



Seqrite Endpoint Security 7.6

Administrator's Guide

SEPS SME
SEPS Business
SEPS Total
SEPS Enterprise Suite

<http://www.seqrite.com/>

Copyright Information

Copyright © 2008–2021 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. while Microsoft and Windows are registered trademarks of Microsoft Corporation. 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.

Document Update Date

January 6, 2022


About This Document

Document History

Version	Change date	By Whom	Action
1.1	October 2020	QA and Technical Writer	EPS 7.6 released
1.2	June 2021	QA and Technical Writer	EPS 7.6 Service Pack 5.0 released
1.3	November 2021	QA and Technical Writer	EPS 7.6 Updated Build released

Document Convention

This user guide covers all the information required to install and use Seqrite Endpoint Security on Windows operating systems. The following table lists the conventions that we have followed to prepare this guide.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down menu, dialog, button names, hyperlinks, and so on.
	This is a symbol used for a note. Note supplements important points or highlights information related to the topic being discussed.

Contents

1. Introducing Seqrite Endpoint Security	1
How Does Seqrite Endpoint Security Work?	1
Why Seqrite Endpoint Security?	2
New in this release.....	3
Available flavors.....	6
License Subscription	7
Certifications	7
Network Deployment Scenarios	7
Scenario 1.....	8
<i>Network Setup Description</i>	8
Seqrite Recommendation	8
Scenario 2.....	8
<i>Network Setup Description</i>	8
Scenario 3.....	9
Network Setup Description.....	9
Seqrite Recommendation	10
2. Getting Started	11
Prerequisites	11
System requirements for SEPS server.....	11
General requirements.....	11
Operating system requirements	12
Additional software required for SEPS server	13
Java Runtime Environment (JRE) Requirements	13
System requirements for Seqrite EPS clients	13
General requirements.....	14
Operating system requirements	14
System requirements for Mac OS.....	15
System requirements for Linux OS	15
Installing Seqrite Endpoint Security server on Windows Operating System.....	16
Installing Multiple Seqrite Endpoint Security Servers	22
Upgrading Seqrite Endpoint Security to the latest version	22
Best cyber security practices for Enterprises to stay cyber secure	23
3. Post Installation Tasks.....	26

Registration	26
Registering Online	26
Internet Settings	27
Reactivation	27
Reactivating Seqrite Endpoint Security	27
Disabling remote access	28
Configuring Update Manager	28
Accessing Update Manager	28
<i>Features of Update Manager</i>	28
<i>Status</i>	28
<i>Configuration</i>	28
<i>Schedule Scan in Update Manager</i>	30
<i>Connection Settings</i>	30
<i>Reports</i>	31
Configuring ports on the Azure or AWS Cloud machine	32
Uninstalling Seqrite Endpoint Security server	32
4. About Seqrite Endpoint Security Dashboard	33
Log on the Seqrite Endpoint Security Web console	33
Resetting the Web console password	34
<i>Resetting the Web console password with Forgot Password link</i>	34
<i>Resetting the Web console password with Password Reset tool</i>	34
Areas on the Web console	35
Ribbon	36
Dashboard	37
<i>Overview</i>	37
<i>Network Health</i>	39
<i>Status</i>	39
<i>Security</i>	40
<i>Compliance</i>	41
<i>Assets</i>	41
<i>CTA Banner - GoDeep.AI</i>	41
Consolidated Dashboard	42
<i>Virus Incidents</i>	42
<i>License Allocation Summary</i>	43
<i>Status</i>	43
<i>Security</i>	44
Manage Secondary Servers	44
5. Clients	49

