



Thirtyseven4 Total Security *for Mac*

User Guide

Thirtyseven4, L.L.C.
<http://www.thirtyseven4.com>

Copyright Information

© 2013 Thirtyseven4, LLC.

All rights are reserved by Thirtyseven4, LLC.

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmission in any form without prior permission of Thirtyseven4, LLC, P.O. Box 1642, Medina, Ohio 44258.

Marketing, distribution or use by anyone outside of Thirtyseven4, LLC constitutes grounds for legal prosecution.

Thirtyseven4 is a registered trademark of Thirtyseven4, LLC.

End-User License Agreement

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

1. License Grant and Restrictions

In consideration for the license fee paid at time of purchase and subject to the conditions set forth in this Agreement, Company grants to User, a non-exclusive, non-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 AWARE OF THE POTENTIAL FOR SUCH DAMAGES AND LOSS TO OCCUR.

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

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

6. Controlling Law and Severability

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

enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

7. Non-Binding Mediation

Company and User agree to submit the dispute to non-binding mediation before resorting to litigation. Mediation shall occur in Medina, Ohio before a single mediator jointly selected by the parties. The parties agree to each pay one-half of the mediator's fee. Company and User agree to waive any possible arbitration claims unless Company and User later agree to arbitrate this dispute following mediation, wherein such arbitration shall be binding and incur in lieu of litigation.

8. Limitation of Liability and Fees

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

9. Non-Waiver

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

10. Successors; Assigns

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

11. Use of Site Image

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

12. Complete Agreement


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

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

About the Document

This User Guide covers all the information about how to install and use Thirtyseven4 Total Security in the easiest possible ways. We have ensured that all the details provided in this guide are updated to the latest enhancements of 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 is a direction about how to carry out an action.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

Thirtyseven4 Total Security Highlights

Thirtyseven4 Total Security ensures maximum protection against any possible threats or malware that may infect your system when you browse online, work in network environment, and access emails. You can schedule scanning, set rules for Quarantine and Backup for files, set parental control, and block malicious emails and spams.

Mac Security Helps you customize the settings that concern the protection of files and folders in your system. You can set scanning preferences, apply rules for virus protection, schedule scanning, exclude files and folders from scanning, and set rules for quarantine and backup files.

Web Security Helps you set the protection rules to save your machine from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on.

Parental Control Parental Control in Web Security helps you monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

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

For more information, please visit <http://www.thirtyseven4.com>.

Contents

Copyright Information	2
End-User License Agreement	3
About the Document	6
Thirtyseven4 Total Security Highlights	7
Chapter 1. Getting Started	11
Prerequisites	11
System Requirements	11
Installing Thirtyseven4 Total Security	12
Uninstalling Thirtyseven4 Total Security	13
Chapter 2. Registration, Re-activation, Renewal	14
Registration	14
Registering Online	14
Registering Offline	14
<i>Obtaining product key and installation number</i>	15
<i>Generating Activation key for offline activation</i>	15
<i>Activating Thirtyseven4 Total Security with offline activation key</i>	15
Re-activation	16
Renewal	16
Renewing Online	16
Renewing Offline	17
Chapter 3. About Thirtyseven4 Total Security Dashboard	18
Thirtyseven4 Total Security Dashboard	18
Thirtyseven4 Total Security Features	19
Thirtyseven4 Total Security Menus	19
Quick Access Options	20
News	20
Help Topics	20
About Thirtyseven4 Total Security	21
Updating with definition files	22

Chapter 4.	Thirtyseven4 Total Security Features	23
	Mac Security	23
	Scan Settings	23
	Virus Protection	26
	Schedule Scans	27
	<i>Configuring Schedule Scans</i>	28
	<i>Editing Schedule Scan</i>	29
	<i>Removing Schedule Scan</i>	29
	Exclude Files & Folders	29
	<i>Configuring Exclude Files & Folders</i>	30
	<i>Editing Exclude Files & Folders</i>	30
	<i>Removing Exclude Files & Folders</i>	31
	Quarantine & Backup	31
	<i>Configuring Quarantine & Backup</i>	31
	Web Security	32
	Browsing Protection	32
	<i>Configuring Browsing Protection</i>	32
	Phishing Protection	33
	<i>Configuring Phishing Protection</i>	33
	Parental Control	33
	Configuring Parental Control	33
	Email Security	36
	Email Protection	36
	<i>Configuring Email Protection</i>	37
	Spam Protection	37
	<i>Configuring Spam Protection</i>	37
Chapter 5.	Scanning Options	40
	Scan My Mac	40
	Custom Scan	40
Chapter 6.	Thirtyseven4 Total Security Menus	41
	Reports	41
	Viewing Reports	41
	Settings	42
	Automatic Update	42
	<i>Configuring Automatic Update</i>	42
	Password Protection	43
	<i>Configuring Password Protection</i>	43
	Proxy Support	43
	<i>Configuring Proxy Support</i>	44
	Report Settings	44
	<i>Configuring Report Settings</i>	44

Chapter 7.	Updating Software & Cleaning Viruses	45
	Updating Thirtyseven4 Total Security from Internet	45
	Updating Thirtyseven4 Total Security with definition files	46
	Update Guidelines for Network Environment	46
	Cleaning Viruses	47
	<i>Cleaning viruses encountered during scanning</i>	47
	<i>Scanning Options</i>	47
Chapter 8.	Technical Support	48
	Support	48
	Web Support	48
	Email Support	48
	Phone Support	49
	Live Chat Support	49
	Support Guidelines	49
	Contact Thirtyseven4 Technologies	50

Getting Started

Thirtyseven4 Total Security 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 Total Security on your machine:

- A system with multiple anti-virus software programs installed may result in system malfunction. If any other anti-virus software program is installed on your system, you need to remove it before proceeding with the installation of Thirtyseven4 Total Security.
- Close all open programs before proceeding with installation.
- We recommend you to keep a backup of your data in case your system is infected with viruses.
- Thirtyseven4 Total Security must be installed with administrative rights.

System Requirements

To use Thirtyseven4 Total Security, your system should meet the following minimum requirements:

- Mac OS X 10.6 or later
- Mac Computer with Intel Processor
- 512 MB of RAM
- 700 MB free hard disk space
- Internet connection to receive updates

The requirement is applicable to both 32-bit and 64-bit operating systems unless specifically mentioned.

The requirement is applicable to all flavors of the operating system.

The requirements provided are minimum system requirements. Thirtyseven4 recommends your system has higher configuration than the minimum requirements to obtain best results.

To check for the latest system requirements, visit: <http://www.thirtyseven4.com>.

Clients that support email scan

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

- Apple Mail Ver. 10.3 and later
- Thunder bird
- Sparrow
- Sea Monkey
- MailSmith

Clients that do not support email scan

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

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

SSL connections not supported

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

Installing Thirtyseven4 Total Security

To install Thirtyseven4 Total Security on your machine, follow these steps:

- 1** Insert the installation CD/DVD into the drive.

