM drive · Service Pack 4 · Internet Explorer 6
Windows 2000 Server*	· 300 MHz Pentium (or compatible) processor · 256 MB of RAM · DVD or CD-ROM drive · Service Pack 4 · Internet Explorer 6
Windows XP	· 300 MHz Pentium (or compatible) processor · 256 MB of RAM · DVD or CD-ROM drive · Service Pack 2 and later
Windows Server 2003*	· 300 MHz Pentium (or compatible) processor · 256 MB of RAM · DVD or CD-ROM drive
Windows Vista	· 1 GHz Pentium (or compatible) processor · 512 MB of RAM · DVD or CD-ROM drive
Windows Server 2008*	· 1 GHz Pentium (or compatible) processor · 512 MB of RAM · DVD or CD-ROM drive
Windows Server 2008 R2*	· 1 GHz Pentium (or compatible) processor · 512 MB of RAM · DVD or CD-ROM drive
Windows 7	· 1 GHz Pentium (or compatible) processor · For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM · DVD or CD-ROM drive
Windows 8	· 1 GHz Pentium (or compatible) processor · For 32-bit: 512 MB of RAM; For 64-bit: 1 GB of RAM · DVD or CD-ROM drive
Windows Server 2012*	· 1 GHz Pentium (or compatible) processor · 512 MB of RAM · DVD or CD-ROM drive

- The requirements provided are minimum system requirements. Thirtyseven4 recommends that your system maintains a higher configuration than the minimum requirements to obtain best results.

To check for the latest system requirements, visit at 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 later
- Microsoft Outlook 2000 and later
- Netscape Messenger 4 and later
- Eudora, Mozilla Thunderbird
- 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).

Thirtyseven4 Anti-Rootkit Requirements

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

Thirtyseven4 Self-Protection

- This feature is not supported on Microsoft Windows 2000 operating system.
- For Microsoft Windows XP operating system this feature is supported if Service Pack 2 or later is installed.
- For Microsoft Windows Server 2003 operating system this feature is supported if Service Pack 1 or later is installed.

Thirtyseven4 Browser Sandbox

- This feature is not supported on Microsoft Windows 2000, Microsoft Windows XP 64-bit, and Microsoft Windows 8 operating systems.

Installing Thirtyseven4 AntiVirus

To install Thirtyseven4 AntiVirus, follow these steps:

1. 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 with a list of options.

   In case the CD or DVD drive does not start the CD automatically, follow these steps:

   i. Double-click **My Computer** or the **Computer** icon on the Desktop.

   ii. Right-click the CD-ROM drive and select **Explore**.

   iii. Double-click **Autorun.exe**.

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

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

   - The installer automatically sets the boot time scanner to scan and disinfect the system on the next boot.
   - After disinfection of the system, the system starts and you need to re-initiate the installation. For more details, refer to *Performing Boot Time Scan*, in “Chapter 3: Thirtyseven4 AntiVirus Dashboard”, p-39.

   During the pre-install virus scan if no virus is found in the system memory, the installation proceeds further.

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

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

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

   The Install Location screen appears. The default location where Thirtyseven4 is to be installed is displayed. The disk space required during installation is also mentioned on the screen.

5. If the default location has insufficient space, or you want to install Thirtyseven4 on another location, click **Browse** to change the location or click **Next** to continue.

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

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

Uninstalling Thirtyseven4 AntiVirus

Removing Thirtyseven4 may expose your system to virus threats. However, you can uninstall Thirtyseven4 in the following ways:

1. To uninstall, select **Start > Programs > Thirtyseven4 AntiVirus > Uninstall Thirtyseven4 AntiVirus**.

   A prompt with the message **Do you want to Remove Thirtyseven4 AntiVirus completely from your computer?** *is displayed.*

2. Click **Yes** to continue with the uninstallation.

   If you have password-protected Thirtyseven4, an authentication screen appears.

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

   Thirtyseven4 maintains a repository of Report Files, Quarantine Files, and Backup Files.. You may retain or delete this repository during uninstallation. However, the ***Remove Report Files*** *and* ***Remove Quarantine/Backup Files*** *options are selected by default.*

4. Click **Next** to continue with the uninstallation without saving the repository. If you want to retain the repository, clear the required options and click **Next**.

   The uninstallation process is initiated.

   When uninstallation is complete, a message appears. You may provide feedback and reasons for uninstalling Thirtyseven4 by clicking ***Write to us the reason of un-installing Thirtyseven4 AntiVirus****. Your feedback is valuable to us and helps us to improve the product quality.*

   Please note the product key for future reference. You can save your product key information by clicking **Save to file**. Restart is recommended after Thirtyseven4 uninstallation. 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

Thirtyseven4 AntiVirus must be immediately registered upon installation to activate the copy. Only the activated copy will receive the database updates regularly and you can get technical support whenever required. If your product is not regularly updated, it cannot protect your system against the latest threats.

Registration

You can register Thirtyseven4 AntiVirus in any of the following ways.

Registering online

If you are connected to the Internet you can register your product online. To register Thirtyseven4 AntiVirus online, follow these steps:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Activate Thirtyseven4 AntiVirus**.

   The Registration Wizard opens.

2. Enter the 20-digit Product Key and click **Next** to continue.

   The Registration Information appears.

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

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

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

5. Click **Next** to continue.

   A confirmation screen appears with the details you entered.

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

6. Click **Next** to continue.

   Your product is activated successfully. The date when your license expires is displayed.

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

Registering offline

Thirtyseven4 AntiVirus can be registered offline if your system is not connected to the Internet.

You need to visit the offline activation page on the website of Thirtyseven4 at http://173.192.146.76/useract/act2011 and complete the registration form. Upon completion, a new key will be generated which you have to use to activate your product on your system that is not connected to the Internet.

You can register Thirtyseven4 AntiVirus offline in the following ways.

Obtaining product key and installation number

Before visiting the offline activation page, ensure that you have the product key and the installation number with you. You can obtain the key and installation number in the following ways.

- **Product Key**: Is printed on the User Guide and/or can be found inside the box. If the product is purchased online, then the product key can be obtained from the email confirming the order.
- **Installation Number**: Can be obtained from the Activation Wizard in the following ways:

  i. Select **Start > Programs > Thirtyseven4 AntiVirus > Activate Thirtyseven4 AntiVirus**.

  The Registration Wizard opens.

  ii. Click **Register Offline**.

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

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

- **A valid email address** – A <license>.key file is generated after successful completion of offline activation. This file is sent to the email address that you provided. You should ensure that you enter the correct email address.

Generating activation key for offline activation

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

1. Visit the offline activation page at http://173.192.146.76/useract/act2011.

   An Off-Line Registration page appears.

2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.

   Ensure that you have the product key and installation number with you.

3. Provide the Product Key and Installation Number in the relevant fields and click **Submit**.

   A registration form appears.

4. Enter the relevant information in the registration form. Click **Submit**.

   All asterisk fields are mandatory to fill.

5. A new key is generated. Save this personally.

   Moreover, this key is also sent to your email address provided by you in the registration form.

Activating Thirtyseven4 AntiVirus with offline activation key

Once the offline activation key is generated, you can proceed with activating Thirtyseven4 AntiVirus on your system that is not connected to the Internet in the following ways:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Activate Thirtyseven4 AntiVirus**.

   The Registration Wizard opens.

2. Click **Register Offline**.

   The offline activation screen appears.

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

   Your license is activated successfully and the date when your license expires is displayed.

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

Re-activation

Re-activation is a facility that ensures that you use the product for the full period until your license expires. Re-activation is very helpful in case you format your system when all software products are removed, or you want to install Thirtyseven4 AntiVirus on another computer. In such cases, you need to re-install and re-activate Thirtyseven4 AntiVirus on your system.

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

Renewal

You can renew your product license as soon as it expires by purchasing a renewal code. However, you are recommended to renew your product before your license expires so that your computer is protected without any interruption. You can get a renewal code from the website of Thirtyseven4, or from the nearest distributor or reseller.