Client Status tab	49
Client Action tab	50
Scan	51
<i>Scan Settings</i>	51
Update.....	53
Tuneup	54
<i>Tuneup Settings</i>	55
Application Control Scan.....	55
<i>Scan Settings</i>	56
Vulnerability Scan	57
Data-At-Rest Scan	57
<i>Scan Settings</i>	58
Patch Scan	59
Patch Install.....	60
Temporary Device Access	63
Delete Backup Data.....	63
<i>Delete Settings</i>	64
6. Client Deployment	65
Through Active Directory	65
Synchronizing with Active Directory	66
Editing Synchronization	67
<i>Removing Synchronization</i>	68
<i>Exclusion</i>	68
Remote Install	68
Exception Rules	69
Viewing installation status	71
Notify Install.....	72
Client Packager.....	73
Creating the Windows Seqrite Client Packager	73
Creating the Mac Seqrite Client Packager	75
Creating the Linux Seqrite Client Packager.....	75
<i>To install the Client Agent:</i>	76
Sending the package through email	77
<i>Sending a minimal Client Packager</i>	77
<i>Sending a custom Client Packager</i>	77
Login Script.....	78

Installing Login Script	78
Opening Login Script Setup	78
Assigning Login Script	78
Installing Seqrite Endpoint Security on Mac Operating Endpoints	79
Remote Installation of Seqrite Endpoint Security on Mac System	80
Remote installation using Apple Remote Desktop or Casper	80
<i>Creating Client Agent package</i>	81
<i>Installing Client Agent using Apple Remote Desktop or Casper</i>	81
Connecting remotely using Secure Shell	82
<i>Using Terminal (for Mac or Linux OS)</i>	82
<i>Using PuTTY (for Windows OS)</i>	84
<i>Installing Seqrite Mac Client Agent</i>	84
Creating the Mac Seqrite client installer	85
Installing client on Linux-based Endpoints	86
Disk Imaging	87
Firewall Exception Rules	88
Remote Uninstall	88
Stop Uninstallation Notifications	89
7. Manage Groups	90
Adding a Group	90
Adding a Subgroup	91
Deleting a Group	91
Renaming a Group	91
Importing from Active Directory	92
Setting Policy to a Group	92
Assigning Group Administrator	93
Unassigning Group Administrator	93
Changing Group of an Endpoint	94
Exporting groups and policies	94
Importing groups and policies	95
8. Manage Policies	96
Understanding Security Policy Scenario	96
Creating Policies	98
Creating a new policy	98
Copying a policy	99
Renaming a policy	99

Deleting a policy.....	99
Importing and Exporting Policies	100
<i>Exporting a policy</i>	100
<i>Importing a policy</i>	100
Policy Fetch Utility	101
9. Assets	102
Enabling Asset Management	102
Viewing the details for Endpoints	102
Downloading Complete Asset Details Report.....	104
10. Settings.....	105
Client Settings	105
Scan Settings	105
<i>Scanner Settings</i>	106
<i>Virus Protection Settings</i>	107
<i>Advanced DNAScan Settings</i>	108
<i>Block suspicious packed files</i>	109
<i>Automatic Rogueware Scan Settings</i>	109
<i>Disconnect Infected Endpoints from the network</i>	109
<i>Exclude Files and Folders</i>	109
<i>Exclude Extensions</i>	111
Email Settings.....	111
<i>Email Protection</i>	111
<i>Configuring Email Clients</i>	112
<i>Trusted Email Clients Protection</i>	113
<i>Spam Protection</i>	114
External Drives Settings	116
<i>External Drives Settings</i>	116
<i>Autorun Protection Settings</i>	117
<i>Mobile Scan Settings</i>	117
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	117
Firewall.....	119
<i>Managing the Exceptions rule</i>	121
Web Security	125
<i>Browsing Protection Settings</i>	127
<i>Phishing Protection Settings</i>	127
<i>Web Categories</i>	128
Application Control	130
Advanced Device Control.....	132