A window with the installer and uninstaller packages appears.

In case, the installer does not appear, search for the disk image on your desktop and open it. Download or copy the installation file ([Thirtyseven4 Total Security.dmg](#)) to your desktop, and then open it.

- 2** To launch the installer, click Thirtyseven4 Total Security.pkg.

The user acceptance agreement screen appears.

- 3** Click Continue.

- 4** On the Welcome screen, click Continue.

The Read Me file appears. You are expected to read the Read Me file in its entirety.

- 5** Click Continue.

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

- 6** Click Continue.

- 7** Click Agree to proceed with the installation.

- 8 To initiate the installation, click Install.

Thirtyseven4 Total Security is set to be installed on your machine at the fixed location. Moreover, you cannot change the location while installing the software.

- 9 Provide your user credentials when prompted.

Thirtyseven4 Total Security installation process starts.

- 10 To initiate the activation process, click Register Now.

- 11 Click Register Later or Continue to perform activation later.

- 12 On Summary page, click Close to close the installer window.

Uninstalling Thirtyseven4 Total Security

Uninstalling Thirtyseven4 Total Security exposes your system and your valuable data to virus threats. However, in case you need to uninstall Thirtyseven4 Total Security, follow these steps:

- 1 Insert the installation CD/DVD into the drive.

A window with the installer and uninstaller packages appears.

In case it does not appear, search for the disk image on your desktop and open it. Download or copy the installation file ([Thirtyseven4 Total Security.dmg](#)) to your desktop, then open it.

- 2 To launch the un-installer, click Thirtyseven4 Un-installer.app.

Follow the instructions on the uninstallation wizard.

- 3 On the Welcome screen, click Yes.

- 4 Enter your password credentials and click OK.

You are prompted for credentials only if the Password Protection is enabled for Thirtyseven4 Total Security.

Thirtyseven4 Total Security maintains a repository of Report Files, Quarantine Files, Backup Files, Black list email address and White list email address. You may retain or delete this repository during uninstallation. However, the Remove Report Files, Remove Quarantine/Backup Files and Remove list of black-list & white-list email senders options are selected by default.

- 5 To continue with uninstallation without saving the repository, click Next. If you want to retain the repository, deselect the options to the respective repositories and click Next.

- 6 Provide your user credentials.

The uninstallation process starts.

Upon completion, a message Thirtyseven4 Total Security has been successfully un-installed appears. You can provide your feedback and reasons for uninstalling Thirtyseven4 Total Security by clicking *Write to us the reason of un-installing Thirtyseven4 Total Security*. Your feedback helps us improve the product quality.

Please note the product key for future reference. You can copy the product key by clicking Copy to pasteboard also. You can also open a document and directly paste this information into the document. Restart is recommended after uninstallation. To restart click Restart Now, or click Restart Later to continue working on your machine and restart after some time.

2

Registration, Re-activation, Renewal

Registration

Thirtyseven4 Total Security needs to be registered upon installation. It is strongly recommended that you register the copy immediately after installation to receive database updates regularly and get technical support. If the product is not regularly updated, it cannot protect your machine against new threats.

Registering Online

- 1 Go to Application > Thirtyseven4 Total Security.
- 2 On the Thirtyseven4 Total Security Dashboard, click Register Now. Alternatively, you can go to Menu > Help > Activation.
- 3 On the Registration Wizard, enter the 20-digit Product Key and click Continue.

The Registration Information appears.

- 4 Enter relevant information in the Purchased From and Register for text boxes and then click Continue.
- 5 Provide relevant information in the Name, Email Address, Contact Number text boxes. Select your choices in the Country, State and City lists.

In case your State/Province and City are not available in the list, you can type your locations in the respective boxes, and then click Continue.

A confirmation screen appears with the details entered in the preceding step. If any modifications are needed click Go Back to go to the previous screen and modify wherever required, and then click Continue.

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

- 6 To close the Registration Wizard, click Finish.

Registering Offline

It is recommended that you register Thirtyseven4 Total Security online as it is easier and faster. However, if your machine is not connected to the Internet, you can register Thirtyseven4 Total Security offline also.

To register offline, you need to visit the offline activation page on the website of Thirtyseven4 <http://173.192.146.76/useract/act2011> and fill in the registration form. Upon completion of the offline registration form, a new key is generated that you have to use to activate your product.

You can register Thirtyseven4 Total Security 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 or is to 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*: It can be obtained from the Activation Wizard in the following ways:
 - i. Go to Application > Thirtyseven4 Total Security.
 - ii. On the Thirtyseven4 Total Security Dashboard, click Register Now. Alternatively, you can go to Menu > Help > Activation.
 - iii. On the Registration Wizard, click Register Offline.

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

You can note down the URL for offline activation and 12-digit Installation Number personally or click *Copy to pasteboard* to copy the information to the machine pasteboard. You may also open a document and directly paste this information into the document.

Generating Activation key for offline activation

To generate activation key, follow these steps:

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

An activation page appears. Click the hyperlink *Click here to proceed to Step 1* on the website under your product type. Ensure that you have the product key and the installation number with you.

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

All asterisk fields are mandatory to fill.

- 4 A new key is generated. Save it for future reference.

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

Activating Thirtyseven4 Total Security with offline activation key

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

- 1 Go to Application > Thirtyseven4 Total Security.
- 2 On the Thirtyseven4 Total Security Dashboard, click Register Now. Alternatively, you can go to Menu > Help > Activation.

- 3 On the Registration Wizard, click Register Offline.

The offline activation screen appears. Click Browse to locate the path where the <license>.key is stored and then click Continue. Your license is activated successfully and the expiry date is displayed.

- 4 To close the Registration Wizard, click Finish.

Re-activation

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

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 machine is protected without any interruption. You can get the renewal code from Thirtyseven4, or from the nearest distributor or reseller.

Renewing Online

To renew your machine online, follow these steps:

- 1 Go to Thirtyseven4 Total Security > Menu > Thirtyseven4 Total Security > About Thirtyseven4 Total Security.
- 2 On the About Thirtyseven4 Total Security screen, click Renew Now.
If your license is about to expire soon or has already expired then the Renew Now button is displayed on Dashboard itself. Click Renew Now to go to the activation page.
- 3 Select *I want to renew with renewal code. I already have renewal code with me* and then click Next.
- 4 On the Registration Information screen, 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 Total Security is renewed successfully.
- 6 To complete the renewal process, click Finish.



In case you do not have the renewal code, select *I do not have renewal code with me. I want to purchase renewal code online* and then click Buy Now.

In case you renewed your license but its expiry date has not extended, select *I have already renewed my license. Please update my license from server* and then 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 Total Security can be renewed offline if your machine is not connected to the Internet.

You need to visit the offline renewal page on the website of Thirtyseven4 at <http://173.192.146.76/useract/renew>. Upon completion of offline renewal process, a new key is generated that you have to use to renew your product on the computer that is not connected to the Internet.