You can renew Thirtyseven4 AntiVirus in any of the following ways.

Renewing online

If your computer is connected to the Internet, you can renew Thirtyseven4 AntiVirus online in the following ways:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Activate Thirtyseven4 AntiVirus**.
2. If your copy of Thirtyseven4 has expired then click **Renew Now** on the Thirtyseven4 Dashboard. If your copy of Thirtyseven4 has not expired, then click **About** in the Help menu and click **Renew Now**.

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

   The Registration Information appears.
4. Enter relevant information in the **Purchased From**, **Email Address** and **Contact Number** text boxes, and then click **Next**.

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

5. Click **Next**.

   The license of Thirtyseven4 AntiVirus is renewed successfully.

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

- In case you do not have the renewal code, select the **I do not have renewal code with me. I want to purchase renewal code online** option and click Buy Now.
- In case you renewed your license but its expiration date has not extended, select the **I have already renewed my license. Please update my license from server** option 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

Thirtyseven4 AntiVirus can be renewed offline if your system is not connected to the Internet.

Visit the offline renewal page on the website of Thirtyseven4 at http://173.192.146.76/useract/renew and complete the registration form. Upon completion of the offline renewal process, a new key will be generated which you have to use to renew your product on the computer that is not connected to the Internet.

You can renew Thirtyseven4 AntiVirus offline in the following ways:

Getting the details of Thirtyseven4 AntiVirus

Before visiting the offline renewal page, you should have the following details ready with you:

- **Product Key and Installation Number** – You can get the product key and installation number by filling in the Renewal form in the following steps:
  i. Select **Start > Programs > Thirtyseven4 AntiVirus > Thirtyseven4 AntiVirus**.
  ii. If your copy of Thirtyseven4 has expired, then click **Renew Now** on the Thirtyseven4 Dashboard. If your copy of Thirtyseven4 has not expired, then click **Help > About** and click **Renew Now**.
  iii. Click **Renew Offline**.

  The offline renewal details screen appears.

  iv. You can either note down the offline renewal URL, Product Key and 12-digit Installation Number or click Save to file to save these details.
- **A valid email address** – A <license>.key file is generated upon successful completion of offline renewal. This file is sent to the email address that you provided. You should ensure that your email address is correct.

Generating activation key for offline activation

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

1. Visit the offline activation page at http://173.192.146.76/useract/renew.

   An Off-Line Renewal page appears.

2. Under your product type, click the hyperlink **Click here to proceed to Step 1**.

   Ensure that you have the product key and installation number with you.

3. Enter the Product Key, Installation Number, Purchased Renewal Code and Purchased From details and click **Submit**.

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

Receiving <license> .key file

You can download the <license>.key from the Acknowledgement screen after successful completion of the offline renewal. The <license>.key file is also sent as an attachment to the email address. You can download the file and transfer it to the system on which Thirtyseven4 is installed.

Renewing Thirtyseven4 AntiVirus with <license>.key file

Once the <license>.key file is transferred to the system on which Thirtyseven4 AntiVirus is installed, perform the following steps:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Thirtyseven4 AntiVirus**.

2. If your copy of Thirtyseven4 has expired then click **Renew Now** on the Thirtyseven4 Dashboard. If your copy of Thirtyseven4 has not expired, then click **About** in the Help menu and click **Renew Now**.

3. Click **Renew Offline**.

   The offline renewal details screen appears.

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

   The copy of Thirtyseven4 is renewed and the renewed validity is displayed.

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

Can Thirtyseven4 be installed on another PC?

Once a product key of Thirtyseven4 is activated on a PC it cannot be re-used. If you try to re-use the Product Key to activate another copy of Thirtyseven4, it is considered as a pirated copy and will be blocked.

One product key can be used only for one computer.

Things to Do if the Product Key is Lost

Product Key serves as your identity to Thirtyseven4. If you lose the Product Key, please contact Thirtyseven4 Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

Chapter 3 Thirtyseven4 AntiVirus Dashboard

The Thirtyseven4 Main Dashboard serves as the key interface to all the features of Thirtyseven4 AntiVirus. You can also access the Dashboard and certain features of Thirtyseven4 AntiVirus from the taskbar of your system. Thirtyseven4 protects the entire system even with the default settings. You can start Thirtyseven4 to check the status of Thirtyseven4 protection, to manually scan, view reports and update the product.

You can manually start Thirtyseven4 in any one of the following ways:

- Select **Start > Programs > Thirtyseven4 AntiVirus > Thirtyseven4 AntiVirus**.
- On the taskbar, double-click the **Thirtyseven4 AntiVirus** icon or right-click the **Thirtyseven4 AntiVirus** icon and select **Open Thirtyseven4 AntiVirus**.
- Select **Start** > **Run**, type **Scanner** and press the **Enter** key.

Thirtyseven4 AntiVirus Dashboard

The Thirtyseven4 AntiVirus Dashboard is the main area where you can access all the features. Dashboard is divided into various sections. The top section has the product menus, the middle section has the protection options and the bottom section has the most frequently accessed features of Thirtyseven4 AntiVirus.

The protection options include Files & Folders, Emails, Internet & Network, and External Drives & Devices. With these options, you can secure your system to avoid malware and viruses from infiltrating your system.

Files & Folders	Helps you protect files and folders against malicious threats. With Files & Folders, you can configure Scan Settings, Virus Protection, DNAScan, Block Packed Files, Automatic Rogueware Scan, Scan Schedule, Exclude Files & Folders, and Quarantine & Backup.
Emails	Helps you configure Email Protection and Trusted Email Clients Protection.

Internet & Network	Helps you configure the settings for Internet & Network protection. With this option, you can configure Firewall Protection, Browsing Protection, Malware Protection, Browser Sandbox, and News Alert.
External Drives & Devices	Helps you configure protection for external drives. You can configure protection such as Autorun Protection, Scanning External Drives, and Data Theft Protection.

The second section includes the product menus that help you configure the general settings of Thirtyseven4 and tools for preventing virus infection. You can diagnose the system and view the reports of various activities of the features and access Help and license details.

Settings	Helps you customize features such as Automatic Update, Internet Settings, Registry Restore, Self Protection, Password Protection, Reports Settings, Report Virus Statistics, and Restore Default Settings.
Tools	Helps you diagnose the system in case of virus attacks, clean application and Internet activities, restore the Internet Explorer settings modified by malwares, isolate the infected and suspicious files, remove roguewares and prevent USB drives against autorun malware infection. You can also exclude files from virus protection.
Reports	Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Scheduler, Quick Update, Memory Scan, Registry Restore, Boot Time Scanner, AntiMalware Scanner, Browsing Protection, and Firewall Protection.
Help	Helps you access Help for Thirtyseven4 AntiVirus, see details about product version, virus database, validity details, license details and seek Technical Support.

The bottom section includes the following.

News	Displays the latest news from Thirtyseven4. You can see all the news by clicking **See All**.
Scan	Provides you with various scan options such as Full System Scan, Custom Scan, Memory Scan, and Boot Time Scan.
Support	Helps you get to the support system available in **Support**.
Like	Follow us on Facebook.

Right Shell Menu Options

The Thirtyseven4 AntiVirus icon in the taskbar helps you access and use some of the important features that are as follows:

Open Thirtyseven4 AntiVirus	Helps you launch Thirtyseven4 AntiVirus.
Launch AntiMalware	Helps you launch Thirtyseven4 AntiMalware.
Enable / Disable Silent Mode	Helps you enable / disable all Thirtyseven4 prompts and notifications.
Secure Browse	Helps you launch your default browser in Sandbox for secure browsing.
Enable / Disable Virus Protection	Helps you enable / disable Thirtyseven4 Virus Protection.
Update Now	Helps you update Thirtyseven4 AntiVirus.
Scan Memory	Helps you scan system memory for viruses.

Chapter 4

Thirtyseven4 Protection Center

Thirtyseven4 Protection Center is your instant interface to vital protection settings that can affect files, folders, emails, and so on. It helps you configure protection rules against viruses that try to infiltrate your system through Internet, external drives, and emails.

