Seqrite Endpoint Security

for Mac

User Guide

SME
Business
Total
Enterprise Suite

http://www.seqrite.com

Copyright Information

Copyright © 2017 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

About the Document

This User Guide covers all the information about how to install and use Seqrite 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.

Seqrite Endpoint Security Highlights

Seqrite 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.seqrite.com.

Contents

Chapter 1. Getting Started

Seqrite 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 Seqrite 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 Seqrite 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.
- Seqrite Endpoint Security must be installed with administrative rights.

System Requirements

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

- Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, 10.11 and 10.12
- Mac Computer with Intel Processor
- 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.seqrite.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 Seqrite Endpoint Security on Mac System

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

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

1. On the Seqrite Endpoint Security server, go to Start > Programs > Seqrite EPS Console 7.2 > Client Packager.
2. In the Client Agent Package list, select Custom.
3. In the OS Platform list, select Mac.
4. In the Antivirus setup included list, select Yes or No depending on whether you want to include antivirus setup in Client Packager.
   - If you include the antivirus setup in the installer package, you cannot distribute the installer through email. However, you can distribute the installer without the antivirus setup through email.
5. Download the Mac Client build from any one of the following URLs:

   http://dlupdate.quickheal.com/builds/seqrite/72/en/mclsetp.zip

   http://download.quickheal.com/builds/seqrite/72/en/mclsetp.zip

   Copy and extract the downloaded build to the

   "Seqrite\Endpoint Security 7.2\Admin\Web\Build." Folder.
6. Click Create.
   - If antivirus is included in the installer package, a MCCLAGAV.TAR file is created in the acmac folder. However, if antivirus is not included in the installer, a MCCLAGNT.TAR file is created in acmac folder.

7 On the Mac endpoint, copy and extract any of the created TAR files (MCCLAGAV.TAR and MCCLAGNT.TAR) and run the MCLAGNT.DMG file from the extracted folder to install Seqrite EPS Mac Client.

When the administrator downloads MCCLAGNT.TAR from the link provided in the email for 'Notify Install', the setup will be downloaded from the ACMAC folder of EPS server.

For roaming endpoints with MAC OS, only Custom client packager can be used for installing EPS client.

Notify Install allows you to send an email notification to the endpoints in the network to install the Seqrite Endpoint Security client.

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

1 Log on to the Seqrite Endpoint Security web console and then select Clients > Client Deployment > Notify Install.

The Notify Install screen appears.

2 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.

3 Click Send Notification.

The default email program on your system opens. Send the mail using the email program.

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

1 To install SEPS 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.

2 Click 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 (MCLAGNT.DMG).

5 Run the Installer to start the Seqrite Endpoint Security installation.

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 SEPS web console cannot be sent if Mac client user is not logged on to the Mac machine.

Installing Seqrite Endpoint Security on Mac System Remotely

You can install Seqrite Mac Client Agent in any 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)

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 Seqrite Mac Client Agent, ensure the following requirements.

- The administrator computer with ARD or Casper installed must have Mac OS 10.6 or later / OS X server.
- Mac Seqrite Client installer must be created on Seqrite Endpoint Security (SEPS) server. To know about how to create client installer, see Installing Seqrite Endpoint Security on Mac System.
- 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.

Creating Client Agent package

To create Client Agent package, follow these steps:

1. On the Seqrite Endpoint Security server, browse to the folder "<installation directory>\Seqrite\Endpoint Security 7.2\Admin\Web\Build".

   <installation directory> indicates the path where Seqrite Endpoint Security has been installed.
2. Copy the folder acmac to the administrator Mac computer.
3. Open Terminal.app on the administrator Mac computer and go to the acmac folder.
4. 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.

Installing Client Agent using Apple Remote Desktop or Casper

This procedure has been provided to help you install Client Agent on the remote Mac client computers using ARD or Casper. For more details, you may consult the documentation of the respective software applications.

Deploying Seqrite Mac Client using Apple Remote Desktop

In addition to the Prerequisites described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Seqrite 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 Seqrite 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.

Deploying Seqrite Mac Client using Casper

In addition to the Prerequisites described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Seqrite 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 Seqrite 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 Agent using this method.

Prerequisites

Before you install Seqrite Mac Client Agent, 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, see the following Apple knowledge base article that applies to your version of the Mac operating system.
  - For 10.8, OS X Mountain Lion: see Prevent others from discovering your computer
  - For 10.9, OS X Mavericks: see Prevent others from discovering your Mac
  - For 10.10, OS X Yosemite: see Prevent others from discovering your Mac
  - For 10.11, OS X El Capitan: see Prevent others from discovering your Mac
  - For 10.12, macOS Sierra: see Prevent others from discovering your Mac
- Mac Seqrite Client installer must be created on the Seqrite Endpoint Security server. To know about how to create client installer, see Installing Seqrite Endpoint Security on Mac System.