You can renew Thirtyseven4 Total Security offline in the following ways:

- 1 Go to Thirtyseven4 Total Security > Menu > Thirtyseven4 Total Security > About Thirtyseven4 Total Security.

- 2 On the About Thirtyseven4 Total Security screen, click Renew Now.

If your license is about to expire soon or has already expired then the Renew Now button is displayed on Dashboard itself. You can click Renew Now to go the activation page.

The Registration page appears with the message that your system is not connected to the Internet.

- 3 Click Renew Offline to renew the product offline.

The Offline Renewal page appears with license validity date, a webpage link that you have to visit to get the license key file, and the product key, and installation number.

- 4 Visit the offline renewal page at <http://173.192.146.76/useract/renew>.

An activation page appears. Click the hyperlink *Click here to proceed to Step 1*.

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

- 5 Enter the Product Key, Installation Number, Purchased Renewal Code and Purchased From details and then click Submit.

- 6 The renewal confirmation page displays the product key, user name, email address and phone number, and then click Submit.

However, you can change your email address and phone number if required.

- 7 When you receive the license key file, save it and share the file to the machine on which Thirtyseven4 Total Security is installed.

- 8 Click Browse on the Offline Renewal page to select the license key file from the location you have saved, and click Continue.

Your license is renewed successfully.

About Thirtyseven4 Total Security Dashboard

You can access Thirtyseven4 Total Security from the desktop in any of the following ways:

- Click the Thirtyseven4 icon in the menu bar and then select Open Thirtyseven4 Total Security.
- Click the Thirtyseven4 Total Security icon in Dock, if you have added Thirtyseven4 Total Security to the Dock tray.
- In the Doc tray, click Finder and then select Applications under FAVORITES. Click Thirtyseven4 Total Security in the Applications pane to open the application.

Thirtyseven4 Total Security Dashboard


When you open Thirtyseven4 Total Security, Dashboard appears. The Thirtyseven4 Total Security Dashboard is the main area from where you can access all the features. Dashboard is divided into various sections: Thirtyseven4 Total Security menu, system security notification area, Thirtyseven4 Total Security features, news and scan your machine option.

System security notification area indicates whether your system is secured and whether you need to take any action with the help of message and protection icon, while news area displays news about new events such as security alerts, some special release of Thirtyseven4 and so on.

System security notification area provides indication of the security status of Thirtyseven4 Total Security with the help of colored icons. The colored icons and their specific meaning are described as follows:

Icons	Description
Green	Indicates that Thirtyseven4 Total Security is configured with optimal settings and your system is protected.
Orange	Indicates that a feature of Thirtyseven4 Total Security needs your attention, if not immediately, but at the earliest.
Red	Indicates that Thirtyseven4 Total Security 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.

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

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

Thirtyseven4 Total Security Features

Thirtyseven4 Total Security ensures complete protection against any possible threats or malware that may infect your system through various means. Thirtyseven4 Total Security shields your system in the following ways:

Features	Description
Mac Security	Helps you configure scan preferences, virus protection, schedule scan, exclude files and folders from scanning, and set rule for quarantine and files backup.
Web Security	Helps you protect your system against malicious threats when you are browsing the Internet, or when you transfer data across in the network, and parents can control their children's' Internet usage.
Email Security	Helps you protect your system against malicious threats and spams that try to sneak into your system through emails.

The following are frequently used features:

Features	Description
News	Displays the latest information related to security from Thirtyseven4 labs.
Scan	Launches the scanner that scans the machine based on scanning preferences.

Thirtyseven4 Total Security Menus

With the Thirtyseven4 Total Security menus, you can configure the general settings for taking updates automatically, password protect your Thirtyseven4 Total Security so that no unauthorized person can access the Thirtyseven4 Total Security application, provide settings for proxy support and removing reports from the list automatically.

The Thirtyseven4 Total Security menu includes the following:

Menu	Description
Reports	Helps you customize and configure the settings of Thirtyseven4 Anti-Virus such as Automatic Update, Internet Settings, Password Protection, Reports Settings.
Settings	Helps you view the activity reports of Scanner, Virus Protection, Email Protection, Quick Update, Anti-Phishing, Browsing Protection, Parental Control.

Quick Access Options

Quick access options are the options that you use to access Thirtyseven4 Total Security, turn on or off Virus Protection, update the product, and scan the machine when required.

The quick access options include the following:

Options	Description
Open Thirtyseven4 Total Security	Launches Thirtyseven4 Total Security.
Enable / Disable Virus Protection	Helps you turn on or turn off Virus Protection.
Update Now	Helps you update Thirtyseven4 Total Security.
Scan My Mac	Helps you scan your machine for viruses.

News

The News section displays the latest bytes of information and developments from the Thirtyseven4 lab. Whenever there is something new about computer protection, security alert, 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.

Help Topics

The Help topics assist you in understanding Thirtyseven4 Total Security features, how to use them, and seek technical support when required.

To access the desktop integrated Help topics, follow these steps:

- 1 Go to Thirtyseven4 Total Security > Menu > Help > Thirtyseven4 Total Security Help.
The Help topics appear.
- 2 Search for the information that you want.

About Thirtyseven4 Total Security

The About Thirtyseven4 Total Security screen includes the information about the product, license, options for renewing license, updating the product, viewing details of the user license.

To access the About Thirtyseven4 Total Security screen, follow these steps:

- Go to Thirtyseven4 Total Security > Menu > Thirtyseven4 Total Security > About Thirtyseven4 Total Security Help.

The About screen appears.

The About screen includes the following information:

- *Thirtyseven4 Total Security product details:* Product Name, Product Version, Service Pack, Virus Database Date.
- *License Information:* Customer Name, Registered for (individual or organization name), License validity date.
- *View Details:* Includes detailed information on product license, and two buttons—Update License to update your license, and Print License to take out the print of the license information.
- *Print License Details:* Click Print License Details to print the existing subscription information.
- *Renew Now:* Helps you renew your license online.
- *Update Now:* Helps you update your machine with the latest signature.



The License Information and the End-User License Agreement (EULA) are available under this section.

Update License Details: Helps you to synchronize your existing license information with Thirtyseven4 Activation Server. In case you want to renew your existing subscription and you do not know how to renew it or you face problem during renewal, you can call Thirtyseven4 Support team and provide your Product Key and Renewal Code. Thirtyseven4 Support team will renew your copy. You just need to follow these steps:

- Be connected to the Internet.
- Click Update License Details.
- Click Continue to update your existing subscription.

Updating with definition files

If you already have the update definition file with you, you can update Thirtyseven4 Total Security without connecting to the Internet. It is specifically useful for Network environments with more than one machine. You are not required to download the update file from the Internet on all the machines within the network using Thirtyseven4.