Thirtyseven4 Protection Center is split into various sections. The top strip of the Protection Center acts as a security status indicator with color coded icons that indicates the security status. Each colored icon has an action associated with it that needs to be executed by the user.

The icons and the description of their status are as follows.

Red		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.
Green		Indicates that Thirtyseven4 AntiVirus is configured with optimal settings and your system is protected.
Yellow		Indicates that a feature of Thirtyseven4 AntiVirus needs your attention at your earliest convenience, but not immediately.

Thirtyseven4 Protection Center also provides you with various categories of protection and customizable settings. These categories are the areas or medium through which malware can gain access and infect your system.

Each of these categories displays vital features that must always be kept turned on. If you turn off any of these features, the corresponding category icons turn to red. The categories and their corresponding features displayed on Dashboard are as follows.

Files & Folders	Scan Settings, Virus Protection, DNA Scan, Quarantine & Backup
Emails	Email Protection
Internet & Network	Firewall Protection, Browser Sandbox
External Drives & Devices	Autorun Protection, Scan External Drives, Data Theft Protection

Files & Folders

With Files & Folders, you can set the protection rules for files and folders in your system. You can set the protection rules for the following settings.

Scan Settings

With Scan Settings, you can define about how to initiate the scan of your system and what action should be taken when a virus is detected. However, the default settings are optimal that ensures the required protection to your system.

To configure Scan Settings, follow these steps:

1. Open **Thirtyseven4 AntiVirus Security**.
1. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
2. Click **Scan Settings**.
3. Under **Select scan mode**, select **Automatic (Recommended)** to initiate the scan automatically, or select **Advanced** for advanced level scanning.
4. Under **Select action to be performed when virus is found**, select an appropriate action.
5. If you want to take a backup of the files and folders before taking an action on them, select **Backup before taking action**.
6. To save your settings, click **Save Changes**.

Select scan mode

Automatic (Recommended): The Automatic scan type is the default scan type , which is recommended as it ensures the optimal protection that your system requires. This setting is an ideal option for novice users as well.

Advanced: The Advanced scan type helps you customize the scanning behavior. This is ideal for experienced users only. When you select the Advanced option,

the Configure button is activated and you can configure the Advanced setting for scanning.

Action to be performed when a virus is found

Repair	If a virus is found during a scan, it repairs the file or automatically Quarantines it, if it cannot be repaired. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. If the infectious file has a Backdoor, Worm, Trojan, or Malware then Thirtyseven4 AntiVirus Security automatically deletes the file.
Delete	Deletes a virus-infected file without notifying you. When the scan is over, a summary window appears providing the details about all the actions taken and other scan details. Once the files are deleted, they cannot be recovered.
Skip	If this option is selected the files are scanned but no action is taken on the infected files and they are skipped. Select this option if you want to take no action even if a virus is found. When the scan is over a summary report appears providing all the scan details.
Backup before taking action	The scanner keeps a backup of the infected files before disinfecting them. The files that are stored in the backup can be restored from the Quarantine menu.

Configuring Advanced Scan Mode

To configure Advanced Scan mode, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Scan Settings**.
4. Under **Select scan mode**, select **Advanced**.

   The Configure button is activated.
5. Click **Configure**.

   The advanced scan setting details screen appears.
6. Under **Select item to scan**, select **Scan executable files** if you want to scan only the executable files or select **Scan all files** if you want to scan all files.

   However, the Scan executable files option is selected by default.

   It takes time to execute Scan all files and the scanning process slows your system considerably.

7. Select one of the following items for scanning:

- Scan archive files: Select this option if you want to scan the archive files such as zip files, RAR files and so on.
- Scan packed files: Select this option if you want to scan packed files.
- Scan mailboxes: Select **Quick scan of mailboxes** for a brief scan or else select **Through scan of mailboxes** to scan thoroughly.

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

Scan archive files

The Scan archive files help you further set the scan rules for archive files such as ZIP files, RAR files, CHM files, and so on.

To configure the Scan archive files, follow these steps:

1. Select **Scan archive files**.

   The Configure button is activated.

2. Click the **Configure** button.

   The Scan archive files details screen appears.

3. Under **Select action to be performed when virus is found**, select any one of the following: Delete, Quarantine, and Skip.
4. In **Archive Scan Level**, select the level till you want to scan the files and folders.
5. Under **Select the type of archive that should be scanned**, select the archive files types.
6. Click **OK** to save your settings.

Action to be taken when a virus is found	
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	Skips the virus and archive file without taking any action.

Archive Scan level	Set the level to scan inside an archive. The default scan level is set to level 2. However, increasing the default 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 of the common archive file types are selected by default that you can customize based on your requirement.

Select All	Helps you select all the archive file types in the list.
Deselect All	Helps you clear all the archive file types in the list.

Scan packed files

With **Scan packed files**, the scanner will scan packers also. Packers are the files that pack together many files, or compress a single file to reduce the file size. Moreover, these files do not need a third-party application to get unpacked. They have an inbuilt functionality for packing and unpacking.

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

Scan mailboxes

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

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

Virus Protection

With Virus Protection, you can continuously keep monitoring your system for viruses that might have tried to infiltrate from various sources such as email attachments, Internet downloads, file transfer, file execution and so on.

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

To configure Virus Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Turn **Virus Protection** ON.
4. Click **Virus Protection**.

   The Virus Protection details screen appears.
5. Do the following:
   - **Display alert messages** – Select this option if you want to get the alerts about various events such as when malware is detected. However, this option is selected by default.
   - **Select action to be performed when virus is detected** – Select an appropriate action when a virus is detected during the scan.
   - **Backup before taking action** – Select this option if you want to take a backup of a file before taking an action on a file. Files that are stored in the backup can be restored from the Quarantine menu.
   - **Enable sound when threat is detected** – Select this option if you want to be alerted with sound whenever a virus is detected.
6. Click **Save Changes** to save your setting.

Action to be taken when a virus is detected

Repair	During scan if a virus is found, it repairs the file or automatically Quarantines it if it cannot be repaired.
Delete	Deletes a virus-infected file without notifying you.
Deny Access	Restricts access to a virus infected file from use.

Turning Off Virus Protection

Turning **Virus Protection** OFF is suggested only when absolutely necessary. Moreover, you can set it off for a certain period of time so that it turns ON automatically thereafter. However, when you try to turn off Virus Protection, a message is displayed.

The following are the options for turning Virus Protection OFF:

- Turn on after 15 minutes
- Turn on after 30 minutes
- Turn on after 1 hour
- Turn on after next reboot
- Permanently disable

Select an option and click **OK**.

Once you turn off Virus Protection, the icon color of the Files & Folders option on Dashboard changes from green to red and a message “System is not secure” is displayed. If you have selected any of the options for turning off temporarily or after next boot then the icon color changes back from red to green after the certain time passes or at the next boot. If you have selected to disable permanently, then the icon color remains red until you turn Virus Protection on manually.

DNA Scan

DNA Scan is the indigenous technology of Thirtyseven4 to detect and eliminate new and unknown malicious threats in the system. DNA Scan technology successfully traps suspected files with very less false alarms. Additionally it copies the suspected file in the Quarantine directory before taking any action. The Quarantined-suspicious files can be submitted to our research labs for further analysis that helps in tracking new threats and curb them on time. After the analysis, the threat is added in the known threat signature database and the solution is provided in the next updates to the users.

Whenever DNA Scan detects a new malicious threat in your system, a message about it is sent to you, or prompts you for taking an action during memory scanning if the scanning is set with Prompt settings. One copy of DNA Scan suspected files is also quarantined that you can submit later to the research labs. You can submit the suspicious files either automatically or manually through email. The submission takes place whenever Thirtyseven4 AntiVirus updates itself and finds new DNA Scan suspected files in the Quarantine folder. It sends new DNA Scan suspicious quarantined files in an encrypted file format to the Thirtyseven4 research labs.

To configure DNA Scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Turn **DNA Scan** ON.
4. Click **DNA Scan**.