<i>Creating policy for Advanced Device Control</i>	132
<i>Adding exceptions to the device control list</i>	135
<i>Adding Device to Server</i>	136
Data Loss Prevention	136
<i>Add-on Features</i>	137
<i>Preventing leakage of data</i>	139
File Activity Monitor.....	141
<i>Enabling File Activity Monitor</i>	141
Update Settings.....	142
Internet Settings	143
Patch Server	144
General Settings.....	144
Schedule Settings	147
Client Scan.....	147
<i>Client Schedule Scan</i>	147
<i>Scanner Settings</i>	148
<i>Antimalware Scan Settings</i>	149
<i>Boot Time Scan Settings</i>	149
Application Control	149
<i>Application Control Schedule Scan</i>	150
<i>Scan and Report</i>	150
<i>Tuneup</i>	150
<i>Tuneup Schedule Scan</i>	150
<i>Tuneup Settings</i>	151
Vulnerability Scan	151
<i>Scheduling Vulnerability Scan</i>	151
<i>Scan and Report</i>	152
Data-At-Rest Scan	152
Patch Scan	153
11. Reports	155
Client	155
Viewing Reports of Virus Scan	155
Viewing Reports of Unscanned Endpoints.....	156
Viewing Reports of AntiMalware Scan	157
Viewing Reports of Web Security	157
Viewing Reports of Tuneup.....	158
Viewing Reports of Advanced Device Control	159
Viewing Reports for Data Loss Prevention (DLP).....	160

<i>On Access Scan</i>	160
<i>On Demand/Schedule Scan</i>	161
Viewing Reports for Application Control	162
Viewing Reports of IDS/IPS	164
Viewing Reports of Firewall	166
<i>Viewing Reports of Wi-Fi</i>	167
Viewing Reports of Vulnerability Scan.....	167
Viewing Reports for File Activity Monitor	168
<i>Viewing reports for file activity</i>	169
Viewing Reports for Asset Management	170
<i>Viewing reports for asset management</i>	170
Viewing Reports of Patch Management	171
Viewing Reports of Backup Data.....	173
Server	174
Manage	174
Settings.....	174
Export.....	175
Delete Reports	175
12.Admin Settings.....	177
Server	177
Change Password	177
Change Email Address.....	177
Notification	178
<i>Email & SMS Notification</i>	178
<i>Buy Now</i>	180
SMTP Settings	181
Manage Devices	182
<i>Cleaning USB device</i>	182
<i>Adding device where EPS client is installed/ not installed</i>	183
<i>Adding device in the dcconfig tool through Admin folder</i>	184
<i>Adding exceptions to the device control policy</i>	185
Data Loss Prevention	186
<i>User Defined Dictionary</i>	187
<i>Domain Exceptions</i>	188
<i>Custom Extensions</i>	189
<i>Applications</i>	190
<i>Network share Exception</i>	192
Redirection.....	193

Manage Users	195
<i>Creating New Users</i>	196
<i>Modifying Existing Users</i>	196
<i>Deleting Users</i>	197
Internet Settings	197
Patch Management.....	197
<i>Installing Patch Server</i>	198
<i>Adding New Patch Server</i>	198
<i>Removing Patch Server</i>	199
<i>Configuring Patch Server</i>	199
<i>Upgrading Windows 10 to latest version through Seqrite Patch Management</i>	202
General.....	203
<i>Multiserver Migration Period</i>	203
Clients.....	204
Client Installation	204
Inactive Client Settings.....	204
Asset Management	205
Roaming Clients	205
<i>Reinstallation</i>	206
Data Loss Prevention (DLP)	207
<i>Enabling DLP feature</i>	207
13. Update Manager	209
Viewing Update Manager Status	209
Update Manager Settings	210
<i>Update Manager Schedule</i>	210
Alternate Update Managers	211
<i>Recommendation</i>	211
<i>Adding New Alternate Update Manager</i>	211
<i>Viewing details of Alternate Update Managers</i>	212
<i>Modifying Existing Alternate Update Manager details</i>	213
<i>Alternate Update Manager Schedule</i>	214
<i>Deleting Alternate Update Manager</i>	214
14. License Manager	216
Status	216
Update License Information	217
View license history	217
License Order Form.....	217
Renew my license	218