- 1 Go to Thirtyseven4 Total Security > Menu > Thirtyseven4 Total Security > Check for Updates....
- 2 On the Welcome to Total Security Update screen, click Continue.
The *Select the mode you prefer for updating Total Security* screen appears.
- 3 Select *Pick from specified location*.
- 4 Type the path or click the File button to the file location, and then click Continue.

Note: Quick Update picks up the definition file from the designated path, verifies its applicability on the installed version and updates your copy of Thirtyseven4 Total Security accordingly.

4

Thirtyseven4 Total Security Features

The Thirtyseven4 Total Security features include the most important features that help you set the scanning preference, protection rules for your machine, scanning schedule, set rules for Quarantine and Backup for files, apply protections for online browsing, set parental control, and block malicious emails and spams.

These features provide optimum protection to your system. Moreover, these features have to be kept enabled all the time. If you disable these features, for any reasons, then the corresponding icons for them will turn red.

Mac Security

The Mac Security option on Dashboard helps you customize the settings that concern the protection of files and folders in your system. With Mac Security, you can set scanning preferences, apply rules for virus protection, schedule scanning, exclude files and folders from being scanned, and set rules for quarantine and backup files.

Mac Security includes the following:

Scan Settings

With Scan Settings, you can customize the way a scan is to be performed and the action that needs to be taken when a virus is detected. However the default settings are optimal and can provide the required protection to your machine.

To configure Scan Settings, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
The Mac Security setting details screen appears.
- 2 Click Scan Settings.
- 3 Set the appropriate option for scan type, action to be taken if virus is found in the files, and whether you want to take the backup of the previous setting.
- 4 Click Save to save your settings.

Select scan type

- *Automatic (Recommended):* Automatic scanning type is the default scanning mode, which is recommended as it ensures optimal protection that your machine requires. This setting is an ideal option for novice users as well.
- *Advanced:* Select Advanced mode if you want to customize the scanning behavior. This is ideal for experienced users only. When you select the Advanced option, the Configure button is enabled and you can configure the Advanced setting for scanning.

Action to be taken when virus is found

Action that you select here will be taken automatically if virus is found, so select an action carefully. The actions and their descriptions are as follows:

Actions	Description
Repair	During scanning if a virus is found, 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 is a Backdoor, Worm, Trojan, or Malware, then Thirtyseven4 Total 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 Type

To configure Advanced Scan type, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
The Mac Security setting details screen appears.
- 2 Click Scan Settings.
- 3 In Scan type, select Advanced.
The Configure button is enabled.

- 4 Click **Configure**.
The Advanced Scan setting details screen appears.
- 5 Check *Items to be scanned* for Windows-based malwares.
By default this option is selected.
- 6 Select one of the following items for scanning:
 - *Scan executable files*: Select this option if you want to scan only the executable files.
 - *Scan all files*: Select this option if you want to scan all types of files. However, it takes time to execute this option and the scanning process slows down considerably.
- 7 Turn *Scan archived files* ON, and then configure the scanning preference for the archive files such as zip files and so on.
- 8 To close the Archive Files screen, click OK. To close the Advanced Scan setting, click OK and then click Save to save your settings.

Scan archive files

If you select *Scan archive files*, then the scanner will also scan archive files such zip files, archive files, and so on. If you select *Scan archive files*, the **Configure** button is enabled and helps you configure the way scanner should treat malicious archive files. You can scan files of various archive file types till five levels down so to ensure no files are left from being scanned.

Following are the actions that you can select to be taken when a virus is found in any of the archive files:

Actions	Description
Quarantine	Select this option if you want to quarantine an archive file that contains a virus.
Delete	Select this option if you want to delete an archive file that contains virus-infected files. However you are not notified if a file is deleted, though its report is generated that you may see in the Reports list.
Skip	Select this option if you want to take no action even if a virus is found in any of the archive files. However this option is selected by default.


Archive Scan level

Set the scan level till which you want to scan the archive files. You can set till five levels down inside the archive files. By default, the scanning is set to level 2. However you can increase the archive scan level which may though affect the scanning speed.

Select archive type to scan

You can select the archive file types that you want to scan from the archive files list. Some of the common archive file types are selected by default. However, you can change your setting as you prefer.

Types	Description
Select All	Select this option to select all the archive file types available in the list.
Deselect All	Select this option to clear all the archive types available in the list.

 When the scan is complete, a summary report appears providing the details about all the actions taken and other scan details, irrespective of the option that you had configured.

Virus Protection

With Virus Protection, you can continuously monitor your machine from viruses, malwares, and other malicious threats. Such threats try to sneak into your machine 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 enabled to keep your machine clean and protected from any potential threats. However, Virus Protection is enabled by default that you can disable if required.

To configure Virus Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
The Mac Security setting details screen appears.
- 2 To protect your machine from malicious threats, turn Virus Protection ON.
- 3 To configure Virus Protection further, click Virus Protection.
- 4 On the Virus Protection screen, do the following:
 - *Items to scan* – Select this checkbox if you want to scan Windows-based malwares. However, this checkbox is selected by default.
 - *Scan network volume* – Select this option if you want to scan network volumes that are mounted on your machine. However, this option is turned on by default.
 - *Display notifications* – Select YES if Display notifications is selected, it displays an alert message whenever a malware is detected. This feature is selected by default.
 - If virus found – Select an action to be taken when virus is found in a file such as Repair, Delete, and Deny Access.
 - 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 backup can be restored from the Quarantine menu.
- 5 To save your setting, click Save.

Action to be taken when virus is detected

Actions	Description
Repair	During scanning 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

Turn Virus Protection OFF. However when you try to turn off Virus Protection, an alert message is displayed. Turning Virus Protection OFF is suggested only when you really require this. Moreover, you can set it off for a certain period of time so that it turns ON automatically thereafter.

Following are the options for turning Virus Protection OFF for a certain period:

- 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, its icon color changes from green to red in Menu Bar Tray, which means that Virus Protection has been disabled temporarily or permanently based on your selection. 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 enable Virus Protection manually.

Schedule Scans

With Schedule Scans, you can define time when to begin scanning of your machine automatically. You can schedule multiple number of scan schedules so that you can initiate scanning of your machine at your convenient time. Frequency can be set for daily and weekly scans, that can additionally refine your request to schedule it to occur at fixed boot at fixed time.

Configuring Schedule Scans

To configure Schedule Scans, follow these steps:

1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.

2 On the Mac Security setting screen, click Schedule Scans.

The Scheduled Scans details screen appears. Here you see a list of all schedules for scanning, if you had defined any before.

3 To create a new schedule for scanning, click Add.

The Add Scheduled Scan screen appears where you can create a new scan schedule name, its frequency, and other details.

4 In the Scan name text box, type a scan schedule name.

5 Set Scan Frequency:

- *Daily*: Select the Daily option if you want to initiate scanning of your machine daily. However this option is selected by default.
- *Weekly*: Select the Weekly option if you want to initiate scanning of your machine on a certain day of the week. When you select the Weekly option, the Weekly list is enabled where you can select a day of the week.

