



Thirtyseven4 EDR Security

User Guide for Mac

Thirtyseven4, LLC.
www.thirtyseven4.com

Copyright © 2024 Thirtyseven₄, LLC.

All Rights Reserved.

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 transmitted in any form without prior permission of Thirtyseven₄, LLC, P. O. Box 16₄2, Medina, Ohio 44258.

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

Trademarks

Thirtyseven₄ and DNAScan are registered trademarks of Thirtyseven₄, LLC.


Release Date

June 17, 2024

About the Document

This User Guide covers all the information about how to install and use Thirtyseven4 EDR 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 EDR Security Highlights

Thirtyseven4 EDR 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

About the Document	3
Thirtyseven4 EDR Security Highlights	4
Chapter 1. Getting Started.....	8
Prerequisites.....	8
System Requirements.....	8
Installing Thirtyseven4 EDR Security on Mac System.....	9
Installing Thirtyseven4 EDR Security Mac client on macOS Catalina and later.....	10
Permission required to support macOS Catalina and later.....	14
Installing Thirtyseven4 EDR Security on Mac System Remotely	18
Creating Mac client Installer.....	18
Installing using Apple Remote Desktop or Casper	19
<i>Prerequisites.....</i>	<i>19</i>
<i>Installing Mac Client using Apple Remote Desktop or Casper</i>	<i>20</i>
<i>Creating Mac client package</i>	<i>20</i>
<i>Deploying Thirtyseven4 Mac Client using Apple Remote Desktop.....</i>	<i>20</i>
<i>Deploying Thirtyseven4 Mac Client using Casper</i>	<i>21</i>
Connecting remotely using Secure Shell	21
Using Terminal (for Mac or Linux OS).....	21
<i>Prerequisites.....</i>	<i>21</i>
Installing Thirtyseven4 Mac Client.....	22
Using PuTTY (for Windows OS)	23
<i>Prerequisites.....</i>	<i>23</i>
<i>Installing Thirtyseven4 Mac Client.....</i>	<i>24</i>
Chapter 2. About Thirtyseven4 EDR Security Dashboard	26
Thirtyseven4 EDR Security Dashboard.....	26
Thirtyseven4 EDR Security Features	27
Thirtyseven4 EDR Security Menus	27
Quick Access Options	27
Help Topics	28
About Thirtyseven4 EDR Security	28
Updating with definition files	28
Chapter 3. Thirtyseven4 EDR Security Features	30
Mac Security.....	30
Scan Settings.....	30

	Virus Protection	33
	Schedule Scans	34
	<i>Configuring Schedule Scans</i>	34
	<i>Editing Schedule Scans</i>	35
	<i>Removing Schedule Scans</i>	36
	Exclude Files & Folders	36
	<i>Configuring Exclude Files & Folders</i>	36
	<i>Editing Exclude Files & Folders</i>	36
	<i>Removing Exclude Files & Folders</i>	37
	Quarantine & Backup	37
	<i>Configuring Quarantine & Backup</i>	37
	Web Security	38
	Browsing Protection	38
	<i>Configuring Browsing Protection</i>	38
	Phishing Protection	39
	<i>Configuring Phishing Protection</i>	39
	Email Security	39
	Email Protection	39
	<i>Configuring Email Protection</i>	39
	Spam Protection	40
	<i>Configuring Spam Protection</i>	40
Chapter 4.	Scanning Options	43
	Scan My Mac	43
	Custom Scan	43
Chapter 5.	Thirtyseven4 EDR Security Menus	44
	Reports	44
	Viewing Reports	44
	Settings	44
	Automatic Update	45
	<i>Configuring Automatic Update</i>	45
	Self Protection	46
	<i>Configuring Self Protection</i>	46
	Password Protection	46
	<i>Configuring Password Protection</i>	46
	Device Control	46
	<i>Configuring Device Control on Mac Client</i>	47
	Proxy Support	48
	<i>Configuring Proxy Support</i>	48
	Report Settings	49
	<i>Configuring Report Settings</i>	49
Chapter 6.	Updating Software & Cleaning Viruses	50
	Updating Thirtyseven4 EDR Security from Internet	50

	Updating Thirtyseven4 EDR Security with definition files.....	50
	Update Guidelines for Network Environment.....	51
	Cleaning Viruses	51
	<i>Cleaning viruses encountered during scanning</i>	52
	<i>Scanning Options</i>	52
Chapter 7.	Technical Support.....	53
	Accessing support options	53
	Support by Phone	53
	Other sources of support	53
	If the Product Key is Lost	53
	Head Office Contact Details.....	54

Chapter 1. Getting Started

Thirtyseven4 EDR 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 EDR 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 EDR 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 EDR Security must be installed with administrative rights.

System Requirements

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

- Mac OS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13 and 14
- Mac devices with Intel Processor or Apple M1, M2, M3 chip
- Minimum 512 MB of RAM, 2 GB or more is recommended
- 1200 MB free hard disk space

The requirements provided are minimum system requirements. We recommend that your system should have higher configuration 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 EDR Security on Mac System

Before you install the Mac client, create a Mac Client installer on the Thirtyseven4 EDR Server in the following way.

To create a Mac Thirtyseven4 Client installer, follow these steps:

- 1 Log on to the Thirtyseven4 EDR Security.
- 2 Go to Deployment.
- 3 Click the **Create Installer** button to create the Client Installer.
- 4 Enter the **Installer Name** and select **Group**.
- 5 In the **OS platform** list, select Mac.
- 6 A default Validity period of 30 days is selected. You can change it to 60 or 90 days if required.
- 7 A default folder path to install is displayed. Make note of it.
- 8 Click **Create**. The <Installer Name>.TAR file is created.

The installer without an antivirus setup is created and appears in the list on the Deployment > Client Installer page. You can download this installer.

Note

With Standalone Installer, you can create a Mac client installer with an antivirus setup.

Email Install Link

Email Install link allows you to send an email notification to the endpoints in the network to install the Thirtyseven4 EDR Security client.

To notify clients to install the Thirtyseven4 Mac client, follow these steps:

- 1 Log on to the Thirtyseven4 EDR Security.

2 Select Deployment > Email Install link.

The Email Install link screen appears.

3 In the To field, type the email address.

In case of multiple recipients insert a semi-colon (;) between email addresses.

You may modify the subject line of the message if required.

4 Click Send Email.

A Notify Install message containing a link for the installer file is sent from the administrator before installing Thirtyseven4 EDR Security.

5 To install Thirtyseven4 Client on a Mac system, type the installer link in the browser.

The link is sent to you to your email address.

A web page appears that displays the prerequisites for the installation and includes a link to the installer file ([Download Mac Client](#)). Read the prerequisites carefully.

6 Click the Download Mac Client link.

A tar file is downloaded that includes the installer.

