



Thirtyseven4 Endpoint Security for *Mac*

User Guide

Total
Business

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

Copyright Information

Copyright © 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 Endpoint 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.

Flavors of Thirtyseven4 Endpoint Security Compared

Features	Flavors	
	Business	Total
Virus Protection	✓	✓
Email Protection	✓	✓
Phishing Protection	✓	✓
Browsing Protection	✓	✓
Web Security		✓
Device Control		✓
Spam Protection		✓

Thirtyseven4 Endpoint Security Highlights

Thirtyseven4 Endpoint 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, 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.

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	1
End-User License Agreement	2
About the Document	5
Flavors of Thirtyseven4 Endpoint Security Compared	6
Thirtyseven4 Endpoint Security Highlights	7
Chapter 1. Getting Started	10
Prerequisites	10
System Requirements	10
Installing Thirtyseven4 Endpoint Security	11
Chapter 2. About Thirtyseven4 Endpoint Security Dashboard.....	12
Thirtyseven4 Endpoint Security Dashboard	12
Thirtyseven4 Endpoint Security Features	12
Thirtyseven4 Endpoint Security Menus	13
Quick Access Options	13
News.....	14
Help Topics	14
About Thirtyseven4 Endpoint Security	14
Updating with definition files	14
Chapter 3. Thirtyseven4 Endpoint Security Features	16
Mac Security.....	16
Scan Settings	16
Virus Protection	19
Schedule Scans	20
<i>Configuring Schedule Scans</i>	20
<i>Editing Schedule Scans</i>	21
<i>Removing Schedule Scans</i>	22
Exclude Files & Folders.....	22
<i>Configuring Exclude Files & Folders</i>	22
<i>Editing Exclude Files & Folders</i>	23
<i>Removing Exclude Files & Folders</i>	23
Quarantine & Backup	23
<i>Configuring Quarantine & Backup</i>	24
Web Security	24
Browsing Protection	25

	<i>Configuring Browsing Protection</i>	25
	Phishing Protection.....	25
	<i>Configuring Phishing Protection</i>	25
	Email Security	25
	Email Protection	25
	<i>Configuring Email Protection</i>	26
	Spam Protection	26
	<i>Configuring Spam Protection</i>	26
Chapter 4.	Scanning Options	29
	Scan My Mac.....	29
	Custom Scan.....	29
Chapter 5.	Thirtyseven4 Endpoint Security Menus	30
	Reports.....	30
	Viewing Reports.....	30
	Settings	31
	Automatic Update	31
	<i>Configuring Automatic Update</i>	31
	Password Protection	32
	<i>Configuring Password Protection</i>	32
	Device Control	32
	<i>Configuring Device Control</i>	32
	Proxy Support.....	33
	<i>Configuring Proxy Support</i>	33
	Report Settings.....	33
	<i>Configuring Report Settings</i>	33
Chapter 6.	Updating Software & Cleaning Viruses	35
	Updating Thirtyseven4 Endpoint Security from Internet	35
	Updating Thirtyseven4 Endpoint Security with definition files	36
	Update Guidelines for Network Environment.....	36
	Cleaning Viruses	37
	<i>Cleaning viruses encountered during scanning</i>	37
	<i>Scanning Options</i>	37
Chapter 7.	Technical Support	38
	Support.....	38
	Web Support.....	38
	Email Support	38
	Phone Support	38
	Live Chat Support	39
	Support Guidelines.....	39
	Contact Thirtyseven4, LLC.....	39

Chapter 1. Getting Started

Thirtyseven4 Endpoint 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 Endpoint Security on your Mac 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 Endpoint 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 Endpoint Security must be installed with administrative rights.

System Requirements

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

- Mac OS X 10.6, 10.7, 10.8, 10.9
- Mac Computer with Intel Processor
- 512 MB of RAM
- 1200 MB free hard disk space
- Internet connection to receive updates

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 Endpoint Security

To install Thirtyseven4 Endpoint Security, follow these steps:

Before you install Thirtyseven4 Endpoint Security, you get a Notify Install message from administrator which includes a link to the web page for the installer file.