6 Set Scan Time:

- *Start scan at first boot*: Select the *Start scan at First Boot* option to schedule the scanner to scan at 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 irrespective at what time you start the system.
- *Start scan at Fixed Time*: Select the *Start scan at fixed time* option if you want to initiate the scanning of your machine at a certain time. When you select Fixed Time, the Start Time list is enabled where you can fix the time for scanning. However this option is selected by default.

7 Set Scan priority.

- *High*: Select the High option if you want to have the scanning priority at high.
- *Low*: Select the Low option if you want to have the scanning priority at low. However this option is selected by default.

8 Scan location:

- Click Configure to open the Scan location screen, where you can select files and folders for scanning. You can set multiple locations. Select the Drives, folder or multiple folders to be scanned and press OK. You can configure Exclude Subfolder while scanning specific folder. This will ignore scanning inside the subfolders while scanning.

9 Scan settings:

- Click Configure to open the Scan Settings screen. Under Scan Settings, you can specify specific items to be scanned, action required to be taken if a virus is found and use of advance options while scanning. By default setting is set for adequate options for scanning.
- In Scan type, select one of the options from Automatic and Advanced. To know about how to configure scan setting, see [Scan Settings](#), p-23.
- Select YES if you want to have a backup of files before taking any action on them, otherwise select NO if you want no backup of files. This option is selected by default.

10 To save your settings, click Save.

Editing Schedule Scan

You can modify any of the scheduled scans whenever required. To edit a scheduled scan, follow the steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, click Schedule Scans.
A list of all scan schedules appears.
- 3 Select a scan schedule and then click Edit.
- 4 In the Add Schedule Scan screen, change the scan schedule as required.
- 5 To save your settings click Save and then click Close.

Removing Schedule Scan

If you do not require a scan schedule, you can remove it whenever you require. To remove a scan schedule, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, click Schedule Scans.
A list of all scan schedules appears.
- 3 Select a scan schedule, and then click Remove.
- 4 Click YES to confirm if you are sure to remove the scan schedule, and then click Close.

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. This helps you avoid unnecessary repetition of scanning of the files which have already been scanned or you are sure should not be scanned. You can exclude files from scanning from both of the scanning modules Mac Security Scanner and Virus Protection.



Total Security Scanner scans files and folders when you scan manually while Virus Protection scans each file and folder when accessed automatically.

Configuring Exclude Files & Folders

To configure Exclude Files & Folders, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, 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.

- 3 Click Add.
- 4 On the New Exclude Item screen, click the File button or Folder button to add relevant file or folder to the list.
When you add a folder you can check Exclude Subfolders so that the subfolders are also excluded from scanning.
- 5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.
- 6 To close the Exclude Files and Folders screen, click Close.

Editing Exclude Files & Folders

You can change your setting for Exclude Files & Folders if you require so in the following ways:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, 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 that you have added.

- 3 Under Location, select a file or folder, and then click Edit.
- 4 On the New Exclude Item screen, click the File button or Folder button to add another file or folder to the list.
When you add a folder you can check Exclude Subfolders so that the subfolders are also excluded from scanning.
- 5 Select a file or folder, and then click Open to add the selected file or folder and then click Save to save your settings.
- 6 To close the Exclude Files and Folders screen, click Close.

Removing Exclude Files & Folders

You can remove any files or folders that you included in the Exclude Files & Folders list if you require so in the following ways:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, 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 that you have added.

- 3 Under Location, select a file or folder, and then click Remove. You can remove all files and folders from the list by clicking Remove All.

The selected files or folders are removed from the exclusion list.

- 4 To close the Exclude Files and Folders screen, click Close.

Quarantine & Backup

Quarantine & Backup helps in safely isolating the infected or suspected files. When a file is added to Quarantine, Thirtyseven4 Total Security 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 infected file before repairing if the Backup before repairing option is selected in the Scanner Settings.

With Quarantine & Backup, you can also set a rule for removing the files after a certain period of time and having a backup of the files.

Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Mac Security.
- 2 On the Mac Security setting screen, click Quarantine & Backup.
- 3 In Delete files automatically after, drag the slider to select days after which the files should be removed from the Quarantine folder automatically.



Setting this feature helps in removing the quarantine/backup files after the configured period of time. The removal of files is set to 30 days by default.

- 4 Click View Files to see the quarantined files. You can take any of the following actions on the quarantined files:
 - *Add File:* You can add files from folders and drives to be quarantined manually.
 - *Restore Selected:* You can restore the selected files manually if required so.

- *Submit Selected:* You can submit the suspicious files to Thirtyseven4 research lab for further analysis from the Quarantine list. Select the file which you want to submit and then click Submit.
- *Delete Selected:* You can delete the selected files from the quarantine list.
- *Remove All:* You can remove all the Quarantine files from the Quarantine list.
- Submit Quarantine file functionality.

In Quarantine, when you select a file and click the Submit button, a prompt appears requesting permission to provide your email address. You also need to provide a reason for submitting the files. Select one of the following reasons:

- *Suspicious File* – Select this reason if you feel that a particular file in your system has been the cause of suspicious activity in the system.
- *File is un-repairable* – Select this reason if Thirtyseven4 has been able to detect the malicious file on your system during its scans, but has not been able to repair the infection of the file.
- *False positive* – Select this reason if a non-malicious data file that you have been using and are aware of its function, has been detected by Thirtyseven4 as a malicious file.

Web Security

With Web Security, you can set the protection rules to save your machine from malicious files that can sneak into your system during online activities such as banking, shopping, surfing and so on. You can also set parental control to monitor online activities of your children and other users so that you restrict them from accessing any unwanted websites.

Web Security includes the following:

Browsing Protection

With Browsing Protection, you can block malicious websites while browsing so that you do not come in contact with malicious websites and you are secure. However, Browsing Protection is enabled by default.

Configuring Browsing Protection

To configure Browsing Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 Enable Browsing Protection.

You can disable Browsing Protection whenever you prefer.

Phishing Protection

With Phishing Protection, you can prevent access to phishing and fraudulent websites. Phishing is a fraudulent attempt, usually made through email, to steal your personal information. It usually appears to have come from well-known organizations and sites such as banks, companies and services with which you do not even have an account and, ask you to visit their sites telling you to provide your personal information such as credit card number, social security number, account number or password.

Phishing Protection automatically scans all accessed web pages for fraudulent activity protecting you against any phishing attack as you surf the Internet. It also prevents identity theft by blocking phishing websites, so you can do online shopping, banking and website surfing safely.

Configuring Phishing Protection

To configure Phishing Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 Enable Phishing Protection.

You can disable Phishing Protection whenever you prefer. However, you are advised always to keep Phishing Protection enabled.

Parental Control

With Parental Control, the parents can have full control over the Internet activity of their children or other users. Parents can decide which websites their children should visit and which they should not. Using the Parental Control feature, the parents can restrict categories of websites or block specific websites. The parents can also schedule Internet accessibility for their children.