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

8 Double-click the installer file ([MCLAGNT.DMG](#)).

9 Run the Installer to start the Thirtyseven4 EDR Security installation.

Note:

-
- Device Control and data Loss Prevention depend upon Virus Protection.
 - Phishing Protection, Browsing Protection, and Web Security may create multiple reports for a single instance if a restricted URL is run on an Opera browser.
 - Notification for Remote Scan, Remote Update, and Remote Un-install from Thirtyseven4 web console cannot be sent if the Mac client user is not logged on to the Mac machine.
-

Installing Thirtyseven4 EDR Security Mac client on macOS Catalina and later

MacOS Catalina and the later versions require approval from the users to run the Installer for EDR Security for Mac when tar file is extracted on the Desktop/Downloads folder.

- 1** While installing the Thirtyseven4 Mac client, a prompt appears to ask permission to access the Desktop/Downloads/Documents folder where the MCCLAGNT.TAR/MCCLAGAV.TAR file is extracted.
- 2** To continue installation, click **OK**.
 - For Users having macOS Catalina, the following system extension prompts will appear one by one when the installation starts. Click **Open Security Preferences** on all the prompts.



Self-protection (ggcext) prompt



Online protection (Opsext) prompt



Data Loss Prevention (dlpext) prompt



File Activity Monitor (famext) prompt

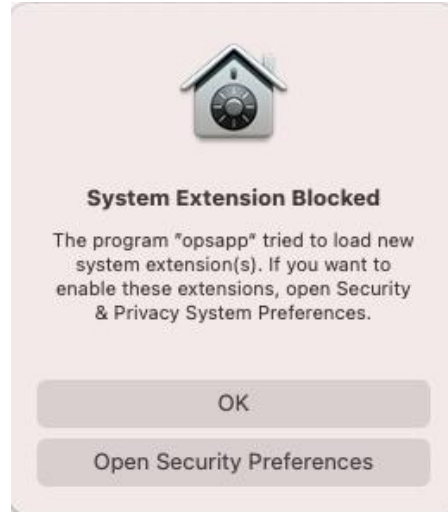


Web Security (webflt) prompt

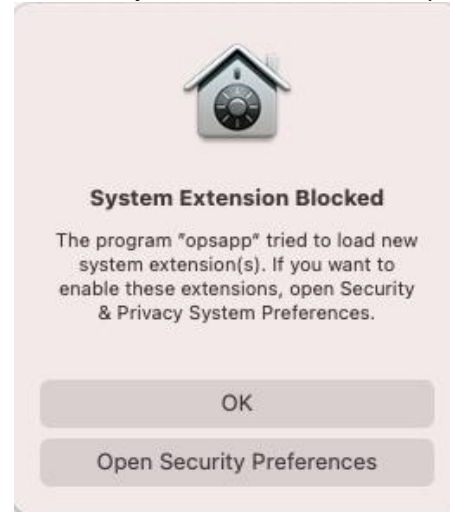


Email Security (mailflt) prompt

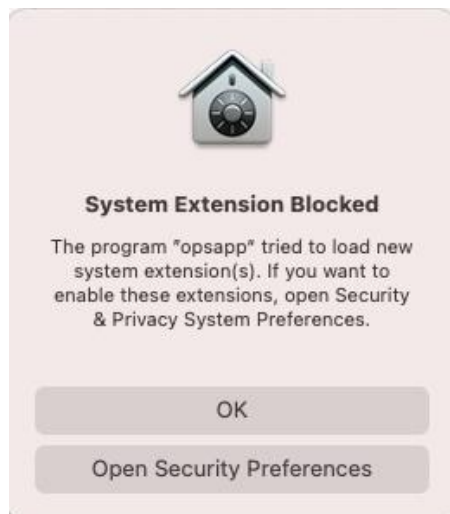
- For Users having macOS Big Sur and later, the following prompts will appear one by one when the installation starts. Click **Open Security Preferences** on all the prompts.