Add license for new endpoints	219
Buy additional feature	219
Edition Upgrade	220
Upgradation to Higher Version	220
15. Patch Management.....	221
Workflow of Patch Management	221
System requirements for Patch Management server	221
Installing Patch Management server	222
Back up the patch server data	224
Offline Patch Synchronizer.....	224
Patch Server Control Panel	225
Uninstalling patch server	225
16. SyslogAgent Tool – SIEM Integration.....	226
Workflow of SyslogAgent tool	226
Installing SyslogAgent Tool	227
Using SyslogAgent tool	227
Updating Configuration	227
Uninstalling SyslogAgent Tool.....	228
17. Technical Support	229
Support by Phone	229
Other sources of support.....	230
If the Product Key is Lost	230
Head Office Contact Details	230

Introducing Seqrite Endpoint Security

For every organization, security of valuable data and resources is of paramount concern. Today, Web technology is an integral part of business processes for all organizations. This puts them more at risk from new and unknown threats and attacks. Seqrite Endpoint Security (SEPS) is a software that provides a complete security solution to small and enterprise-level networks against various kinds of malicious threats such as; viruses, Trojans, worms, backdoors, spyware, riskware, adult content, and hackers.

Seqrite Endpoint Security is a Web-based management application that integrates and provides protection for desktops, laptops, and network servers. It allows you to access all clients and servers in the network and manage them remotely. You can deploy antivirus software applications, configure security policies, signature pattern updates, and software updates on the clients and servers. You can also monitor clients to check whether there are any policy breaches or security threats within the organization and take appropriate actions for ensuring security across the networks.

How Does Seqrite Endpoint Security Work?

Seqrite Endpoint Security (SEPS) works on the Client/Server architecture where the console manages all the client agents deployed on the network. The console and client agents can be installed on almost all flavors of Microsoft Windows operating systems. The client agents can also be installed on the machines with Linux and Mac operating systems. For a detailed description of console and client agent system requirements and compatibilities, see [System Requirements](#).

SEPS helps the administrators deploy Seqrite Antivirus remotely on the specified computers, groups or domains, which are part of the same domain. Whenever the server copy of Seqrite Antivirus is updated, all computers configured to update from the server will be automatically updated without user intervention. SEPS monitors these processes so that an administrator can view the computers that have Seqrite Antivirus installed, the virus database date of Seqrite, whether Virus Protection is enabled, and if viruses are active in the memory of workstations. If any virus is found active in the memory of a workstation, that workstation gets disconnected from the network. If it detects that Seqrite is uninstalled from any workstation(s), it reinstalls Seqrite remotely without user intervention. This keeps the computers and the network safe from virus threats.

Why Seqrite Endpoint Security?

- **Comprehensive Endpoint Security and Control**
Seqrite Endpoint Security is a simple yet powerful platform to manage security and helps to enforce control over data, application, web access with a wide range of features such as Advanced Device Control, DLP, Asset Management, Application Control, etc.
- **Multilayered Protection**
Seqrite Endpoint Security is certified by various industry certifications and integrates innovative technologies like Advanced DNA Scan, Behavior Detection, Anti Ransomware, Anti exploit to protect your systems from malware and advanced threats at different levels.
Multi layered protection helps to mitigate file based and file less attacks by using combination of signature based and signature less technologies. Detection engine uses pattern-based mechanisms to mitigate threats.
- **Global Threat Intelligence support**
Seqrite Security Labs is a renowned and leading source of threat research, threat intelligence and cybersecurity. The Security Labs analyses data fetched from millions of Seqrite products across the globe to deliver timely and improved protection to its users. Global threat intelligence service has auto sandboxing capability to check whether files are malicious or non-malicious.
- **Advanced Protection for Virtual Environments**
Install and manage EPS Clients on the supported operating systems that run in the virtual environments like VMware.
- **Data Protection**
Seqrite Endpoint Security protects against data loss and theft, provides security for the data residing on endpoints, file servers (File server Protection) and Windows storage server (storage security) against any malicious attacks.
- **Deception Technology**
Deception technology in Seqrite Endpoint Security can detect, analyze, and defend against zero-day and advanced ransomware attacks, often in real time.
- **Anti-theft Protection for data**
Seqrite Endpoint Security offers data theft Protection through DLP feature. This feature ensures that your confidential data is protected.
- **Cloud-Assisted Security Network**
Seqrite's Cloud assisted security network provides protection to the clients based on intelligence and assessment of global threats on a real-time basis, and URL categorization for classification of websites on a threat perception.
- **System Watcher**