Installing Seqrite Mac Client Agent

To install Seqrite Mac Client Agent using Terminal, follow these steps:

1 On the Seqrite Endpoint Security server, browse to the folder "<installation directory>\Seqrite\Endpoint Security 7.2\Admin\Web\Build".

<installation directory> indicates the path where Seqrite Endpoint Security has been installed.

2 Copy the folder acmac to the administrator Mac computer.

3 Open Terminal on the Mac administrator computer and go to the acmac/Remote_Installation folder.

4 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"

5 Enter the password of the remote computer to connect to it.

6 Enter the command `sudo sh /tmp/install.sh`.

7 Enter the password of the remote computer when prompted.

8 Enter the command `exit` to close remote SSH session.

9 Repeat steps 4 through 8 to install Seqrite Mac Client Agent 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 Seqrite Mac Client Agent, 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, see the following Apple knowledge base article that applies to your version of the Mac operating system.
  - For 10.8, OS X Mountain Lion: see Prevent others from discovering your computer
  - For 10.9, OS X Mavericks: see Prevent others from discovering your Mac
  - For 10.10, OS X Yosemite: see Prevent others from discovering your Mac
  - For 10.11, OS X El Capitan: see Prevent others from discovering your Mac

- For 10.12, macOS Sierra: see Prevent others from discovering your Mac

- Mac Seqrite Client installer must be created on the Seqrite Endpoint Security server. To know about how to create client installer, see Installing Seqrite Endpoint Security on Mac System.

Installing Seqrite Mac Client Agent

To install Seqrite Mac Client Agent using PuTTY, follow these steps:

1 On the Seqrite Endpoint Security server, open cmd.exe and go to the folder "<installation directory>\Seqrite\Endpoint Security 7.2\Admin\Web\Build\acmac".

<installation directory> indicates the path where Seqrite Endpoint Security has been installed.