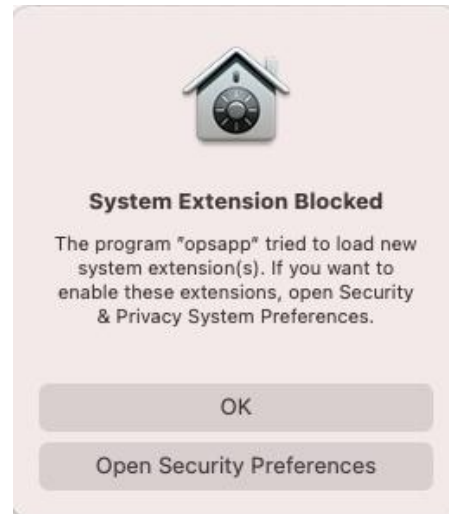
Self-protection (ggcext) prompt



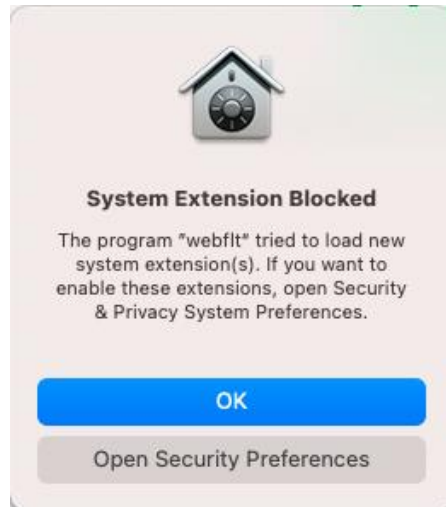
Online protection (Opsext) prompt



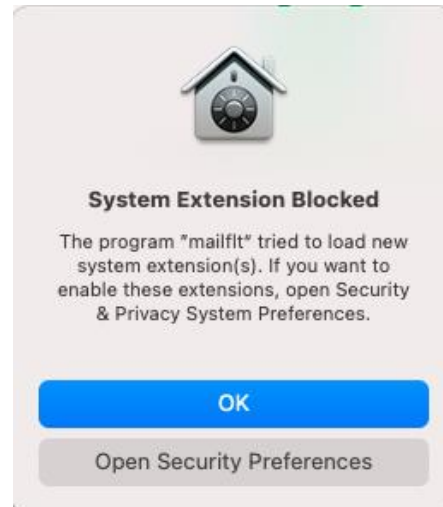
Data Loss Prevention(dlpext) prompt



File Activity Monitor (famext) prompt

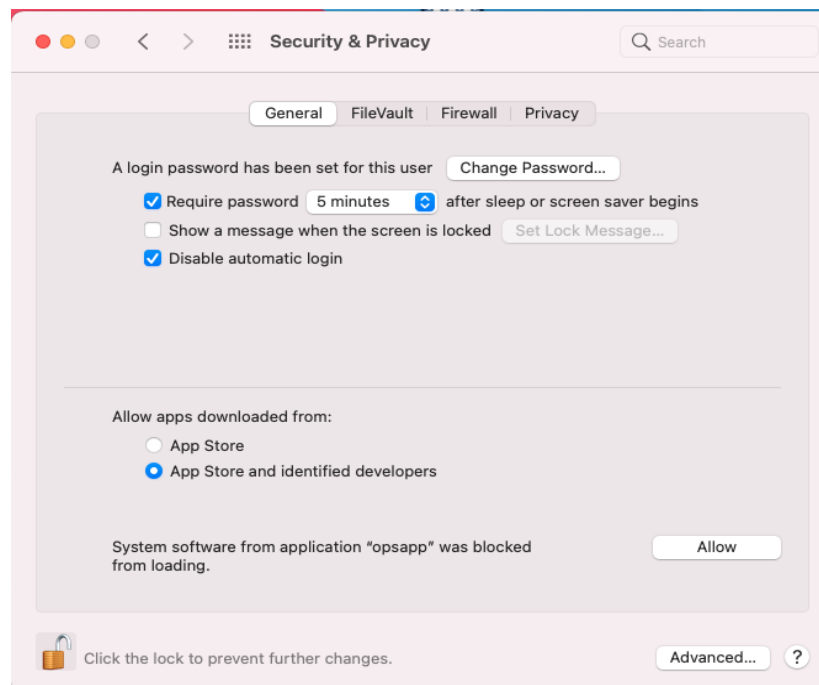


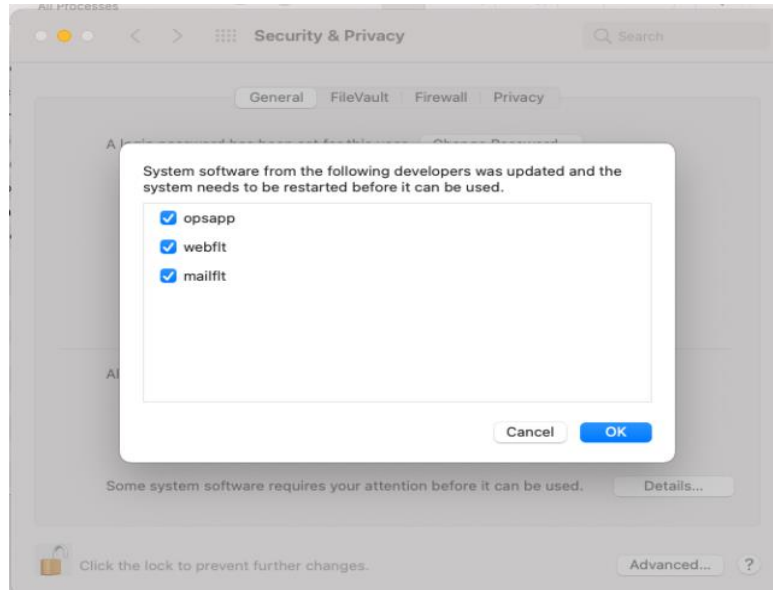
Web Security (webflt) prompt



Email Security (mailflt) prompt

- 3 User needs to **ALLOW** all the above-shown system extension prompts to ensure the following settings on macOS Catalina and later.
 - i. Go to **System Preferences > Security & Privacy**.
 - ii. Click the lock icon and provide the password if it is locked.
 - iii. Click **Allow** as shown in the following screenshot.





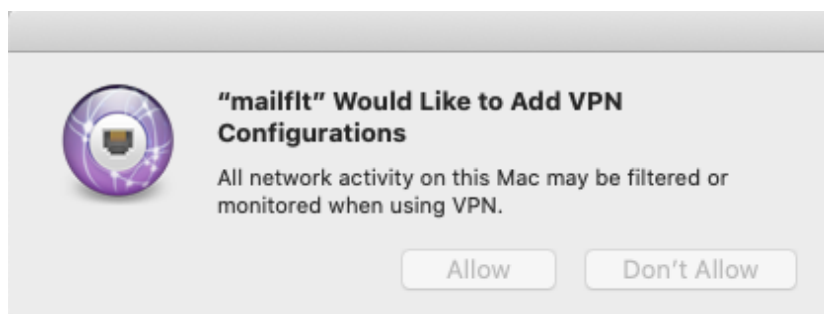
Note: On macOS Catalina “Placeholder Developer” is shown instead of the corresponding app name. Issue is acknowledged by Apple and according to Apple, will be solved in Big Sur. <https://developer.apple.com/forums/thread/130056>

- iv. The list of updated system software appears. Click **Ok**.
- v. Restart your computer.

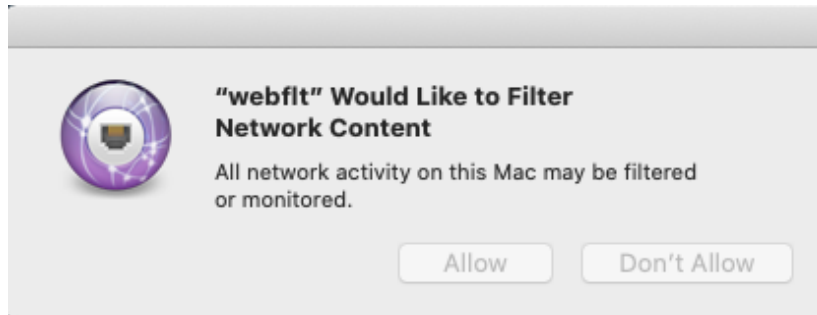
Permission required to support macOS Catalina and later

Product’s [Thirtyseven4] & Services would require permission to access system files on macOS Catalina and later. After Allowing all Apps and Services, system restart is required.

- 1 Post successful installation of Thirtyseven4 EDR Security, the following prompts appear.
 - For Users having macOS Catalina, the following prompts will appear. Click **Allow** on all the prompts.



Email Security VPN configurations

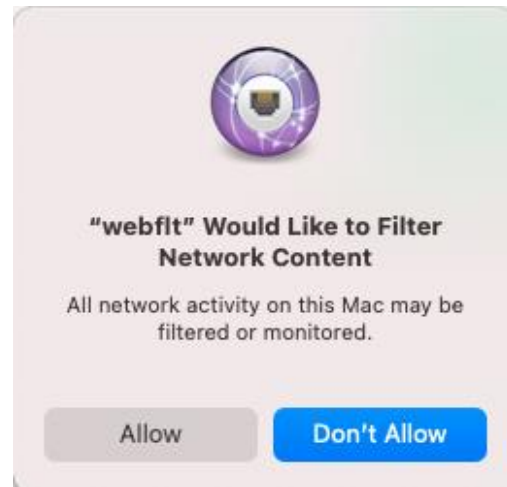


Web Security Network content

- For Users having macOS Big Sur and later, the following prompts will appear. Click **Allow** on all the prompts.