Parental Control is smart enough to categorize all the sites accessed. It has a list of categories of sites that you can allow or deny based on your requirement. This is perfect for parents, who want to ensure that their kids visit the right kind of websites and are not exposed to materials unsuitable for kids.

Important things to do before configuring parental control!

To get utmost benefits from the parental control feature, we recommend you follow a few steps:

Configuring Parental Control

To configure Parental Control, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 On the Web Security setting screen, click Parental Control.

- 3 Configure the following options based on your requirement:
 - *Restrict access to websites based on the category*: When you select this option, you restrict access to all websites under a similar category.
 - *Restrict access to websites as specified by user*: When you select this option, you restrict access to specific websites only.
 - *Schedule Internet access*: This option helps you schedule Internet accessibility for your children or other users.
- 4 To save your settings, click Save.

Restrict access to websites based on category

The Restrict access to websites based on the category feature in Parental Control has a vast range of website categories to allow or deny access to them based on the requirements. Once you restrict or allow a website category, all the websites falling under a category are blocked or allowed. This is helpful if you are sure to restrict or allow all the websites under a category. Moreover, if you want to restrict most of the websites in a category but allow certain websites of that category, which is either required or you rely on, you can do so by excluding such websites in the Exclude list.

To configure access restriction for website categories, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 On the Web Security setting screen, click Parental Control.
- 3 Under Restrict access to websites, switch *Based on the category* to YES to restrict website categories.

The Configure button is enabled.
- 4 Click Configure.
 - A list of website categories whose access can be allowed or denied appears. Click the Allow or Deny button available next to each category that you want to allow or restrict as required. Moreover, the default settings are perfect for novice users and they can retain the default settings for their children.
 - You can also exclude a website from being blocked, despite it being in the blocked category, by adding it to the Exclude list. For example, if you have blocked the Social Networking and Chat category, but you still want to provide access to Facebook, you can do so by enlisting the website in the Exclude list.
 - i. On the Web Category list, click Exclude for excluding the websites.
 - ii. Enter the URL of the website in the list that you want to allow users to access and then click Add.

Similarly if you want to remove a website from the exclusion list, select the URL that you want to remove and click Remove. Click Remove All to delete all the URLs from the exclusion list.
 - iii. To save the changes, click OK.
- 5 Click OK and then click Save to save your settings,.

Restrict access to websites as specified

The Restrict access to websites as specified by user feature in Parental Control helps you block specific websites. This is helpful when you are sure to restrict certain websites and when your list is shorter than it can be in a website category. This is also helpful when a website does not fall in a correct category or you have restricted a website category yet a certain website is accessible that you want to block.

To configure access restriction for specific websites, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 On the Web Security setting screen, click Parental Control.
- 3 Under Restrict access to websites, switch *As specified by user* to YES to restrict specific websites.

The Configure button is enabled.

- 4 Click Configure.

A list for adding websites appears.

- 5 Enter the URL of the website to be blocked and then click Add.

You can add as many websites as you require. Moreover, you can remove any website whenever you require so. Select the websites that you want to remove and click Remove. You can also remove all the websites in the list by clicking Remove All.

- 6 Click OK.
- 7 To save your settings, click Save.

Schedule Internet access

The Schedule Internet access feature in Parental Control helps you schedule Internet accessibility for your children so as you have full control over their browsing time. You can allow your children access to the Internet without any restriction or can schedule the Internet accessibility. You can schedule days and time when your children should access the Internet.

To configure Schedule Internet access, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Web Security.
- 2 On the Web Security setting screen, click Parental Control.
- 3 Switch *Schedule Internet access* to YES to configure Internet accessibility to your children.

The Configure button is enabled.

- 4 Click Configure.

The Schedule Internet Access setting details screen appears.

- 5 Select one of the following:
 - *Always allow access to the Internet:* Select this option if you want to allow access without any restriction to your children.
 - *Allow access to the Internet as per the schedule:* Select this option if you want to schedule Internet accessibility for your children. When you select this option, the routine chart for the days of the week is enabled.
 - Click a cell in the routine chart for a time period of a day. You can select any time period of any day based on your requirement.
 - If you want to schedule a regular period of time for the entire week (like 8:00 AM to 10:00 AM for all days in a week), hover over the time period, or if you want to restrict access to Internet for an entire day (like Sunday) hover over the day, an arrow appears. Click the time period or the day, your restriction applies accordingly. Your children can access the Internet only during the allowed schedule.
- 6 To save your setting, click OK.

Time Specification	Description
Allowed Time	All the cells appearing in green color indicate allowed time frequency for accessing the Internet.
Blocked Time	All the cells not appearing in green color indicate blocked time frequency for accessing the Internet.

Email Security

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 spam, or malware.

Email Security includes the following.

Email Protection


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

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


Configuring Email Protection

To configure Email Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Email Security.
- 2 On the Email Security setting screen, enable Email Protection.
Protection against malwares coming through emails is enabled.
- 3 To configure further, protection rules for emails, click Email Protection.
- 4 Turn *Notify on email* ON if you want an alert message when a virus is detected in an email or attachment.

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

- 5 Select one of the following actions to be taken if virus is found.
 - *Repair*: Select Repair to get your emails or attachment repaired when a virus is found
 - *Delete*: Select Delete to delete the infected emails and attachments.

 If the attachment cannot be repaired then it is deleted.

- 6 Switch *Backup before taking action* to YES if you want to have a backup of the emails before taking an action on them.

You can revert to default settings anytime you require so by clicking Set Defaults.

- 7 To save your settings, click Save.

Spam Protection

With Spam Protection, you can block all unwanted emails such as spam, phishing and porn emails, from reaching into your mailbox. Spam Protection is enabled by default and we recommend you always keep the feature enabled.

Configuring Spam Protection

To configure Spam Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Email Security.
- 2 On the Email Security setting screen, turn Spam Protection ON.
- 3 To configure further protection rules for spam, click Spam Protection.
- 4 Turn *Tag subject with text* ON to include the tag "spam" to the suspicious emails.

- 5 Select one of the following:
 - Turn White List ON if you want to allow emails from the email addresses enlisted in the white list to skip from spam protection filter, and then click Configure to enter the email addresses.
 - Turn Black List ON if you want to filter out emails from the email addresses enlisted in the black list and then click Configure to enter the email addresses.
- 6 Click OK.
- 7 To save your settings, click Save.

Setting spam protection rule for White List

White List is the list of email addresses from which all emails are allowed to skip from spam protection filter irrespective of their content. No emails from the addresses listed here are passed through the SPAM filter. It is suggested that you configure only such email addresses which you rely fully.

To add email addresses in the White List, follow these steps:

- 1 Turn White List ON.
The Configure button is enabled.
- 2 Click Configure.
- 3 Enter the email addresses in the list and click Add.