   The DNA Scan details screen appears.
5. Under **Select suspicious files**, select either of the following:
   - **Do not submit files** – Select this option if you do not want to submit files to the Thirtyseven4 research labs.
   - **Submit files** – Select this option if you want to submit the suspicious files. You can also select the **Show notification while submitting files** to get prompts for permission before submitting the files to the Thirtyseven4 Research labs.

If Show notification while submitting files option is not selected, Thirtyseven4 submits the suspicious files without notifying you.

Manual submission can be done through the Quarantine tool.

Block Suspicious Packed Files

Suspicious Packed Files helps you identify and block suspiciously packed files. Suspiciously packed files are the files that are packed using pre-defined list of suspicious packers. Such packers are mostly used to pack malicious files, and when unpacked can cause serious harm to the computer. It is recommended that you always keep this option turned on as it prevents spread of threats.

To configure Block Suspicious Packed Files, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Turn **Block Suspicious Packed Files** ON.

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

Automatic Rogueware Scan

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

To configure Automatic Rogueware Scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Turn **Automatic Rogueware Scan** ON.

   However, Automatic Rogueware Scan is turned on by default.

Scan Schedule

With Scan Schedule, you can define a schedule when to begin scanning of your system automatically. You can define multiple numbers of scan schedules so that the scan is initiated at your convenience. Scanning regularly helps you to keep your system free of virus and other types of threats.

Configuring Scan Schedule

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Scan Schedule**.

   The Scan Schedule details screen appears.
4. To define a new scan schedule, click **New**.
5. In **Scan Name**, type a scan name.
6. Under Scan Frequency, select the following based on your preferences:

· Scan Frequency:

  § Daily: Select the Daily option if you want to initiate scanning of your system daily. However, this option is selected by default.

  § Weekly: Select the Weekly option if you want to initiate scanning of your system on a certain day of the week. When you select the Weekly option, the Weekdays drop-down list is activated so you can select a day of the week.

- Scan time:
  - Start at first boot: Select **Start at first boot** to schedule the scanner to begin at the first boot of the day. When you select Start at first boot, you do not have to specify the time of the day to start the scan. Scanning takes place only during the first boot regardless what time you start the system.
  - Start at: Select **Start at** if you want to initiate the scanning of your system at a certain time. When you select Start at, the time drop-down list is activated where you can set the time for scanning. However, this option is selected by default.

    You can also define how often the scan should begin in the **Every day(s)** and **Repeat scan after every** options.
- Scan priority.
  - High: Select High if you want to have the scanning priority at high.
  - Low: Select Low if you want to have the scanning priority at low. However, this option is selected by default.

7. Under **Scan Settings**, you can specify scan mode, define the advanced options for scanning, action to be performed when virus is found and whether you want a backup of the files before taking any action on them. However, the default setting is adequate for scanning to keep your system clean.
8. Provide **User Name** and **Password**.
9. Select **Run task as soon as possible if missed** to initiate scan of the missing tasks.

   This option is available only on Microsoft Windows Vista and later operating systems.
10. Click **Next**.

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

    You can also select **Exclude Subfolder** to exclude subfolders from being scanned. Click **OK**.
13. On the Configure Scan Schedule screen, click **Next**.
14. Check the summary of your scan schedule.
15. Click **Finish** to close the Scan Schedule dialogue.
16. Click **Close** to close the Scan Schedule screen.

Editing a scan schedule

You can change the scan schedule if required. To edit a scheduled scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Scan Schedule**.

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

Deleting a scan schedule

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

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Scan Schedule**.

   The Scan Schedule details screen appears.
4. Select the scan schedule that you want to remove and then click **Remove**.

   The confirmation screen appears.
5. Click **Yes** to remove the selected scan schedule.
6. Click **Close** to close the Scan Schedule screen.

For more details about Scan Schedule, refer to Scan Settings, p- 17.

Exclude Files & Folders

With Exclude Files & Folders, you can decide which files and folders should not be included during scanning for known viruses or issues, DNA Scan, and packers. This helps you avoid unnecessary repetition of the scanning of files which have already been scanned or that you are sure should not be scanned. You can exclude files from being scanned from the following scanning modules:

- Scanner
- Virus Protection
- Memory Scanner
- DNAScan

Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Exclude Files & Folders**.

   The Exclude Files & Folders details screen appears. Here you see a list of files and folders to be excluded from scanning, if you have added any.
4. To add a new file or folder, click **Add**.

   The New Exclude Item screen appears.
5. In the Item text box, provide the path to the file or folder. You can also click the file or folder icon to select the path.

   Ensure that you provide the path to the correct file or folder, else a message appears.
6. Under Exclude From, select the modules from which you want to exclude the selected file or folder.

   You can select either Known virus detection or any from DNAScan and Suspicious packed files scan options.
7. Click **OK**.
8. Click **Save Changes** to save your settings.

- If you are getting warning for a known virus in a clean file, you can exclude it for scanning of Known Virus Detection.
- If you are getting a DNAScan warning in a clean file, you can exclude it from being scanned for DNAScan.

Quarantine & Backup

With Quarantine & Backup, you can safely isolate the infected or suspected files. When a file is added to Quarantine, Thirtyseven4 AntiVirus encrypts the file and keeps it inside the Quarantine folder. Being kept in an encrypted form, these files cannot be executed and hence are safe. Quarantine also keeps a copy of the infected file before repairing if you have selected **Backup before repairing** in the Scanner Settings.

With Quarantine & Backup, you can configure the rules for the files to be removed after a certain period of time and have a backup of the files.

Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Files & Folders**.

   The Files & Folders setting details screen appears.
3. Click **Quarantine & Backup**.

   The Quarantine & Backup details screen appears.
4. Select **Delete quarantine/backup files after** and set the number of days after which the files should be removed from the Quarantine folder automatically. However 30 days is set by default.
5. Click **View Files** to see the quarantined files. In the list of Quarantine files, you can take any of the following actions on the quarantined files:
   - Add: You can add files from folders and drives to be quarantined manually.
   - Remove: You can remove the Quarantine files from the Quarantine list.
   - Restore Selected: You can restore the selected files manually if required so.
   - Remove All: You can remove all the Quarantined files from the Quarantine list.
   - Send: You can send the selected files to our research labs.
   - Close: Helps you close the quarantine dialogue.

Emails

With Email Security, you can customize the protection rules for receiving emails from various sources. You can set rules for blocking emails which are suspicious of malware.

Email Security includes the following.

Email Protection

With Email Protection, you can set the protection rules for all incoming emails. You can block the infected attachment in the emails that may be suspicious of malware and viruses. You can also customize the action that needs to be taken when malware is detected in the emails.

However, Email Protection is turned on by default and the default settings provide the required protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection.

Configuring Email Protection

To configure Email Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Emails**.

   The Emails setting details screen appears.
3. Turn **Email Protection** ON.

   However, Email Projection is turned on by default.

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

   

   The message on viruses includes the following information: Virus Name, Sender Email Address, Email Subject, Attachment Name, and Action Taken.
6. Under **Select action to be performed when virus is found**, select **Repair** to get your emails or attachment repaired when a virus is found, or select **Delete** to delete the infected emails and attachments.

   

   If the attachment cannot be repaired then it is deleted.

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

Attachment Control Settings

Block attachments with multiple extensions	Helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
Block emails crafted to exploit vulnerability	Helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
Enable attachment control	Helps you block email attachments with specific extensions or all extensions. However, this option is not selected by default. If you select this option, the following are available: **Block all attachments**: Helps you block all types of attachments in emails. **Block user specified attachments:** Helps you block email attachments with certain extensions. If you select this option, the **Configure** button is activated. For further settings, click **Configure** and set the following: · Under **User specified extensions**, select the extensions that you want to retain so as to block the email attachments with such extensions and delete all the remaining extensions. · If certain extensions are not in the list that you want to block, type such extensions in the extension text box and then click **Add** to add them in the list. · Click **OK** to save changes.