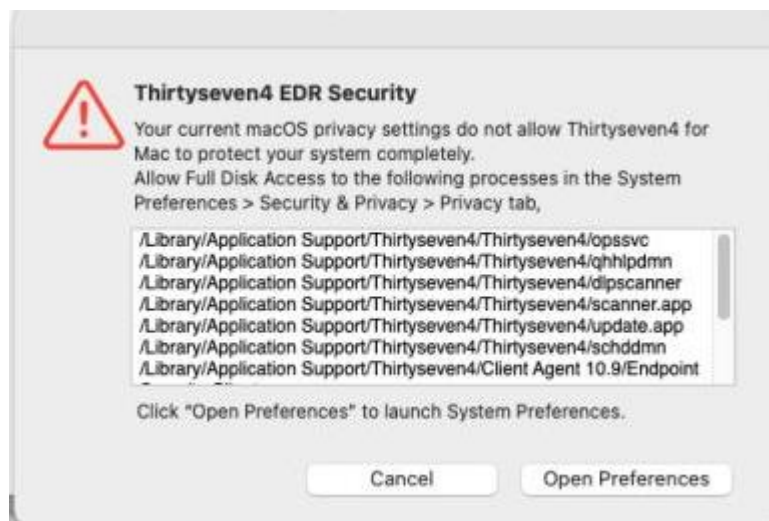


Email Security VPN configurations



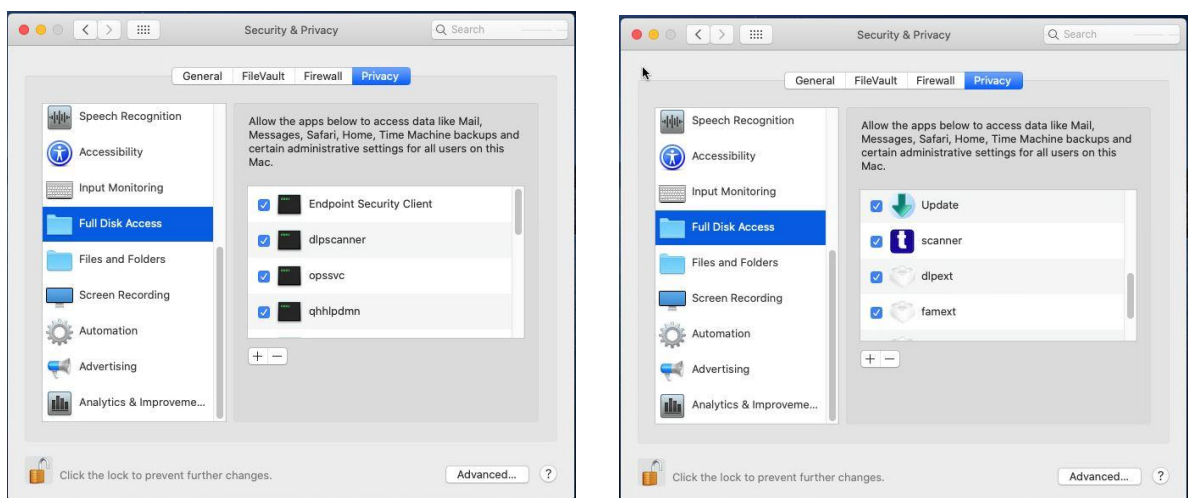
Web Security Network content

- Avprompt prompt message will appear as shown below.



AVprompt message

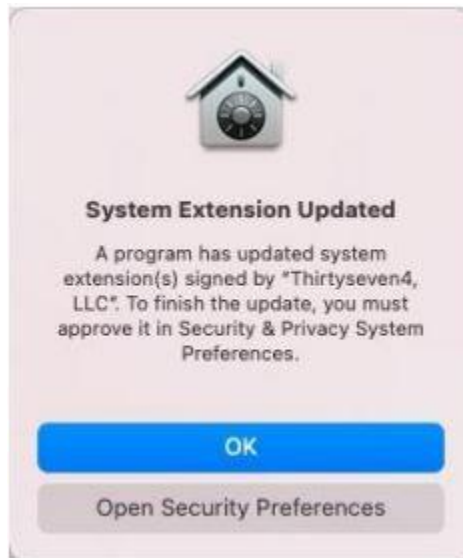
- 3 Do the following settings on macOS.
 - i. Open **System Preferences**.
 - ii. Go to **Security & Privacy > Privacy** tab.
 - iii. Click the lock icon and provide the password if it is locked.
 - iv. Select **Full Disk Access** in the left pane.
- 4 Add the following processes in the given path and then select the processes in the Security & Privacy Full Disk Access window,
 - /Library/Application Support/Thirtyseven4/ Thirtyseven4/opssvc
 - /Library/Application Support/Thirtyseven4/ Thirtyseven4/qhhlpdmn
 - /Library/Application Support/Thirtyseven4/ Thirtyseven4/dlpsscanner
 - /Library/Application Support/Thirtyseven4/ Thirtyseven4/scanner.app
 - /Library/Application Support/Thirtyseven4/ Thirtyseven4/update.app
 - /Library/Application Support/Thirtyseven4/ Client Agent 10.9/Endpoint Security Client
 - /Library/Application Support/Thirtyseven4/Thirtyseven4/schddmn
 - opsext (already present in the privacy section)
 - ggctxt (already present in the privacy section)
 - Dlpext (already present in the privacy section)
 - famext (already present in the privacy section)
- 5 The processes mentioned earlier may be added automatically. In this case, only select the processes in the Security & Privacy > Full Disk Access window.
- 6 The following screenshot will appear showing **Full Disk Access configuration** in System Preferences.



Full Disk Access

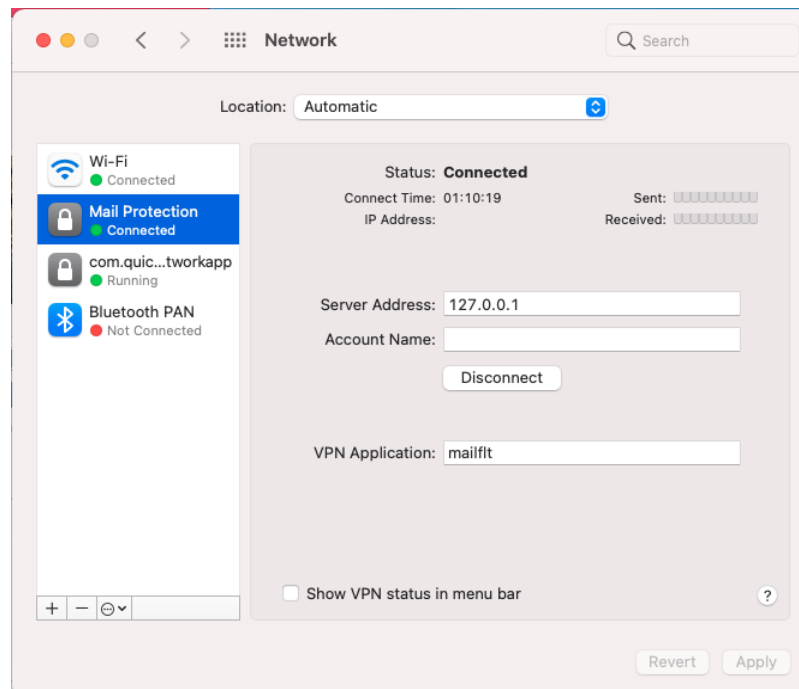
If you install Thirtyseven4 EDR Security Mac client on macOS Catalina for the first time, the following alert prompt appears,