Seqrite Endpoint Security offers real time scans which continuously scans and monitors systems and provides protection.

Seqrite Endpoint Security constantly monitors various events like host file modification, shell modification, or program library injection, etc.

- **Memory Protection**

Seqrite Endpoint Security offers memory protection from the viruses that are active in the memory of workstations.

- **Centralized Management and Control**

User friendly interface for monitoring, configuring, and managing systems in the network with detailed report and graphical dashboard. Primary and Secondary Server architecture to manage distributed network effectively.

- **Scalable solution**

Seqrite Endpoint Security solution is equipped to support large number of concurrent users. The Master- Slave architecture provides flexibility to deploy endpoints (at Head office, regional and branch offices) and manage large number of endpoints.

New in this release

Seqrite Endpoint Security 7.6 brings you the following:

- Endpoint IP Address details included in IDS/IPS, Port Scan and DDoS Report.
- Local and Remote Port details included in the Firewall Report.
- Complete Asset details of all endpoints can be exported in a single report from EPS web console > Clients > Assets > Download Complete Asset Details button.
- Endpoint Name and IP Address details included in SMS Notification for Virus and Ransomware attack.
- Option to configure OCR and File Fingerprinting settings added in EPS web console > Settings > Data Loss Prevention (DLP).
- Enhancement in client deployment method through Active Directory to support enumeration of large number of objects (10,000) in Active Directory while synchronizing Active Directory.
- Patch Management reports section now contains additional reports for Up-to-date, Patch Scan failed, and Patch Installation failed endpoints. Earlier only Missing and Installed patches reports options were available.
- The default applications listed in Application Control feature will be updated automatically to the latest version. The latest application version signatures will be released periodically through AV updates.
- Upgrade support is added for Windows 10 operating system through Seqrite Patch Management.

- Configure Seqrite Patch Server to get upgrade patches for Windows 10 operating system from “Seqrite EPS Web console > Admin Settings > Server > Patch Management > Configure Patch Server > Filters” page.
- In the Products tab, under Microsoft > Windows, select “Windows 10” and “Windows 10, version 1903 and later” and In the Categories tab, select the “Upgrades”.
- Consolidated Dashboard and Manage Secondary Server tabs will not be visible on EPS web console dashboard if EPS server does not have Secondary EPS server.
- On EPS dashboard top 10 incident count will be displayed instead of top 5. The top 10 incident can be exported to csv report.
- Notifications are displayed on browser if any website is blocked by Web Security feature. Earlier only alert messages used to appear. This feature is applicable only for clients installed on Windows platform.
- Master and multi-level secondary server architecture - As per your geographical locations, multiple and multi-level secondary servers are possible as per your requirement.
- EPS server compatibility with Windows 10 21H2, Windows 11, and Windows Server 2022.
- Asset Management feature displays following additional info,
 - OS Product key
 - Software upgrade changes in Reports and Dashboard
- Provision to exclude MD5 from Scan Settings. To do this, go to Settings > Scan Settings > Exclusion.
- In the Scan Settings > Advance > Archive Scan Level, Archive Scan Levels supports up to 16 levels.
- Provision to block/deny all URLs in the Web security feature with single button.
- The License Manager page shows additional details of license usage regarding Master/Secondary server and DLP licenses as applicable.
- Hierarchy representation of Server name on EPS Dashboard

On the Master server, “Hierarchy” name will be represented as “Master”.