Trusted Email Clients Protection

Trusted Email Clients Protection supports most of the commonly used email clients such as Eudora and others. If your email client is different from the ones provided in the list, you can add such email clients in the trusted email client list.

Configuring Trusted Email Clients Protection

To configure Trusted Email Clients, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Emails**.

   The Emails setting details screen appears.

3. Turn **Trusted Email Clients Protection** ON.
4. To add a new email client, click **Trusted Email Clients Protection**.

   The Trusted Email Clients Protection details screen appears.
5. Click **Browse** and select a trusted email client
6. Click **Add** to add the email client in the list.
7. Click **Save Changes** to save your settings.

Internet & Network

With Internet & Network, you can set the protection rules to save your system from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on.

Internet & Network includes the following.

Firewall Protection

Firewall Protection works silently in the background and monitors network activity for malicious behavior. Firewall Protection first detects any malware and if found eliminates before the malware can infiltrate into the system.

Configuring Firewall Protection

To configure Firewall Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Internet & Network**.

   The Internet & Network setting details screen appears.
3. Turn **Firewall Protection** ON.

   Firewall Protection is activated.

Browsing Protection

With Browsing Protection, you can block malicious websites while browsing so that you are prevented from coming in contact with malicious websites and you are secure. However, Browsing Protection is turned on by default.

Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Internet & Network**.

   The Internet & Network setting details screen appears.
3. Turn **Browsing Protection** ON.

   Browsing Protection is activated.

Malware Protection

With Malware Protection, you can protect your system from threats such as spywares, adwares, keyloggers, and riskwares while you are connected to the Internet.

Configuring Malware Protection

To configure Malware Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Internet & Network**.

   The Internet & Network setting details screen appears.
3. Turn **Malware Protection** ON.

   Malware Protection is activated.

Browser Sandbox

With Browser Sandbox, you can apply a strict security mechanism to prevent access to all untrusted and unverified sites whether they are commercial sites, suppliers, sellers, third-parties, advertisements, entertainments sites.

Configuring Browser Sandbox

To configure Browser Sandbox, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Internet & Network**.

   The Internet & Network setting details screen appears.
3. Turn **Browser Sandbox** ON.

4. Click **Browser Sandbox**.
5. Select the Browser security level.

   However, the default setting is optimum and ideal for the novice users.
6. Do the following:
   - § To protect your confidential data (such as bank statements, pictures, important documents etc.) while you are surfing, select **Prevent browser from accessing confidential folders**, and then select the folder that you want to protect.

     The data in the confidential folder will not be accessible by the browser and other applications running under Browser Sandbox and hence your data are safe against confidential breach.
   - § To protect your data from being manipulated, select **Prevent browser from modifying the protected data**, and then select the folder that you want to protect.

     The data in the protected folder will be accessible but they cannot be manipulated, or modified.
   - § To download content while surfing in a certain folder, select **Allow browser to store all downloads in the specified folder** and then give the path to the folder.

     This helps you download content while surfing in a certain folder that you need for future use.
7. Select **Show green border around browser window** to indicate that your browser is running in Sandbox.

   However, this is not a mandatory feature for security and you may not select this feature if you prefer.
8. To clean Sandbox cache, click the **Delete** button.

   This helps to clean temporary files.
9. Click **Save Changes** to save your settings.

News Alert

With News Alert, you get the latest news alert about the cyber security, important information related to Thirtyseven4 etc. the latest news is also available on Thirtyseven4 Dashboard. If you do not want to get the news alert, turn News Alert off.

Turning News Alert OFF

To turn News Alert off, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Internet & Network**.

   The Internet & Network setting details screen appears.
3. Turn **News Alert** OFF.

External Drives & Devices

With External Drives & Devices, you can set protection rules for all external devices and drives such as CDs, DVDs, USB-based drives and so on. Whenever your system comes in contact with any external devices or drives, your system is at risk that malware may infiltrate.

Autorun Protection

Autorun Protection 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.

Configuring Autorun Protection

To configure Autorun Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **External Drives & Devices**.

   The External Drives & Devices setting details screen appears.
3. Turn **External Drives & Devices** ON.

   Autorun Protection is activated.

Scan External Drives

With Scan External Drives, you can scan the USB-based drives as soon as they are attached to your system. The 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.

Configuring Scan External Drives

To configure Scan External Drives, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **External Drives & Devices**.

   The External Drives & Devices setting details screen appears.
3. Turn **Scan External Drives** ON.

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

Scan External Drives does not work if **Data Theft Protection** is turned on, and its option **Block complete access to external drives** is selected.

Data Theft Protection

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

Configuring Data Theft Protection

To configure Data Theft Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **External Drives & Devices**.

   The External Drives & Devices setting details screen appears.
3. Turn **Data Theft Protection** ON.

   Data Theft Protection is activated.

4. Click **Data Theft Protection**.
5. Do any of the following:
   - Select **Read only and no write access to external drives** to allow transfer of data from the USB drives and CD/DVD devices to the system but not vice versa . However, this option is selected by default.
   - Select **Block complete access to external drives** to block transfer of data between the system and all external devices.
   - Select **Authorize USB drive** if you want to restrict accessing the USB drives and CD/DVD devices. If this option is selected, and you connect an external device to your system, you are prompted for password to access the external device . Only when you authorize, the external device can be accessed. This option is available only if Thirtyseven4 Password Protection in Settings is turned on.
6. Click **Save Changes** to save your settings.

Chapter 5 Quick Access Features

Quick Access Features provides you with quick access to important features such as Scan and so on. It also provides latest news about Thirtyseven4.

Secure Browse icon

The Thirtyseven4 Secure Browse icon on your desktop helps you launch your default browser in Sandbox for secure browsing. This helps you browse securely even if you have kept Browser Sandbox turned off.

Scan

The Scan option available on Dashboard provides you with various options of scanning your system to suit your requirements. You can initiate scanning of your entire system, drives, network drives, USB drives, folders or files, certain locations and drives, memory scan, and boot time scan. Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan as you prefer.

Performing Manual Scans

If virus protection is enabled with default setting, a manual scan is not required as the system is 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 requirement. Although the default settings for manual scanning are usually adequate, you can adjust the options for manual scanning by selecting **Files & Folders > Scan Settings** from the Dashboard.

Performing Full System Scan

With Full System Scan, you can initiate a complete scan of all boot records, drives, folders and files on your computer (excluding mapped network drives).

To initiate a full system scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, select **Scan > Full System Scan**.

   The scanning starts.

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

Performing Custom Scan

With Custom Scan, you can scan specific records, drives, folders, and files on your system that you require. This is helpful when you want to scan only certain items and not the entire system.

To initiate Custom Scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, select **Scan > Custom Scan**.

   The custom scan preference screen appears.
3. Click **Add** and then locate the path to the files and folders that you want to scan. You can select multiple folders for scanning.
4. After setting your scan preference, click **Start Scan**.

   The scanning starts.

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

Performing Memory Scan

To perform a memory scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, select **Scan > Memory Scan**.

   The scanning starts.

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

The following fields are displayed during a scan:

Files scanned	Displays the total number of files scanned.
Archive/Packed	Displays the number of archive or packed files scanned.
Threats detected	Displays the number of threats detected.
DNAScan warnings	Displays the number of files detected by DNAScan.

Boot/Partition viruses	Displays the number of Boot/Partition viruses.
Files repaired	Displays the number of malicious files that have been repaired.
Files quarantined	Displays the number of malicious files that have been quarantined.
Files deleted	Displays the number of malicious files that have been deleted.
I/O errors	Displays the number of I/O errors occurred during the scan.
Scanning status	Displays the current status of the scan being performed.

Performing Boot Time Scan

Boot Time Scan is very useful to 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 set Boot Time Scan, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, select **Scan > Boot Time Scan**.

   Boot Time Scan has the following options:

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

News

The News section displays the latest updates of information and developments from the Thirtyseven4 Labs. Whenever there is any new information about the computer protection, security alerts, or other important issues, news about such things are displayed here. However to get the latest information, you must own licensed version of the product.