2 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/
```

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/.

3 Open .\Remote_Installation\Softwares\putty.exe.

4 Enter the IP address of the remote Mac client computer and click *Open*.

5 In the PuTTY terminal Window, enter the user name and password of an administrator user on the remote computer.

6 Upon getting connected to the remote computer, type the following command `sudo sh /tmp/install.sh`.

7 Type the command `exit` to close SSH connection.

8 Repeat steps 2 through 7 to install on a different Mac client computer.

Chapter 2. About Seqrite Endpoint Security Dashboard

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

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

Seqrite Endpoint Security Dashboard

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

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

Icons	Description
Green	Indicates that Seqrite Endpoint Security is configured with optimal settings and your system is protected.
Orange	Indicates that a feature of Seqrite Endpoint Security needs your attention, if not immediately, but at the earliest.
Red	Indicates that Seqrite Endpoint 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. Seqrite Protection Center is split into two sections.

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

Seqrite Endpoint Security Features

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

Seqrite Endpoint Security Menus

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

The Seqrite Endpoint Security menu includes the following:

Menu	Description
Settings	Helps you customize and configure the settings of Seqrite 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 Seqrite 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 Seqrite Endpoint Security	Launches Seqrite Endpoint Security.
Enable / Disable Virus Protection	Helps you turn on or turn off Virus Protection.
Update Now	Helps you update Seqrite Endpoint Security.
Scan My Mac	Helps you scan your machine for viruses.
Update from Internet	Helps you take the updates from the Internet. The client computer first tries to take the updates from the Endpoint Security Server. If the server is not reachable, the updates will be automatically taken from the Internet. Keep this option selected when the client is out of network.

News

The News section displays the latest bytes of information and developments from the Seqrite 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 Seqrite 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 Seqrite Endpoint Security > Menu > Help > Seqrite Endpoint Security Help.

   The Help topics appear.

2. Search for the information that you want.

About Seqrite Endpoint Security

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

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

- Go to Seqrite Endpoint Security > Menu > Seqrite Endpoint Security > About Seqrite Endpoint Security.

  The About screen appears.

The About screen includes the following license information:

- *Seqrite 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 Seqrite 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 Seqrite.

1. Go to Seqrite Endpoint Security > Menu > Seqrite 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 Seqrite Endpoint Security accordingly.

Chapter 3. Seqrite Endpoint Security Features

The Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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.

8 To close the Archive Files screen, click OK. To close the Advanced Scan setting, click OK and then click Save to save your settings.

Scan archive files

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

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

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

Archive Scan level

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

Select archive type to scan

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

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

- When the scan is complete, a summary report appears providing the details about all the actions taken and other scan details, irrespective of the option that you had configured.
- Notification for the features such as Scan, Update, and Remote Uninstall from SEPS web console will not be sent to the users if they are not logged in 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 Seqrite 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 Seqrite 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 - 20.
  - 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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, Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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. Seqrite Endpoint Security Menus

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

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

Reports

Seqrite 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 Seqrite 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 Seqrite 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 Seqrite Endpoint Security such as you can decide whether you want to take the updates automatically, password-protect your Seqrite 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, Seqrite 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 Seqrite 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 Dashbaord.
4. Select one of the following:
   - *Download from 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 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.

Self Protection

With Self Protection, you can restrict unauthorized users from altering or tampering the files, folders, configurations, and Plist entries of Seqrite Endpoint 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 Seqrite Endpoint 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 Seqrite 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:

3. On the Seqrite Endpoint Security Dashboard, click Settings.

   Password Protection is turned off by default that you can turn on if required.
4. On the Settings screen, turn Password Protection ON.

   The password protection screen appears.
5. 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.
6. To reset your password, click Password Protection.
7. 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 Seqrite Endpoint Security console.

Configuring Device Control on Mac Client

To configure Device Control, follow these steps:

1. On the Seqrite Endpoint Security Dashboard, click Settings.
2. On the Settings screen, turn Device Control ON.

   However, Device Control is turned off by default.

Following are the exceptional conditions

- If the option 'Read only ' is selected in Device Control of SEPS 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.
- Attached CD/DVD will get both read and write permissions even though the Read only setting is applied in SEPS 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.
- 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 Mac client with USB devices attached to the system, such devices get unmounted for a few seconds after installation.
- If a USB device with NTFS file system is attached during Mac client installation, two copies of one attached USB may be visible for a few seconds.
- If you are installing Mac client on Mac OSX 10.9 with FAT USB devices attached to the system, such devices get unmounted until they are disconnected and reconnected.
- USB storage device will not be formatted with Mac OS extended (Journaled, Encrypted) file format.
- Data Loss Prevention: If Mac Applications are installed and launched from any location other than "Applications" folder when DLP is enabled and all file types are monitored for blocking in those applications, the applications won't be launched.
- If block permission is set to i-devices, then i-devices will not get blocked when connected to the Mac system. This is applicable only for Mac OS 10.12.

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 username and password credentials. The following Seqrite 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 Seqrite 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 Seqrite 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 Seqrite Endpoint Security are released regularly on the website of Seqrite that contain detection and removal of newly discovered viruses. To prevent your machine from new viruses, you should have the updated copy of Seqrite Endpoint Security. By default Seqrite 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 Seqrite Endpoint Security updates are:

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

Updating Seqrite Endpoint Security from Internet

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

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

  Update of Seqrite Endpoint Security is initiated.

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

If you have the update definition file with you, you can update Seqrite 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 Seqrite website on one computer and then update all other machines with definition files.

To update Seqrite Endpoint Security through definition file, follow these steps:

1. On the Seqrite 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 Seqrite Endpoint Security is updated from the specified location.

Update Guidelines for Network Environment

Seqrite 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 SEQRITEUPD folder in any location. For example: SEQRITEUPD .
3. Assign the Read-Only sharing right to this folder.
4. On the Seqrite 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 SEQRITEUPD folder. Click Open.
8. To save your setting, click Save.
9. On all other computers within the network, launch Seqrite 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\SEQRITEUPD folder from Network Neighborhood. Alternatively, you can type the path as \\SERVER\SEQRITEUPD.
14. To save the settings, click Save.

Cleaning Viruses

Seqrite warns you of a virus infection when:

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

Cleaning viruses encountered during scanning

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

Seqrite 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 support executives of Seqrite.

The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, send emails about your queries, or call us directly.

To see the support options, follow these steps:

1. Open Seqrite Endpoint Security.
2. On the Seqrite Endpoint Security menu bar, go to Help > Support.

Support includes the following options.

Phone support: Helps you call our support team to get your issues resolved.

Contact number for phone support: 1800 212 7377

Submit a Query (Email Support): Helps you send us your query. We will revert with an appropriate answer soon.

Chat With Us (Live chat support): Helps you chat with our support executives to get your issues resolved instantly.

Locate Dealer: Helps you locate a dealer nearest to your location.

Product FAQs: Includes FAQs (Frequently Asked Questions) where you can read answer to the most common queries.

Other Sources of Support

To get other sources of support, visit: http://www.seqrite.com/contact_support.

For support in specific country, , visit: http://www.seqrite.com/int_techsupp.

Head Office Contact Details

Quick Heal Technologies Limited

(Formerly Known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor,

Viman Nagar, Pune 411014.

Telephone: +91 20 66813232

Official Website: http://www.seqrite.com

Email: support@seqrite.com