On the Secondary Server, displays the hierarchy of the Server you have logged-on. This shows the names of the parent servers up to Master. Example: Master / Primary001 / Secondary001. In this case, the logged-on Server name is Secondary001, and the parent Server is Primary001, which is reporting to the Master.
- Displays online/offline status of Secondary Server on the Dashboard > Manage Secondary Server. The Green dot indicates online status. The Red dot indicates offline status. If the last connected time of Secondary server with the Master/parent server exceeds 2 hours, the status will be shown as offline.

- Centralized Policy Deployment
For this build, Policy will be enforced by default.
- On the Master server, the administrator will assign a policy for the Secondary Server. This policy is applied to the Secondary Server, its endpoints till the leaf Secondary Server. On the Secondary Server, this policy is not allowed to modify/override. So, the “Set Policy” option is disabled on “Manage Groups” page.
- Provision to add Multiple IP addresses, and DNS names (URL) in exception of Seqrite Firewall.
- GDPR - General Data Protection Regulation check box added on Software License Agreement.
- Displays VDB date along with Update time [hh:mm:ss] on Windows, Mac and Linux Client Scanner and on EPS Web Console.
- Provision to lock license with respect to country. The EPS License should be functional only in the specified countries.
- Provision to select all Patches at once for specific endpoints.
- Provision to store data backup in a customized way. You can add custom extensions to the custom list. Provision for customized backup reports.
- Authorized USB can be accessed in different EPS networks if administrator export policy with authorized USB settings and import into different EPS networks.
- Multiple Domain names/IP address can be added in firewall exceptions.
- On 64-bit Linux operating system - Linux Client AV GUI is now supported.
- When Master admin logs on Secondary server via auto login, then Master admin activity logs will be generated in Secondary sever event logs.
- As a part of branding, added logo for GoDeep.AI on EPS console footer.
- Data Loss Prevention
 - You can add custom application to monitor; also, you can add application to exclude from Data Loss Prevention. Applications added from the standard category will appear as per category in the list and custom application will appear in the Custom list on the DLP policy page.
 - Optical Character Recognition (OCR)

This is a new feature included in the DLP pack. In this feature the confidential/user defined data from image files (JPG, PNG, TIFF, bmp, GIF) is identified in case of data leak and action is performed as per policy. By default, OCR Scanning is disabled. Please contact technical support to enable this feature.

The OCR Scanning feature supports the following channels:

 - Removable Devices
 - Network Share

- Online services of third-party Application/Services
OCR accuracy and performance are best observed when processing high contrast, high DPI images devoid of any distortions. OCR is a resource-intensive operation, and can significantly increase the scan times due to the following factors,
 - Number of image files
 - Image Quality
 - Image Resolution
 - Image Transformations
- File Classification
You can classify existing files as Confidential or Public. Files classified as confidential are treated as sensitive files and any operation to leak is blocked/reported as per DLP policy.
To classify at the time of creating a new file, contact Seqrite Support team to enable required settings.

Available flavors

Seqrite Endpoint Security is available in the following flavors:

- SME (Small and Medium Enterprises Edition)
- Business
- Total
- Enterprise Suite

The following table lists the features that are available in the flavors:

Features	Status			
	SME	Business	Total	Enterprise Suite
IDS/IPS Protection	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
Antiphishing	✓	✓	✓	✓
Browsing Protection	✓	✓	✓	✓
SME Notification	✓	✓	✓	✓
Vulnerability Scan (VS)	✓	✓	✓	✓
Roaming Clients	✓	✓	✓	✓
Asset Management	X	✓	✓	✓
Antispam	X	✓	✓	✓
Web Security	X	✓	✓	✓