Chapter 6

Thirtyseven4 Menus

With the Thirtyseven4 AntiVirus menus, you can configure the general settings for taking updates automatically, password-protect your Thirtyseven4 AntiVirus so that no unauthorized person can change your settings, provide settings for proxy support and set rules for the reports to be removed from the list automatically.

Settings

With Settings, you can apply various protection rules such as you can get the updates from Thirtyseven4 when released, password-protect your settings and set the rule for the reports to be removed and so on. However, the default settings are optimum and can provide complete security to your system. We recommend that you change the settings only when absolutely necessary.

Settings includes the following.

Automatic Update

With Automatic Update, you can get the updates automatically to keep your software updated with the latest virus signatures to protect your system from the latest malware. To get updates regularly, your system on which Thirtyseven4 AntiVirus is installed needs to be connected to the Internet. It is recommended that you always keep Automatic Update turned on. However, Automatic Update is turned off by default.

Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Turn **Automatic Update** ON.

   Automatic Update is activated.
4. Click **Automatic Update**.

5. Select **Show update notification window**, if you want to get notified about the update of Thirtyseven4 AntiVirus. However, this option is turned on by default.
6. Select the update mode from:
   - § **Download from Internet** – Helps you download the updates to your system from the Internet.
   - § **Pick update files from the specified path** – Helps you pick the updates from a local folder or a network folder.
   - § **Download from Admin Console Sever** – Helps you download the updates to your system from Thirtyseven4 server.
   - § **Copy update files to specified location** – Helps you save a copy of the updates to your local folder or network folder.
7. Click **Save Changes** to save your settings.

Internet Settings

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

The following Thirtyseven4 modules require these changes.

- · Registration Wizard
- · Quick Update
- · Messenger

Configuring Internet Settings

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Click **Internet Settings**.
4. Select **Enable proxy settings**.

   The proxy type, server, port, and user credentials text boxes are activated.
5. In **Type** list, select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.

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

   Port number is set as 80 for HTTP and 1080 for SOCKS V4, SOCKS V5 by default.
8. Enter your user name and password credentials.
9. Click **Save Changes** to save your settings.

Registry Restore

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

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

Configuring Registry Restore

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Click **Registry Restore**.
4. Select **Restore critical system registry areas** to restore the critical system registry during the scan. Critical System Registry areas are generally changed by malware to perform certain task automatically or to avoid detection or modification by system applications such as Disabling Task Manager, and Disabling Registry Editor.
5. Select **Repair malicious registry entries** to scan system registry for malware related entries. Malware and its remains are repaired automatically during the scan.

Self Protection

With Self Protection, you can apply protection to your application Thirtyseven4 AntiVirus so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way.

Configuring Self Protection

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Turn **Self Protection** ON.

   However Self Protection is turned on by default.

Password Protection

With Password Protection, you can restrict all other users from accessing Thirtyseven4 AntiVirus so that no unauthorized users can make any changes in the settings. You are recommended to always keep Password Protection turned on.

Configuring Password Protection

To configure Password Protection, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Turn **Password Protection** ON.

   Password Protection setting screen appears.
4. In **Enter new password**, enter a new password if you are setting the password for the first time, and then enter the same password in **Confirm new password**.

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

Report Settings

With Report Settings, you can set rules for the reports to be removed generated on all activities. You can specify the number of days after which the reports should be removed from the list automatically. You may also retain the reports if you need them. However, the default setting for deleting reports is 30 days.

Configuring Report Settings

To configure Report Settings, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Click **Password Protection**.

   The Report Settings screen appears.
4. Select **Delete reports after**, and then select the number of days after which the reports should be removed automatically.

   *However, 30 days is by default. If you clear **Delete reports after**, no reports will be removed.*
5. Click **Save Changes** to apply the settings.

Report Virus Statistics

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

Configuring Report Virus Statistics

To configure Report Virus Statistics, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. Turn **Report Virus Statistics** ON.

   The Report Virus Statistics is activated.

Restore Default Settings

With Restore Default Settings, you can restore your customized settings to the system default settings. This is very helpful when you configure the settings but you are not satisfied with the protection settings or you are doubtful about the protection or you feel your protection is being compromised, you can restore the system default settings. However, you can set any of the settings as you prefer later.

Restoring Default Settings

To restore default settings, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Settings**.

   The Settings details screen appears.
3. On the Restore Default Settings, click the **Default All** button.

   Your Thirtyseven4 AntiVirus is set to default settings.

Tools

With Tools, you can carry out various activities such as you can clean and restore settings, prevent access to drives, diagnose system and so on.

Tools includes the following.

Hijack Restore

With Hijack Restore, you can restore 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, 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 such as Registry Editor and Task Manager.

Using Hijack Restore

To use Hijack Restore, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Hijack Restore**.

   The Hijack Restore screen appears.

4. Select **Check All** to select all the browser settings in the list.
5. Select **Restore default host file**, to restore default host file.
6. Select **Restore important system settings**, to restore important system settings.
7. To initiate restoring your settings, click **Restore Now**.

Restore default host file

The default host file includes the following:

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

Restore important system settings

The restore important system settings option includes the following.

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

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

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

Track Cleaner

With Track Cleaner, you can remove the most recently used (MRU) applications to ensure that your privacy is not breached. Most of the applications store the list of recently opened files in their internal format to help you open them again for quick access. However, in the case that a system is used by more than one user the user's privacy may be compromised. Track Cleaner helps remove all the tracks of such applications and prevent privacy breach.

Using Track Cleaner

To use Track Cleaner, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Track Cleaner**.

   The Track Cleaner screen appears.
4. Select the applications whose traces you want to remove or select **Check All** to select all the applications in the list.
5. To initiate cleaning, click **Start Cleaning**.
6. Upon completion click **Close** to exit.

Anti-Rootkit

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

However, it is recommended that Thirtyseven4 Anti-Rootkit should be used by a person who has 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.

Using Thirtyseven4 Anti-Rootkit

To use Anti-Rootkit, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **Anti-Rootkit**.

   A pop-up appears that recommends closing all other applications before launching Anti-Rootkit.
4. In the left pane on the Anti-Rootkit screen, click the **Start Scan** button.

   Thirtyseven4 Anti-Rootkit starts scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.

   After completion of the scan, the result is displayed in three tabs.
5. Select the appropriate action against each threat displayed. For example, you can terminate the rootkit Process, rename the rootkit Registry entry/Files and Folders.

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

Stop Scanning	Helps you stop the scan while the scan is under way.
Close	Helps you close the Anti-Rootkit. If you choose to close the Anti-Rootkit 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 the Settings feature available on the Anti-Rootkit screen, you can select what item to scan during scan process.

Configuring Thirtyseven4 Anti-Rootkit Settings

1. Open **Thirtyseven4 Anti-Rootkit**.
2. On the Thirtyseven4 Anti-Rootkit screen, click **Tools**.

   The Tools dialog appears.
3. Thirtyseven4 Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.

Auto Scan	Auto Scan is the default scan setting for Anti-Rootkit. Under Auto Scan, the Thirtyseven4 Anti-Rootkit scans the predefined system areas such as: · Hidden Processes. · Hidden Registry entries. · Hidden Files and Folders. · Executable ADS.

Custom Scan	Helps you customize the scan setting for Anti-Rootkit for the following: **Detect Hidden Process** – scans for the hidden processes running in the system. **Detect Hidden Registry Items** – scans for the hidden items in Windows Registry. **Detect Hidden files and folders** – scans for the hidden files and folders in the system and executable ADS (Alternate Data Streams). You can choose option: · Scan drive on which Operating System is installed · Scan all fixed drives · ADS (Alternate Data Streams) to scan for executable ADS.
Report File Path	Thirtyseven4 Anti-Rootkit creates a scan report file at the location from which it is executed. However, you can specify different location.

Overview of Alternate Data Streams – ADS

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 may 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

1. Open **Thirtyseven4 Anti-Rootkit**.
2. In the left pane on the Thirtyseven4 Anti-Rootkit screen, click the **Start Scan** button.
3. Thirtyseven4 Anti-Rootkit starts scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.