- 1 Type the link in the browser.

A web page appears that displays the prerequisites for installation and includes a link to the installer file (Download MAC Client). Please read the prerequisites carefully.

- 2 Click through the [Download MAC Client](#) link.

A tar file is downloaded that includes the installer.

- 3 Go to the location where you have saved the tar file and extract all its components.

- 4 Double-click the installer file ([EPSMACCL.dmg](#)).

- 5 Run the Installer to start the Thirtyseven4 Endpoint Security installation.

Thirtyseven4 Endpoint Security is installed successfully.

Note:

- If you are installing Mac client on Mac OSX 10.9 while an FAT USB device is already attached to the machine, such a device will not be displayed as mounted. To show the device mounted, you need to disconnect the device and reconnect it.
- If a USB device is already attached to the machine and you are installing Mac client, the device may not be shown as mounted for a fraction of seconds.
- If an NTFS USB device is attached to the machine during installation of Mac client, two copies of the attached USB may be visible for a few seconds.
- TSEPS server redirection is not supported for the clients that are installed on Mac platform.

Chapter 2. About Thirtyseven4 Endpoint Security Dashboard

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

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

Thirtyseven4 Endpoint Security Dashboard

When you open Thirtyseven4 Endpoint Security, Dashboard appears. The Thirtyseven4 Endpoint Security Dashboard is the main area from where you can access all the features. Dashboard is divided into various sections: Thirtyseven4 Endpoint Security menu, system security notification area, Thirtyseven4 Endpoint 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 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.

Thirtyseven4 Endpoint Security Features

Thirtyseven4 Endpoint Security ensures complete protection against any possible threats or malware that may infect your system through various means. Thirtyseven4 Endpoint 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.

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 Endpoint Security Menus

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

The Thirtyseven4 Endpoint Security menu includes the following:

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

Quick Access Options

Quick access options are the options that you use to access Thirtyseven4 Endpoint 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 Endpoint Security	Launches Thirtyseven4 Endpoint Security.
Enable / Disable Virus Protection	Helps you turn on or turn off Virus Protection.
Update Now	Helps you update Thirtyseven4 Endpoint 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 Endpoint 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 Endpoint Security > Menu > Help > Thirtyseven4 Endpoint Security Help.
The Help topics appear.
- 2 Search for the information that you want.

About Thirtyseven4 Endpoint Security

The About Thirtyseven4 Endpoint Security screen includes the Company information with which Thirtyseven4 Endpoint Security is register.

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

- Go to Thirtyseven4 Endpoint Security > Menu > Thirtyseven4 Endpoint Security > About Thirtyseven4 Endpoint Security Help.
The About screen appears.

The About screen includes the following license information:

- *Thirtyseven4 Endpoint Security License Information:* Organization Name and Virus Database Date.
- *Update Now:* This button helps you update you license .whenever required.

Updating with definition files

If you already have the update definition file with you, you can update Thirtyseven4 Endpoint 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 Endpoint Security > Menu > Thirtyseven4 Endpoint Security > Check for Updates....
- 2 On the Welcome to Endpoint Security Update screen, click Continue.
The *Select the mode you prefer for updating Endpoint 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 Endpoint Security accordingly.

Chapter 3. Thirtyseven4 Endpoint Security Features

The Thirtyseven4 Endpoint 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, Web Security 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 Endpoint 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 Endpoint 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 Endpoint 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.

- 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.
- Notification for the features such as Scan, Update, and Remote Uninstall from TSEPS web console will not be sent to the users if they are not logged on to Mac.

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 Endpoint 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 Endpoint 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-16.
 - 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 Scans

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

- 1 On the Thirtyseven4 Endpoint 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 Scans

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 Endpoint 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.