Edit or Remove Email: To edit an email address, select the email address in the list and click Edit. To remove an email address, select an email address and click Remove.

Import White List: You can import the White List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

Export White List: You can export the White List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.

- 4 To save your settings, click OK.

Setting spam protection rule for Black List

Black List is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -". This feature should be specifically evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.

To add email addresses in the Black List, follow these steps:

- 1 Turn Black List ON.
The Configure button is enabled.
- 2 Click Configure.

- 3 Enter the email addresses in the list and click Add.

Important: While entering an email address, be careful that you do not enter the same email address in the black list that you entered in the white list, else a message appears.

Edit or Remove Email: To edit an email address, select the email address in the list and click Edit. To remove an email address, select an email address and click Remove.

Import Black List: You can import the Black List by clicking Import. This is very helpful if you have a long list of email addresses to enlist.

Export Black List: You can export the Black List by clicking Export. This exports all the email addresses existing in the list. This is helpful if you want to import the same email addresses later. You can simply import the email addresses list.

- 4 To save your settings, click OK.

Adding Domains to White List or Black List

To add specific domain in the White List or Black List, follow these steps:

- 1 Turn White List or Black List On and click Customize.
- 2 Type the domain and click Add. For editing an existing entry, click Edit.
Note: The domain should be in the format: *@mytest.com.
- 3 To save the changes, click OK.

5

Scanning Options

Scan My Mac option on Dashboard provides you with options of scanning your system in various ways so that you can scan as you require. You can initiate scanning of your entire system, drives, network drives, USD drives, folders or files, certain locations (Custom Scan). Although the default settings for manual scan are usually adequate, you can adjust the options for manual scan.

Scan My Mac

Scan My Mac is a complete scanning of your system. With Scan My Mac, you can scan the entire machine, files and folders excluding mapped network drives, folders, and files whenever you think your system needs scanning. However if you keep Virus Protection enabled, you need not run a manual scan. Moreover, the default setting for manual scan is usually adequate, you can adjust the options for manual scan if required.

To initiate Scan My Mac, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click the Scan My Mac list showing at the bottom right.
- 2 On the scan option, click Scan My Mac to initiate complete scanning of your machine. Upon completion of the scan, you can view the scan report under Reports > Scanner Reports.

Custom Scan

With Custom Scan, you can scan specific records, drives, folders, and files on your machine 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 On the Thirtyseven4 Total Security Dashboard, click the Scan My Mac list showing at the bottom right .
- 2 On the scan option, click Custom Scan.
- 3 Click Add to locate the path of the desired folder or drives that you want to scan.

You can select multiple folders for scanning. If you want to remove a file from being scanned, select the file and click Remove. To remove all the files from scan, click Remove All.

- 4 To initiate scanning, click Start Scan.

Upon completion of the scan, you can view the scan report under Reports > Scanner Reports.

6

Thirtyseven4 Total Security Menus

The Thirtyseven4 Total Security menus, available on the top left corner on the Thirtyseven4 Total Security Dashboard, give you instant access to the settings and report topics options irrespective of the feature being accessed.

With the Thirtyseven4 Total Security menus, you can configure general settings to take the updates automatically, password-protect your Thirtyseven4 Total Security settings so unauthorized users cannot access your settings, set proxy support, and schedule removing reports from the report list.

Reports

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

The reports on the following features of Thirtyseven4 Total Security can be viewed:

- Scanner
- Virus Protection
- Email Protection
- Automatic Update
- Browsing Protection
- Phishing Protection
- Parental Control

Viewing Reports

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

- 1 On the Thirtyseven4 Total Security Dashboard, click Reports.
A Reports list appears.
- 2 To view the report of a feature, click the report name. For example, if you want to view the report on Virus Protection, click Virus Protection Reports.

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

Buttons	Actions
Details	Helps you view a detailed report of the selected record.
Delete	Helps you delete the highlighted report in the list.
Delete All	Helps you delete all the reports.
Close	Helps you to exit from the window.

Settings

With Settings, you can configure some of the common settings of Thirtyseven4 Total Security such as you can decide whether you want to take the updates automatically, password-protect your Thirtyseven4 Total Security settings so unauthorized users cannot access your settings, set proxy support, and scheduling the removal of reports from the report list. However, the default settings are optimal and ensure complete security to your system.

Settings includes the following.

Automatic Update

With Automatic Update, Thirtyseven4 Total Security can take the updates automatically to keep your software updated with the latest virus signatures to protect your system from new malwares. To get the updates regularly, your machine on which Thirtyseven4 Total Security is installed needs to be connected to the Internet. It is recommended that you always keep Automatic Update enabled, which is enabled by default.

Configuring Automatic Update

To configure Automatic Update, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Settings.
- 2 On the Settings screen, turn Automatic Update ON and then click Automatic Update.
- 3 On the Automatic Update screen, turn Show notification YES.

By default this feature is enabled. If Show Notification is turned on, you receive a notification each time new updates are received and you get a notification pop-up on Dashbaord.

- 4 Select one of the following:
 - *Download from Internet:* This option helps you download the updates to your machine from Thirtyseven4 server. This option is selected by default.
 - *Pick from specified path:* Select this option if you want to pick the updates from a local folder or a network folder. This is helpful when your machine is not connected to the Internet. After selecting this option, browse the path to pick the updates from the shared location.

- 5 Switch Save update files to YES.

Select this option if you want to save a copy of the updates downloaded to your local folder or network folder. The Browse button is enabled. The Save update files option is enabled when you select Download from Internet.

- 6 Click Browse to specify a folder or network folder to save a copy of the updates downloaded from the Internet.
- 7 To save your settings, click Save.

Password Protection

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

Configuring Password Protection

To configure Password Protection, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Settings.
Password Protection is turned off by default that you can turn on if required.
- 2 On the Settings screen, turn Password Protection ON.
The password protection screen appears.
- 3 Enter password in the New Password text box and then confirm the password by entering it in Retype New Password.
If you are setting the password for the first time, then Existing Password is disabled.
- 4 To reset your password, click Password Protection.
- 5 To save your setting, click Save.

Proxy Support

With Proxy Support, you can enable proxy support, 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 then you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in Internet settings.

However, if you configure Proxy Support, you have to enter your user name and password credentials. The following Thirtyseven4 modules require these changes:

- Registration Wizard
- Mac Security Update
- Messenger
- Web Security (Browser protection, Phishing protection and Parental Control)

Configuring Proxy Support

To configure Proxy Support, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Settings.
- 2 On the Settings screen, click Proxy Support.
- 3 On the Proxy Support screen, turn Proxy support ON to enable proxy support.
The Select proxy type, Enter server, Enter port, and user credentials text boxes are enabled.
- 4 Select the proxy type from HTTP, SOCKS V4, SOCKS V5 based on your preference.
- 5 In the Enter Server text box, enter the IP address of the proxy server or domain name.
- 6 In Enter port text box, enter the port number of the proxy server.
By default port number is set as 80 for HTTP and 1080 for SOCKS V4, SOCKS V5.
- 7 Enter user name and password credentials.
- 8 To save your settings, click Save.