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

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

Action to be taken on Scan Results

Process	After the scan is complete, Thirtyseven4 Anti-Rootkit will detect and display a list of hidden Processes. You can select process for termination, but make sure that the list of Processes for termination does not include any known trusted process. Thirtyseven4 Anti-Rootkit also displays a summary of process scanning about total number of Processes scanned and number of hidden Processes detected.
Terminating Hidden Process	After selecting list of Processes for termination, click the Terminate button. If a process is successfully terminated then its PID (Process Identifier) field will show n/a and process name is appended by Terminated. All terminated Processes will be renamed after a restart.

Registry	Similar to the Process scan, Thirtyseven4 Anti-Rootkit displays a list of hidden Registry keys. You can select keys for renaming, but make sure that the list of keys for renaming does not include any known trusted registry key. Thirtyseven4 Anti-Rootkit also displays a summary of Registry scanning about total number of items scanned and number of hidden items detected.
Renaming Hidden Registry Key	After selecting list of keys for renaming, click the Rename button. Renaming operation requires reboot hence Key name will be prefixed by Rename Queued.

Files and Folders	Similarly, Thirtyseven4 Anti-Rootkit displays a list of hidden Files and Folders. You can select Files and Folders for renaming, but make sure that the list of Files and Folders for renaming does not include any known trusted file. Thirtyseven4 Anti-Rootkit also displays a list of executable Alternate Data Streams. Thirtyseven4 Anti-Rootkit also displays a summary of File scanning about total number of files scanned and number of hidden files detected.
Renaming Hidden Files and Folders	After selecting list of Files and Folders for renaming, click the Rename button. Renaming operation requires reboot hence Files and Folders name will be prefixed by Rename Queued.

Cleaning Rootkits through Thirtyseven4 Emergency Disk

At times, rootkits are not cleaned and they reappear during Thirtyseven4 Anti-Rootkit scan. In such a case you can also use Thirtyseven4 Emergency Disk for proper cleaning. For cleaning this way, create Thirtyseven4 Emergency Disk and boot your system through it.

To create Thirtyseven4 Emergency Disk and clean your system through it, follow these steps:

Step 1

To create Thirtyseven4 Emergency Disk, follow the link Create Emergency Disk, p-51.

Step 2

1. Open **Thirtyseven4 Anti-Rootkit**.
2. In the left pane on the Thirtyseven4 Anti-Rootkit screen, click the **Start Scan** button.

   Thirtyseven4 Anti-Rootkit starts scanning your system for suspicious rootkit activity in running Processes, Windows Registry and Files and Folders.

   After completing the scan result is displayed in three different tabs.
3. Take the appropriate action against each threat displayed. For example, you can terminate the rootkit process or rename the rootkit registry entry or files.

Step 3

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

Creating Emergency Disk

You can create your own emergency bootable Disk that will help you boot your Windows computer system and scan and clean all the drives including NTFS partitions. This Disk helps in cleaning badly infected system from file infecting viruses that 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, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.

3. Under Cleaning & Restore Tools, click **Create Emergency Disk**.
4. On the Create Emergency Disk screen, click the link and download the required package.
5. Extract the downloaded package on your system. For example, c:\my documents\qhemgpkg.
6. Provide the extracted package path, and click **Next**.
7. To create Emergency Disk, select any one of the options that are displayed on the screen. For example, select either **Create Emergency USB disk** or **Create Emergency CD/DVD**.
8. Select the disk drive to be converted to an Emergency Disk and click **Next**.

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

Things to remember while creating an Emergency Disk

- It is recommended that you retain a copy of the extracted package on your system.
- 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, 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 **Emergency Disk** into your CD/DVD/USB drive.
2. Restart your system.
3. Emergency Disk starts scanning all the drives automatically. It will disinfect the infection, if found.
4. Restart your system.

Launch AntiMalware

Thirtyseven4 AntiMalware, with its improved malware scanning engine, scans registry, files and folders at a very high 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 in any of the following ways:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Thirtyseven4 AntiMalware**.
2. Right-click the Virus Protection icon on the Windows system tray and select **Launch AntiMalware**.
3. Click **Tools > Launch AntiMalware** from the Thirtyseven4 Dashboard.

Using Thirtyseven4 AntiMalware

On the Thirtyseven4 AntiMalware screen, click **Scan Now** 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 clear specific file, folder or registry entries within the displayed list, but ensure that all cleared items are genuine applications and not malicious ones.

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

Clean	Helps you clean the malwares and its remains from the system. If you clear the specific file, folder or registry entry, you are prompted whether you want to exclude those items in future scan. If you want to permanently exclude those items, click **Yes**, otherwise click **No** for temporary exclusion.
Skip	Helps you skip taking any action against malwares in your system.
Stop Scan	Helps you stop the scan.
Set System Restore point before cleaning	Helps you create System Restore point before the cleaning process starts in your system. This helps you revert to the cleaning done by Thirtyseven4 AntiMalware by using Windows System Restore facility. **Set System Restore point before cleaning** feature is not available on Windows 2000 operating system.
Details	Helps you redirect to Thirtyseven4 Website.

View Quarantine Files

With Quarantine, you can safely isolate 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 the infected file before repairing. However, you can take a backup of the files also before taking an action.

Launching Quarantine Files

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Cleaning & Restore Tools, click **View Quarantine**.

   A list of all quarantined files is displayed.

You can perform the following tasks with the Quarantine feature:

Add	Helps you add a file to Quarantine manually.
Remove	Helps you remove a quarantined file.
Restore	Helps you restore a file from Quarantine to its original location.
Remove All	Helps you remove all the quarantined files.
Send	Helps you send the quarantined file to our research labs for further analysis. Select the file that you want to submit and click **Send**.

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

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

With Thirtyseven4 AntiVirus, you can safeguard your USB devices from autorun malware. The Autorun feature of the removable drive is one of the mediums for malware to infiltrate your system. The USB Drive Protection feature prevents autorun malware 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 malware to other system.

To safeguard removable drives, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Preventive Tools, click **USB Drive Protection**.
4. In the **Select a removable drive** list, all the removable drives plugged into your system are listed. Select the drive and click the **Secure Removable Drive** button.

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

Thirtyseven4 recommends that you keep the autorun feature of your USB drive turned off, however, if you may turn on the Autorun feature of the USB drive following the same process as mentioned in here.

System Explorer

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

To use system explorer, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Diagnostic Tools, click **System Explorer**.

Windows Spy

With Windows Spy, you can find out more information about an application or process whenever required. Sometimes, we keep on getting dialog boxes or messages that are actually shown by spyware or some malware and we are not able to locate the malware. In such a case, this tool can be used to find out more information about the application by dragging the target on to the dialog or window that appears on the screen. This tool will provide following information about the dialog or a window.

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

Using Windows Spy

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

   The Tools details screen appears.
3. Under Diagnostic Tools, click **Windows Spy**.
4. Drag the mouse pointer on the application.

   A window will be opened displaying above mentioned information.
5. If you want to terminate that application or window, click **Kill Process**.

Exclude File Extensions

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

Creating Exclusion List for Virus Protection

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Tools**.

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

Reports

Thirtyseven4 AntiVirus creates and maintains a detailed report of all important activities such as virus scan, updates details, changes in settings of the features, and so on.

The reports on the following features of Thirtyseven4 AntiVirus can be viewed

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

Viewing Reports

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

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus Dashboard, click **Reports**.

   A Reports list appears.
3. In the **Reports for** list, click the feature to view report.

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

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

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

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

For more details about Reports, refer to Reports, p-57.

Help

With the Help feature, you can access the Help topics whenever you want to know about how to use and configure the Thirtyseven4 AntiVirus Security features, how to seek support from Thirtyseven4, LLC., how to update the product, and see the license details of the product.

The Help feature includes the following.

- **Help**: Helps you access the in-built Help topics irrespective whether you are connected to the Internet or not. Select **Help > Help**, you are redirected to the Help page where you can find topics that describe the features of the product and how to use them. (Alternatively, press **F1** key, or click the **Help** button in a dialog to get to the Help page.)
- **Submit System Information**: Helps you submit information of your system to Thirtyseven4 for analysis.