Endpoint 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 Endpoint 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 Endpoint 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 Endpoint 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 Endpoint 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 Endpoint 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 unrepairable* – 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.

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 Endpoint 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 Endpoint 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.

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 Endpoint 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 Endpoint 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.

Note: *Spam Protection is available only with the Total flavor of Thirtyseven4 Endpoint Security.

Chapter 4. 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 Endpoint 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 Endpoint 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.

Chapter 5. Thirtyseven4 Endpoint Security Menus

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

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

Reports

Thirtyseven4 Endpoint 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 Endpoint Security can be viewed:

- Scanner
- Virus Protection
- Email Protection
- Automatic Update
- Browsing Protection
- Phishing Protection
- Web Security

Viewing Reports

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

- 1 On the Thirtyseven4 Endpoint 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 Endpoint Security such as you can decide whether you want to take the updates automatically, password-protect your Thirtyseven4 Endpoint 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 Endpoint Security can take the updates automatically to keep your software updated with the latest virus signatures to protect your system from new malwares. 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 Endpoint 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 Dashboard.

- 4 Select one of the following:
 - *Download from Internet:* This option helps you download the updates to your machine directly from the Thirtyseven4 server. You may select this option in case your machine is not connected with Endpoint Security Server through LAN.
 - *Download from Endpoint Security Sever:* Select this option if you want to pick the updates from Endpoint Security Server. However you can pick the updates from Endpoint Security Sever if your machine is connected through LAN. 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, nor is your machine available in LAN. 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 Endpoint 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 Endpoint 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.

Device Control

With this feature, the administrators can create policies with varying rights. For example, administrators can block complete access to removable devices, give Read only and no write access so that nothing can be written on the external devices. They can also customize access to the devices configured by the administrators. Once the policy is applied to a group, the access rights are also applied.

The Device Control policies can be configured remotely through Thirtyseven4 Endpoint security console.

Configuring Device Control

To configure Device Control, follow these steps:

- 1 On the Thirtyseven4 Endpoint Security Dashboard, click Settings.
- 2 On the Settings screen, Turn Device Control ON.

However, Device Control is turned off by default.



- If the option 'Read only and No write access' is selected in Device Control of TSEPS and a USB device is attached such a device may not be accessible from the left pane in Finder for some time.
- If a USB device is to be shown as mounted or unmounted using terminal commands, the Device Control policy will not apply to that device.

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 Spam Protection)

Configuring Proxy Support

To configure Proxy Support, follow these steps:

- 1 On the Thirtyseven4 Endpoint 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 Endpoint 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.

Chapter 6. Updating Software & Cleaning Viruses

The updates for Thirtyseven4 Endpoint 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 Endpoint Security. By default Thirtyseven4 Endpoint 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 Endpoint Security updates are:

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

Updating Thirtyseven4 Endpoint Security from Internet

The Update Now feature keeps your copy of Thirtyseven4 Endpoint 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 Endpoint Security manually whenever required so in any of the followings ways:

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

Update of Thirtyseven4 Endpoint Security is initiated.

Ensure that your machine is connected to the Internet, Endpoint Security Update connects to the Thirtyseven4 Endpoint 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 Endpoint Security with definition files

If you have the update definition file with you, you can update Thirtyseven4 Endpoint 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 Endpoint Security through definition file, follow these steps:

- 1 On the Thirtyseven4 Endpoint 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 Endpoint Security is updated from the specified location.

Update Guidelines for Network Environment

Thirtyseven4 Endpoint 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 Endpoint 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 Endpoint 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 Endpoint Security Virus Protection/Email Protection.

Cleaning viruses encountered during scanning

Thirtyseven4 Endpoint Security is adequately configured with all the required settings with default installation to protect your machine. If a virus is detected during scanning, Thirtyseven4 Endpoint 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.

Chapter 7. 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 Endpoint 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 Endpoint 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

- *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, LLC

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>.