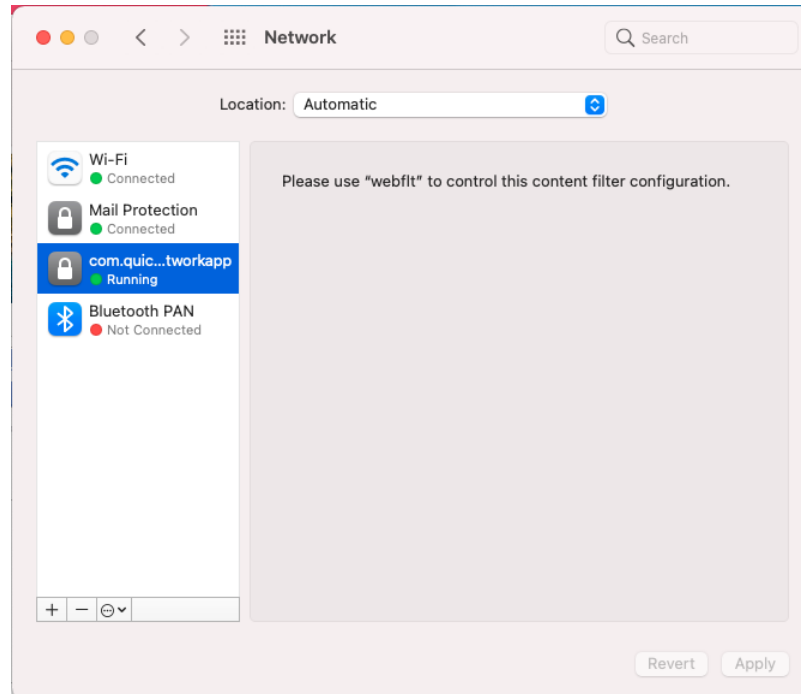
If you install the Thirtyseven4 EDR Security Mac client on macOS Big Sur and later, the following alert prompt appears for 2 times.



Note: The above mentioned prompt does not appear on Apple's M1, M2, M3 chip system.

- 7 To function Thirtyseven4 Thirtyseven4 Mac client on macOS Catalina and later, do the following.
 - i. Click Open Security Preferences.
 - ii. Allow "Thirtyseven4, LLC." from the 'System Preferences >> Security & Privacy'.
- 8 The following screenshot displays mailflt & webflt network extensions connected state in System preferences > Network





Note: Once all the System extensions are allowed and the required permissions are given, then restart your computer.

Please note:

- Device Control, Data Loss Prevention, and File Activity Monitor depend upon Virus Protection.
- Phishing Protection, Browsing Protection, and Web Security may create multiple reports for a single instance if restricted URL is run on Opera browser.
- Notification for Remote Scan, Remote Update, and Remote Un-install from Thirtyseven4 web console cannot be sent if Mac client user is not logged on to the Mac machine.

Installing Thirtyseven4 EDR Security on Mac System Remotely

You can install Thirtyseven4 Mac Client in one of the following ways.

- [Installing using Apple Remote Desktop or Casper](#)
- [Connecting remotely using Secure Shell](#)
 - [Using Terminal \(for Mac and Linux OS\)](#)
 - [Using PuTTY \(for Windows OS\)](#)

Creating Mac client Installer

To create Mac client installer, follow these steps:

- 1 On the Thirtyseven4 EDR Security.
- 2 Go to Deployment, click **Create Installer** button.

The Create Client Installer dialog opens.

- 3 Enter Package Name and Select Group.
- 4 In the OS platform list, select Mac.
- 5 Select validity period in the list box. The validity period can be of 30, 60 or 90 days.
- 6 Click Create.

The <Package Name>.TAR file is created.

The installer without antivirus setup is created and appears in the list on Deployment > Client Installer page. You can download this installer.

Note

With Standalone Installer, you can create Mac client installer with antivirus setup.

Installing using Apple Remote Desktop or Casper

Apple Remote Desktop (ARD) helps you to connect to the Mac client computers remotely in the network, send software to them, install software on them, help other end users in real time, and perform various tasks.

Prerequisites

Before you install Thirtyseven4 Mac Client, ensure the following requirements.

- The administrator computer with ARD or Casper installed must have Mac OS 10.9 and later.
- Mac Thirtyseven4 Client installer must be created on Thirtyseven4 EDR Security . To know about how to create client installer, see [Creating Mac Client Installer](#).
- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Management on the Mac client computers.
- Your administrator computer must have Packages installed on it. Packages is a Mac OS application that helps you to create bundle for your payload and installation. To download Packages, visit <http://s.sudre.free.fr/Software/Packages/about.html>.
- For macOS Catalina and later only, do the following on your Mac system,
 - 1 Open System Preferences.
 - 2 Go to **Security & Privacy > Privacy** tab.
 - 3 Click the **lock** icon and provide password if it is locked.
 - 4 Select **Full Disk Access** in the left pane.
 - 5 Add the following process in the given path and then select the processes in the **Security & Privacy Full Disk Access** window,
`/Library/PrivilegedHelperTools/fr.whitebox.packages/packages_dispatcher`

Installing Mac Client using Apple Remote Desktop or Casper

This procedure helps you install Mac client on the remote Mac client computers using ARD or Casper. For more details, you may refer the documentation of the respective software applications.

Creating Mac client package

- 1 On the Thirtyseven4 EDR Security, download [UEMREMOTEINST.TAR](http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar) from the URL, <http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar>
- 2 Download Mac client builds (with/without AV) from the Thirtyseven4 server. These builds will be in TAR format.
- 3 Rename the Mac client installer as follows:
 - Mac client installer (without AV) - MCCLAGNT.TAR
 - Mac client installer (with AV) - MCCLAGAV.TAR
- 4 Extract [UEMREMOTEINST.TAR](#).
- 5 Copy [MCCLAGNT.TAR](#) or [MCCLAGAV.TAR](#) to "<Download directory>/UEMREMOTEINST".
- 6 Open Terminal.app on the administrator Mac computer and go to the UEMREMOTEINST folder.

- 7 Enter the following commands

```
cd ./Remote_Installation/PKG
sudo sh ./ClientAgentInstaller/CreatePackage.sh
```

Administrator rights are required for executing this command.

When the package creation completes successfully, [ClientAgentInstaller.pkg](#) file is created in the [./Remote_Installation/PKG/ClientAgentInstaller/](#) folder.

If the Client Packager is failed to create on macOS Catalina and later, do the following

- 1 Open System Preferences.
- 2 Go to **Security & Privacy > Privacy** tab.
- 3 Click the **lock** icon and provide password if it is locked.
- 4 Select **Full Disk Access** in the left pane.
- 5 Select the **packages_dispatcher** check box.
- 6 Now again try to create Client Packager, it will be created successfully.