  For details about how to submit System Information, refer to System Information, p-60.
- **Support**: Helps you seek support from the Customer Care of Thirtyseven4, LLC. whenever you face issues regarding the product or its features. Support has the options: Web Support (Visit FAQ), Email Support, Phone Support, and Live Chat Support.

  For more details about Support, refer to Support, p-66.
- **About**: The About section of Thirtyseven4 AntiVirus includes the following information – .

  Thirtyseven4 AntiVirus Version

  License details

  License validity

  Update Now option

Following buttons are also available in the About section:

Renew Now	Renew Now helps you renew your existing subscription.
License Details	License Information and End-User License Agreement (EULA) are available under this section. **Update License Details**: This feature is useful to synchronize your existing License information with Thirtyseven4 Activation Server. If you want to renew your existing subscription and you do not know how to renew it or you face the problem during renewal, you can call Thirtyseven4 Support team and provide your Product key and Renewal Code. Thirtyseven4 Support team will renew your copy. However, you need to follow these steps: 1. Be connected to the Internet. 2. Click **Update License Details**. 3. Click **Continue** to update your existing subscription. **Print License Details**: Click Print License Details to take the print of the existing subscription information.
Update Now	Update Now helps you update virus database of Thirtyseven4 AntiVirus.

System Information

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

To detect new Malwares	This tool gathers information to detect new Malwares from 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 the critical system details and version details of Thirtyseven4 AntiVirus installed on your system in the text and binary format. The Information contains automatic execution of files (through Registry, Autoexec.bat, System.ini and Win.ini) and Running processes along with their supported library details. These details are used to analyze the system for new Malwares and proper functioning of Thirtyseven4 AntiVirus. The above information is used to provide better and adequate services to customers. This tool does not collect any other personally identifiable information such as passwords, nor do we share or disclose this information with anyone. We respect your privacy.

Generating System Information

To generate system information, follow these steps:

1. On the Thirtyseven4 AntiVirus Dashboard, select **Help > Submit System Information**.

   *The System In**formation wiza**rd open**s.***

2. Click **Next** to continue.
3. Select a reason for submitting the system information. If you are suspecting new Malwares in your system, select **I suspect my system is infected by new Malwares** or if you are facing issues while using Thirtyseven4 AntiVirus, select **I am having problem while using Thirtyseven4**. Provide comments in the **Comments** text box and also enter your email address.
4. Click **Finish**.
5. System Information (INFO.QHC) will be generated and sent to Thirtyseven4 Technical Support.

Chapter 7

Updating Thirtyseven4 AntiVirus & Cleaning Viruses

Updates for Thirtyseven4 AntiVirus are released regularly on the website of Thirtyseven4 which contains information pertaining to the detection and removal of newly discovered viruses. To prevent your system from new viruses, you should have the updated copy of Thirtyseven4 AntiVirus. The default setting of Thirtyseven4 AntiVirus is configured to take the updates automatically from the Internet, without the intervention of the user. However, your system must be connected to the Internet to get the updates regularly. Automatic updates can also be applied from a local or a network path, but that path should have the latest set of definitions.

Some important facts about the Thirtyseven4 AntiVirus updates are:

- All the Thirtyseven4 AntiVirus updates are complete updates including Definition File Update, and Engine Updates.
- All the Thirtyseven4 AntiVirus Security updates also upgrade your version whenever required, thus making the new features and technology available for your protection.
- Thirtyseven4 AntiVirus Update is a single step upgrade process.

Updating Thirtyseven4 AntiVirus from Internet

With Update Now, you may update Thirtyseven4 AntiVirus manually whenever you prefer. However, the default setting of Thirtyseven4 AntiVirus is configured to take the updates automatically through the Internet. Your system must be connected to the Internet to get updates regularly. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc).

You can also update Thirtyseven4 AntiVirus manually whenever necessary in any of the followings ways:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Quick Update**.
2. Follow the instructions and click the **Next** button.
3. Select **Download from Thirtyseven4 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 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 have the update definition file with you, you can update Thirtyseven4 AntiVirus without connecting to the Internet. It is useful for Network environments with more than one system. You are not required to download the update file on all the computers within the network using Thirtyseven4. You can download the latest definition files from the website of Thirtyseven4 from http://www.thirtyseven4.com.

To update Thirtyseven4 AntiVirus through definition file, follow these steps:

1. Select **Start > Programs > Thirtyseven4 AntiVirus > Quick Update**.
2. Follow the instructions and click the **Next** button.
3. Select **Pick from specified path**.
4. Click **File** to locate the definition file. Select 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. Select **Start > Programs > Thirtyseven4 AntiVirus > Thirtyseven4 AntiVirus** to open **Thirtyseven4 AntiVirus**.
5. Select **Settings > Automatic Update** from 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 the **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.

Cleaning Viruses

Thirtyseven4 warns you of a virus infection when:

- A virus is encountered during a manual scan.
- A virus is encountered by Thirtyseven4 AntiVirus Virus Protection/Email Protection.

Cleaning viruses encountered during scanning

The default settings of Thirtyseven4 AntiVirus are adequately configured and are optimum to protect your system. If a virus is detected during scanning, Thirtyseven4 AntiVirus tries to repair the virus. However, if it fails in repairing the files of the viruses, such files are quarantined. In case you have customized the default scanner settings, then take an appropriate action when a virus is found.

Scanning Options

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

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

Cleaning virus encountered in memory

"Virus Active in memory" means that a virus is active, and is spreading to other files or 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 are detected, they will be set for deletion in the next boot automatically. Thirtyseven4 AntiVirus memory scan will provide details 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 the 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.

Chapter 8

Technical Support

Thirtyseven4 provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the email or call to receive efficient support from the Thirtyseven4 support executives.

Support

The Support option provides you with a comprehensive online support where you can find answers to your queries in a wide variety of ways. The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, submit your queries, send emails about your queries or call us directly.

Support includes the following.

Web Support

With Web Support, you can submit your queries, and see FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions. However, it is advisable that you check with your queries in FAQ at least once before you resort to other means of support as you may get an answer to your question in FAQ itself.

To use Web Support, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus menu bar, select **Help > Support**.
3. On the Support screen, click **Visit FAQ** to view FAQ.

   Check for the answer to your queries in FAQ. If you do not find the appropriate answer, you may send us your queries.

Email Support

With Email Support, you can send us an email about your queries so that the experts at Thirtyseven4 can reply you with an appropriate answer.

To use Email Support, follow these steps:

1. Open **Thirtyseven4 AntiVirus**.
2. On the Thirtyseven4 AntiVirus menu bar, select **Help > Support**.
3. On the Support screen, click **Submit Ticket** under **Email Support** to submit your queries.

   When you click the Submit Ticket button, you are redirected to our Support webpage where you can submit your queries.
4. You may also email Support at support@thirtyseven4.com.

Technical Support

Thirtyseven4 provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the Thirtyseven4 support executives.

When is the best time to call?

Thirtyseven4, LLC provides technical support between 8:00 AM to 5:00 PM EST, Monday to Friday.

Details that are necessary during the call

- Product Key, that is included inside the box of your product. If the product is purchased online, then the Product Key can be obtained from the email confirming the order.
- Information about your computer system: brand, processor type, RAM capacity, the size of the hard drive and free space on it, as well as information about other peripherals.
- The operating system: name, version number, language.
- Version of the installed anti-virus and the virus database.
- Software installed on your system.
- Is your system connected to a network? If yes, contact the system administrators first. If the administrators cannot solve the problem they should contact the Thirtyseven4 technical support.

- Details: When did the problem first appear? What were you doing when the problem appeared?

What should I say to the technical support personnel?

You need to be as specific as possible and provide maximum details as the support executive will provide solution based on your inputs.

Contact Thirtyseven4 Technologies

Support Centre

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

For more details, please visit http://www.thirtyseven4.com.

Index