Report Settings

With Report Settings, you can set rules for removing the reports generated on all activities automatically. You can specify the number of days when the reports should be removed from the list. You can also retain all the reports generated 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 On the Thirtyseven4 Total Security Dashboard, click Settings.
- 2 On the Settings screen, click Report Settings.
- 3 On the Report Settings screen, turn *Automatically delete reports* ON to remove reports after the specified number of days. If you want to retain all the reports generated, turn *Automatically delete reports* OFF.
- 4 Select the period from the Delete after list after which you want the reports to be deleted.
- 5 To save your setting, click Save.

7

Updating Software & Cleaning Viruses

The updates for Thirtyseven4 Total Security are released regularly on the website of Thirtyseven4 that contain detection and removal of newly discovered viruses. To prevent your machine from new viruses, you should have the updated copy of Thirtyseven4 Total Security. By default Thirtyseven4 Total Security is set to update automatically from the Internet. This is done without the intervention of the user. However, your machine must be connected to the Internet to get the updates regularly. Automatic updates can also be applied from local or network path, but that path should have the latest set of definitions.

Some important facts about the Thirtyseven4 Total Security updates are:

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

Updating Thirtyseven4 Total Security from Internet

The Update Now feature keeps your copy of Thirtyseven4 Total Security updated automatically through the Internet. However your machine must be connected to the Internet to get the updates regularly. This feature works for all types of Internet connections (Dialup, ISDN, Cable, etc.).

You can also update Thirtyseven4 Total Security manually whenever required so in any of the followings ways:

- Click the Thirtyseven4 Total Security icon in the menu bar, and then select Update Now.
- If the Thirtyseven4 Total Security Dashboard is open, click Update Now which appears if the protection is out of date.
- Open Thirtyseven4 Total Security, and then on the menu bar, go to Thirtyseven4 Total Security > About Thirtyseven4 Total Security. On the About Thirtyseven4 Total Security page, select Update Now.

Update of Thirtyseven4 Total Security is initiated.

Ensure that your machine is connected to the Internet, Total Security Update connects to the Thirtyseven4 Total Security website and downloads the appropriate update files for your software and applies it thereafter to your copy thus updating it to the latest available update file.

Updating Thirtyseven4 Total Security with definition files

If you have the update definition file with you, you can update Thirtyseven4 Total Security without connecting to the Internet. It is useful for Network environments with more than one machine. You are not required to download the update file on all the machines within the network. You can download the latest definition files from the Thirtyseven4 website on one computer and then update all other machines with definition files.

To update Thirtyseven4 Total Security through definition file, follow these steps:

- 1 On the Thirtyseven4 Total Security Dashboard, click Settings.
- 2 Turn Automatic Update ON, and then click Automatic Update.
- 3 Turn Show notification ON to receive notification when updated is needed.
- 4 Check *Pick from specified path*, and then specify the location from where the updates are to be picked up.
- 5 To save your settings, click Save.

Your copy of Thirtyseven4 Total Security is updated from the specified location.

Update Guidelines for Network Environment

Thirtyseven4 Total Security can be configured to provide hassle free updates across the network. You are suggested the following guidelines for best results:

- 1 Setup one computer (may be a server) as the master update machine. Suppose server name is SERVER.
- 2 Make QHUPD folder in any location. For example: QHUPD.
- 3 Assign the Read-Only sharing right to this folder.
- 4 On the Thirtyseven4 Total Security Dashboard, click Settings.
- 5 On the Settings screen, click Automatic Update.
- 6 Switch *Save update files* to Yes.
- 7 Click Browse and locate the QHUPD folder. Click Open.
- 8 To save your setting, click Save.
- 9 On all other computers within the network, launch Thirtyseven4 Total Security.
- 10 Go to the Settings details screen and select Automatic Update.
- 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 To save the settings, click Save .

Cleaning Viruses

Thirtyseven4 warns you of a virus infection when:

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

Cleaning viruses encountered during scanning

Thirtyseven4 Total Security is adequately configured with all the required settings with default installation to protect your machine. If a virus is detected during scanning, Thirtyseven4 Total Security tries to repair the virus. However, if it fails to repair 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:

Options	Description
Status Tab	Displays the status on scanning.
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 you know contains non-suspicious items.
Skip File	Helps you avoid scanning the current file. This option is useful while scanning a large archive of files.
Pause	Helps you pause scanning while scanning is under process. This is a temporary break and you may restart scanning after some time.
Stop	Helps you stop the scanning process. This is a permanent break and you cannot restart scanning from the same instance.
Close	Helps you exit from the scanning process.
Scanning Status	Displays the status of scanning process in percent.
Status Tab	Displays the status on scanning.
Action Tab	Displays the action taken on the files.

Technical Support

Thirtyseven4 provides extensive technical support for its 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.

Support

The Support options provide you a comprehensive support where you can find answers to your queries in a wide variety of ways. The Support options include FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions and concerns, submit your queries, send an email about your queries or call us over telephone.

The 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. Moreover it is advisable that you check with your queries in FAQ at least once before you take use of other support systems as you may get an answer to your question in FAQ itself.

To use Web Support, follow these steps:

- 1 On the Thirtyseven4 Total Security menu bar, go to Help > Support.
- 2 On the Support screen, click Visit FAQ under Web Support to view FAQ or submit your queries.

Check the answer to your queries in FAQ. If you do not find an appropriate answer, then submit your queries to us.

Email Support

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

To use Email Support, follow these steps:

- 1 On the Thirtyseven4 Total Security menu bar, go to Help > Support.
- 2 On the Support screen, click Submit under Email Support to submit your queries.

Clicking on the Submit button redirects you to our Support webpage where you can submit your queries online.

Phone Support

With Phone Support, you can call us for instant support from our Thirtyseven4 technical experts.

The following is the contact number for phone support: [1-877-374-7581](tel:1-877-374-7581).

Live Chat Support

With Live Chat Support, you can log on to the chat room of Thirtyseven4 and ask about your issues that you may be facing. You can get technical support directly from with Thirtyseven4 technical executives.

Support Guidelines

When is the best time to call?

Thirtyseven4, LLC provides technical support between **8:00 AM** and **5:00 PM EST** (Eastern Standard time).

Details that are necessary during the call

- *Product Key:* 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 the Mac computer:* Brand, processor type, RAM capacity, the size of the hard drive and free space on it, as well as information about other peripherals.
- *Operating System:* name, version number, language.
- *Software Version:* Version of the installed anti-virus and the virus database.
- *Software Type:* Software product installed on the machine.
- *Internet Connection:* Is the machine connected to a network? If yes - contact the system administrators first. If the administrators can't solve the problem they should contact the Thirtyseven4 technical support.
- *Other 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 input.

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>.