Deployin Thirtyseven4 Mac Client using Apple Remote Desktop

In addition to the [Prerequisites](#) described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 Mac client, ensure that you get Apple Remote Desktop (ARD) tool installed on your administrator computer. To download ARD, visit <https://www.apple.com/in/remotedesktop>.

To deploy Thirtyseven4 Mac client using Apple Remote Desktop, follow these steps:

- 1 Open Apple Remote Desktop.
- 2 Select the Mac client computers from the list of all available computers and then click *Install* to add the package.
- 3 Click the plus (+) sign to locate and add [ClientAgentInstaller.pkg](#) and then click *Install* to begin deployment.

Deployin Thirtyseven4 Mac Client using Casper

In addition to the [Prerequisites](#) described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 Mac client, ensure that you get Casper tool installed on your administrator computer. Casper helps to install software and run scripts remotely on the client computers. To download Casper, visit <http://www.jamfsoftware.com/products/casper-suite/>.

To deploy Thirtyseven4 Mac client using Casper, follow these steps:

- 1 Log on to Casper Admin.
- 2 Drag [ClientAgentInstaller.pkg](#) to the window and then select File > Save.
- 3 Log on to Casper Remote.
- 4 In the Computers tab, select the Mac client computers from the list of available computers.
- 5 In the Packages tab, select [ClientAgentInstaller.pkg](#).
- 6 Click Go.

Connecting remotely using Secure Shell

Secure Shell (SSH) is a network protocol that is used to connect to the remote Mac client computers over secure data communication through command line to manage client computers.

Using Terminal (for Mac or Linux OS)

The administrator computer having either Mac or Linux OS can install client using this method.

Prerequisites

Before you install Thirtyseven4 Mac client, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.

- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac computer under System Preferences > Sharing > Remote Login.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, do the following,
 - 1 In System Preferences, go to **Security and Privacy**.
 - 2 Click the **Lock** icon and provide password if it is locked.
 - 3 Select **Firewall > Firewall Options**.
 - 4 Clear the **Enable stealth mode** check box if it is selected.
 - 5 Click **OK**.
- Mac Thirtyseven4 client installer must be created on the Thirtyseven4 server. To know about how to create client installer, see [Creating Mac Client Installer](#).

Installing Thirtyseven4 Mac Client

To install Thirtyseven4 Mac client using Terminal, follow these steps on the administrator Mac computer:

On the Thirtyseven4 EDR Security, download [UEMREMOTEINST.TAR](#) from the URL,

<http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar>

- 1 Download Mac client builds (with/without AV) from the Thirtyseven4 server. These builds will be in TAR format.
- 2 Rename the Mac client installer as follows:
 Mac client installer (without AV) - MCCLAGNT.TAR
 Mac client installer (with AV) - MCCLAGAV.TAR
- 3 Extract UEMREMOTEINST.TAR.
- 4 Copy [MCCLAGNT.TAR](#) or [MCCLAGAV.TAR](#) to "< Download directory>/UEMREMOTEINST". Download directory is the directory where you have downloaded and extracted UEMREMOTEINST.TAR.
- 5 Open Terminal.app and go to the Remote Installation folder.
- 6 Enter the following command

```
sh ./Scripts/copy.sh <username> <ip_address>
```

Parameter description

[sh ./Scripts/copy.sh](#) is static.

<username> specifies the user name of the remote Mac computer such as 'test'.

<ip_address> specifies the IP address of the remote Mac computer such as '10.10.0.0'.

Example: `sh ./Scripts/copy.sh "test" "10.10.0.0"`

- 7 Enter the password of the remote computer to connect to it.
- 8 Enter the command `sudo sh /tmp/install.sh`.
- 9 Enter the password of the remote computer when prompted.
- 10 A confirmation message appears - "If earlier version of Thirtyseven4 EDR Security client is found on the system, then it will be uninstalled automatically. Do you want to continue?? [Yes/No]:".
- 11 Enter **Yes** or **No**.
 - If you enter **Yes**, installation will proceed.
 - If you enter **No**, installation will be aborted with message "Option No has been selected. Installation aborted."
- 12 Enter the command `exit` to close remote SSH session.
- 13 Repeat steps 6 through 10 to install Thirtyseven4 Mac client on a different remote computer.

Using PuTTY (for Windows OS)

The administrator computer having Windows OS can install Client Agent using this method.

Prerequisites

Before you install Thirtyseven4 Mac client, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac client computer under System Preferences > Sharing > Remote Login.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, do the following,
 - 1 In System Preferences, go to **Security and Privacy**.
 - 2 Click the **Lock** icon and provide password if it is locked.
 - 3 Select **Firewall > Firewall Options**.
 - 4 Clear the **Enable stealth mode** check box if it is selected.

5 Click **OK**.

- Mac Thirtyseven4 client installer must be created on the Thirtyseven4 EDR Security. To know about how to create client installer, see [Creating Mac Client Installer](#).
- If you are using macOS Catalina (10.15) and installing EDR Security for Mac, do the following,

To proceed with installation, macOS Catalina requires your approval to access directory where MCCLAGNT.TAR/MCCLAGAV.TAR file is extracted (Example: Desktop or Downloads or Documents folder). In the System Preferences > Security & Privacy > Privacy > Files and Folders window, select all the options under accaaint to access the directory.

Installing Thirtyseven4 Mac Client

To install Thirtyseven4 Mac client using PuTTY, follow these steps:

On the Thirtyseven4 EDR Security , download [UEMREMOTEINST.TAR](#) from the URL, <http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar>

- 1 Download Mac client builds (with/without AV) from the Thirtyseven4 server. These builds will be in TAR format.
- 2 Rename the Mac client installer as follows:

Mac client installer (without AV) - MCCLAGNT.TAR
Mac client installer (with AV) - MCCLAGAV.TAR
- 3 Extract UEMREMOTEINST.TAR.
- 4 Copy [MCCLAGNT.TAR](#) or [MCCLAGAV.TAR](#) to "<Download directory>/UEMREMOTEINST". Download directory is the directory where you have downloaded and extracted UEMREMOTEINST.TAR.
- 5 Open [cmd.exe](#) and go to the folder "< Download directory>/UEMREMOTEINST".
- 6 Do one of the following:
 - Enter the following command if antivirus is included in the client packager
`.\Remote_Installation\Softwares\pscp.exe .\MCCLAGAV.TAR .\Remote_Installation\Scripts\install.sh <username>@<ip_address>:/tmp/`
 - Enter the following command if antivirus is not included in the client packager
`.\Remote_Installation\Softwares\pscp.exe .\MCCLAGNT.TAR .\Remote_Installation\Scripts\install.sh <username>@<ip_address>:/tmp/`

Note

When MCCLAGAV.TAR as well as MCCLAGNT.TAR files are present, priority is given to the MCCLAGAV.TAR for installing the Thirtyseven4 mac client.

Parameter description

<username> specifies the user name of the remote Mac client computer such as 'test'.

<ip_address> specifies the IP address of the remote Mac client computer such as '10.10.0.0'.

Example: `.\Remote_Installation\Softwares\pscp.exe .\MCCLAGNT.TAR .\Remote_Installation\Scripts\install.sh test@10.10.0.0:/tmp/`.

- 7 Open `.\Remote_Installation\Softwares\putty.exe`.
- 8 Enter the IP address of the remote Mac client computer and click *Open*.
- 9 In the PuTTY terminal Window, enter the user name and password of an administrator user on the remote computer.
- 10 Upon getting connected to the remote computer, type the following command `sudo sh /tmp/install.sh`.
- 11 A confirmation message appears - "If an earlier version of Thirtyseven4 EDR Security client is found on the system, then it will be uninstalled automatically. Do you want to continue?? [Yes/No]:".
- 12 Enter **Yes** or **No**.
 - If you enter **Yes**, installation will proceed.
 - If you enter **No**, installation will be aborted with message "Option No has been selected. Installation aborted."
- 13 Type the command `exit` to close SSH connection.
- 14 Repeat steps 6 through 11 to install on a different Mac client computer.

Note

While installing the Mac client for the first time on Mac OS 10.13, user should allow permission for loading the drivers manually when prompted.

Chapter 2. About Thirtyseven4 EDR Security Dashboard

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

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

Thirtyseven4 EDR Security Dashboard

When you open Thirtyseven4 EDR Security, Dashboard appears. The Thirtyseven4 EDR Security Dashboard is the main area from where you can access all the features. Dashboard is divided into various sections: Thirtyseven4 EDR Security menu, system security notification area, Thirtyseven4 EDR 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 EDR Security with the help of colored icons. The colored icons and their specific meaning are described as follows:

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

Thirtyseven4 EDR Security ensures complete protection against any possible threats or malware that may infect your system through various means. Thirtyseven4 EDR 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
Scan	Launches the scanner that scans the machine based on scanning preferences.

Thirtyseven4 EDR Security Menus

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

The Thirtyseven4 EDR 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, Self 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 EDR 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 EDR Security	Launches Thirtyseven4 EDR Security.
Enable / Disable Virus Protection	Helps you turn on or turn off Virus Protection.
Update Now	Helps you update Thirtyseven4 EDR Security .
Scan My Mac	Helps you scan your machine for viruses.

Help Topics

The Help topics assist you in understanding Thirtyseven4 EDR 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 EDR Security > Menu > Help > Thirtyseven4 EDR Security Help.

The Help topics appear.

- 2 Search for the information that you want.

About Thirtyseven4 EDR Security

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

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

- Go to Thirtyseven4 EDR Security > Menu > Thirtyseven4 EDR Security > About Thirtyseven4 EDR Security .

The About screen appears.

The About screen includes the following license information:

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

Updating with definition files

If you already have the update definition file with you, you can update Thirtyseven4 EDR 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 EDR Security > Menu > Thirtyseven4 EDR Security > Check for Update
- 2 On EDR Security Update screen, click Continue.

Select the mode you prefer for updating the EDR Security screen appears.

- 3 Select the *Pick option from the 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 EDR Security accordingly.

Chapter 3. Thirtyseven4 EDR Security Features

The Thirtyseven4 EDR 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 EDR 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 the 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 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 EDR 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 the Advanced Scan type, follow these steps:

- 1 On the Thirtyseven4 EDR 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 malware.

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 settings, 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 the 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 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 you may see it 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 settings 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 Thirtyseven4 web console will not be sent to the users if they are not logged in to Mac.
- For schedule scan, if the system is shut down at the time of scheduled scan, the scan will not run when the system starts.
- For scheduler policy, if repeat scan is enabled, first scan will run at the scheduled start time + repeat hours.

Virus Protection

With Virus Protection, you can continuously monitor your machine for viruses, malware, 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 EDR 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 check box if you want to scan Windows-based malwares. However, this check box 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 require this. Moreover, you can set it off for a certain period 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 the 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 a 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 the time when to begin scanning your machine automatically. You can schedule multiple scan schedules so that you can initiate scanning of your machine at your convenient time. Frequency can be set for daily and weekly scans, which can additionally refine your request to schedule it to occur at a fixed boot and a fixed time.

Configuring Schedule Scans

To configure Schedule Scans, follow these steps:

- 1 On the Thirtyseven4 EDR 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 you had defined 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 the first boot of the day. When you select Start at first boot,

you do not have to specify the time of the day to start the scan. Scanning takes place only during the first boot 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 folders. 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, actions required to be taken if a virus is found, and use advanced 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 settings, see [Scan Settings](#).
- 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 EDR 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 EDR 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.



Thirtyseven4 EDR 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 EDR Security Dashboard, click Mac Security.
- 2 On the Mac Security settings 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 the 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 EDR 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 EDR 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 help in safely isolating the infected or suspected files. When a file is added to Quarantine, Thirtyseven4 EDR 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 the infected file before repairing if the Backup before Repair option is selected in the Scanner Settings.

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

Configuring Quarantine & Backup

To configure Quarantine & Backup, follow these steps:

- 1 On the Thirtyseven4 EDR 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. 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.
 - *Submit Selected*: You can submit the suspicious files to the 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 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 EDR 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 EDR 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 that are suspicious of spam, or malware.

Email Security includes the following.

Email Protection

With Email Protection, you can enable protection rules for all incoming emails. You can block the infected attachments in the emails that may be suspicious of malware, spam, and viruses. You can also customize the action that needs to be taken when 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 EDR 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 EDR 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 the 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 on which you rely fully.

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

- 1 Turn the 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

The 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 to 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 the specific domain to 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.

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, and certain locations (Custom Scan). Although the default settings for manual scans are usually adequate, you can adjust the options for manual scans.

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 EDR 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 EDR 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 the 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 EDR Security Menus

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

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

Reports

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

The reports on the following features of Thirtyseven4 EDR 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 EDR 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 include the 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 such as you can decide whether you want to take the updates automatically, password-protect your Thirtyseven4 EDR Security settings so unauthorized users cannot access your settings, set proxy support, and schedule the

removal of reports from the report list. However, the default settings are optimal and ensure complete security for your system.

Settings include the following:

Automatic Update

With Automatic Update, Thirtyseven4 EDR Security can take the updates automatically to keep your software updated with the latest virus signatures to protect your system from new malware. 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 EDR 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 the Dashboard.

- 4 Select one of the following:
 - *Download from the Internet*: This option helps you download the updates to your machine directly from the Internet. You may select this option in case your machine is not connected with the EDR Security Server through LAN. This option is selected by default.
 - *Download from Update Agent*: Select this option if you want to pick the updates from the Update Agent.

For the Mac client, to take updates from the Update Agent, the hostname and IP of the Update Agent should be added to the host file on the Mac system.

To add the hostname in the host file, do the following:

- v. Open the Terminal on Mac OS.
 - vi. Enter command `cd /etc`.
 - vii. Enter command `sudo vi hosts`
 - viii. Enter the hostname and IP of the available Update Agents in the host file.
 - ix. Save the host file.
- *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 the 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.

Self Protection

With Self Protection, you can restrict unauthorized users from altering or tampering with the files, folders, configurations, and List entries of Thirtyseven4 EDR Security configured against malware. It is recommended that you always keep self-protection turned on.

Configuring Self Protection

To configure Self Protection, follow these steps:

- 1 On the Thirtyseven4 EDR Security Dashboard, click Settings.
- 2 On the Settings screen, turn Self Protection ON.

However, Self Protection is turned on by default.

Password Protection

With Password Protection, you can restrict all other users from accessing Thirtyseven4 EDR 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 EDR Security Dashboard, click Settings.

Password Protection is turned off by default which you can turn on if required.

- 2 On the Settings screen, turn Password Protection ON.

The password protection screen appears.

- 3 Enter the 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 the 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, and 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, access rights are also applied.

Note

The Device Control feature is not supported on the Apple M1 chip.

The Device Control policies can be configured remotely through the Thirtyseven4 EDR Security console.

Configuring Device Control on Mac Client

To configure Device Control, follow these steps:

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

However, Device Control is turned off by default.

The following are the exceptional conditions

- If the option 'Read only' is selected in Device Control of Thirtyseven4 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.
- The attached CD/DVD will get both read and write permissions even though the read-only setting is applied in the Thirtyseven4 Device Control.
- If any of the iDevices, Webcam, CD/DVD, Internal Card Reader, Mobile Phones, and HFS Encrypted devices are already attached to the endpoint and the Device Control settings are changed, the attached devices need to be re-attached so that the access rights are applied to the new devices.
- Exception functionality is not applicable for Bluetooth, Wi-Fi, Webcam, and External CD/DVD.
- Bluetooth device control is not supported for Monterey Intel.
- Multiple notifications may be generated for CD/DVD.
- Mobile phones except iDevices that are connected in MTP mode, will be detected under the *USB storage devices* category.
 - Mobile Phones connected in MTP mode will be detected under the *Windows Portable Devices* category.
- If you are installing a Mac client with USB devices attached to the system, such devices get unmounted for a few seconds after installation.
- If a USB device with an NTFS file system is attached during Mac client installation, two copies of one attached USB may be visible for a few seconds.
- USB storage device will not be formatted with Mac OS Extended (Journaled, Encrypted) file format.
- Bluetooth blocking functionality does not work on macOS Monterey 12 and later, though the Device Control Blocked prompt appears.

- The 'Authorized Wi-Fi connections' feature is not supported on the Mac operating system. The Advance Device Control feature is not supported on Apple's M1 chip.
- Asset Management: For the Apple_APFS file system, the OS drive will not appear in the Disk storage section of Hardware Details.
- Data Loss Prevention (DLP)
 - If Mac Applications are installed and launched from any location other than the "Applications" folder when DLP is enabled and all file types are monitored for blocking in those applications, the applications won't be launched.
 - DLP block functionality will not work on macOS Catalina 10.15 and later if the attachment is sent through any mail application through the Safari browser.
 - File downloading is getting blocked through the browser if DLP is enabled.

Proxy Support

With Proxy Support, you can enable proxy support, set proxy type, and configure the IP address, and port of the proxy for using an 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 username 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 EDR 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, or 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 the 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, and SOCKS V5.

- 7 Enter the 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 EDR 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 EDR Security are released regularly on the website of Thirtyseven4 and contain the detection and removal of newly discovered viruses. To protect your machine from new viruses, you should have an updated copy. By default, Thirtyseven4 EDR 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 a local or network path, but that path should have the latest set of definitions.

Some important facts about the Thirtyseven4 EDR Security updates are:

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

Updating Thirtyseven4 EDR Security from Internet

The Update Now feature keeps your copy of Thirtyseven4 EDR 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 (dial-up, ISDN, Cable, etc.).

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

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

An update of Thirtyseven4 EDR Security is initiated.

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

If you have the updated definition file with you, you can update it 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 EDR Security through the definition file, follow these steps:

- 1 On the Thirtyseven4 EDR Security Dashboard, click Settings.
- 2 Turn Automatic Update ON, and then click Automatic Update.
- 3 Turn Show notification ON to receive notification when an update is needed.
- 4 Check *Pick from the 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 EDR Security is updated from the specified location.

Update Guidelines for Network Environment

can be configured to provide hassle-free updates across the network. You have suggested the following guidelines for best results:

- 1 Setup one computer (maybe a server) as the master update machine. Suppose the server name is SERVER.
- 2 Make a THIRTYSEVEN4UPD folder in any location. For example THIRTYSEVEN4UPD.
- 3 Assign the Read-Only sharing right to this folder.
- 4 On the Thirtyseven4 EDR 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 THIRTYSEVEN4UPD folder. Click Open.
- 8 To save your setting, click Save.
- 9 On all other computers within the network, launch.
- 10 Go to the Settings details screen and select Automatic Update.
- 11 Select the option *Pick update files from the specified path*.
- 12 Click Browse.
- 13 Locate the SERVER\THIRTYSEVEN4UPD folder from Network Neighborhood. Alternatively, you can type the path as \\SERVER\THIRTYSEVEN4UPD.
- 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 EDR Security Virus Protection/Email Protection.

Cleaning viruses encountered during scanning

Thirtyseven4 EDR Security is adequately configured with all the required settings with default installation to protect your machine. If a virus is detected during scanning, Thirtyseven4 EDR 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 of scanning.
Action Tab	Displays the action taken on the files.
Skip Folder	Helps you avoid scanning the current folder. Scanning moves to other locations. This option is useful while scanning a folder that 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 the scanning process in percent.

Chapter 7. Technical Support

The Support option includes an FAQ where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or call us directly.

Accessing support options

To access the Support options, follow these steps:

1. Log on to the Thirtyseven4 Web console.
2. On the top right of the Thirtyseven4 Dashboard, click the **Support** button.

Support includes the following options:

- **Email Support:** Includes **Submit Ticket** that redirects you to our Support web page. Here you can read some of the most common issues with answers. If you do not find an answer to your issue you submit a ticket.
- **Phone Support:** Includes phone numbers. You can call our support team and get your issues resolved.

Support by Phone

Following is the contact number for phone support: 1-877-374-7581.

To know more phone numbers for support, please visit www.support.thirtyseven4.com

Other sources of support

To get other sources of support, please visit:

www.support.thirtyseven4.com

If the Product Key is Lost

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

Head Office Contact Details

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: www.support.thirtyseven4.com

Web: www.thirtyseven4.com

Sales: sales@thirtyseven4.com