Advanced Device Control	X	✓	✓	✓
SIEM Integration	X	✓	✓	✓
Application Control	X	X	✓	✓
Tuneup	X	X	✓	✓
PC2Mobile	X	X	✓	✓
File Activity Monitor(FAM)	X	X	✓	✓
Patch Management	X	X	✓	✓
Data Loss Prevention (DLP)	X	X	X	✓

Feature Pack Definition:

Pack Name	Features	Flavor
DLP	Data Loss Prevention + Data-At-Rest Scan	Business and Total edition can subscribe DLP feature. SME need to upgrade to Business or Total to subscribe for DLP.

License Subscription

Seqrite provides prepaid license subscription for Seqrite Endpoint Security. Once you subscribe, Seqrite sends you an email containing URL and license key to download and install the setup for Seqrite Endpoint Security. After installation, you need to activate EPS with help of valid license key.

Certifications

Our security solutions are acknowledged year after year by associations, the media and industry organizations. To know more, visit

<https://www.seqrite.com/awards-certifications>

Network Deployment Scenarios

Network setup differs from organizations to organizations depending on their size and architecture. Some organizations prefer a simple network setup with one server and multiple clients while some others may prefer a network setup with subnets or DHCP servers. Also, an organization with a huge network setup may have a single server with multiple LAN cards catering to the needs of networks with different IP ranges.

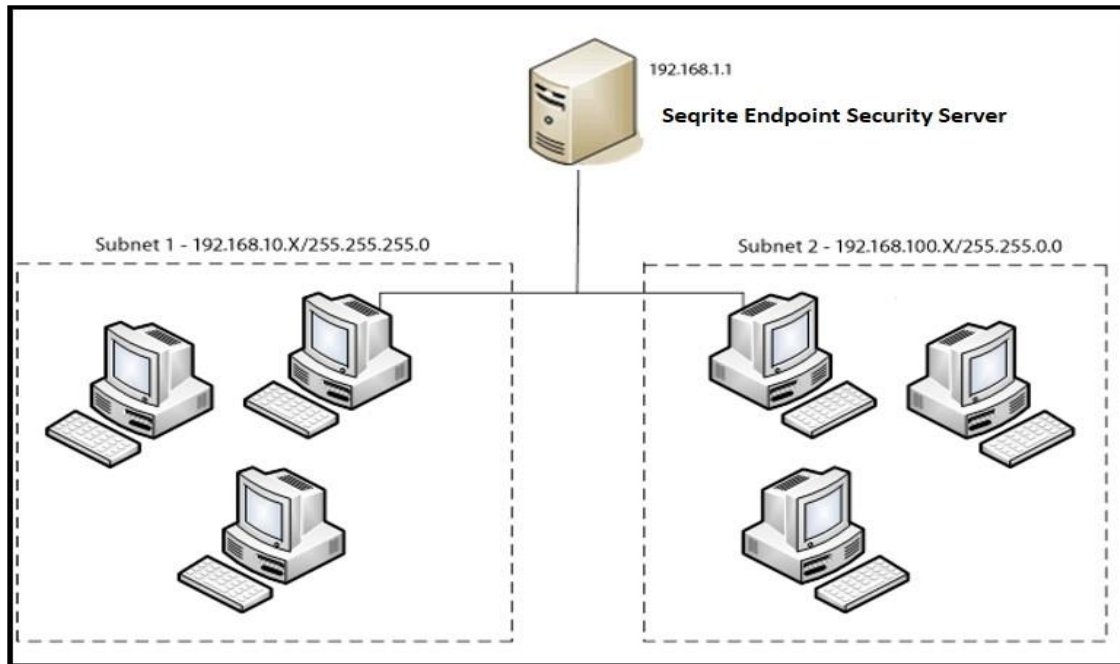
Seqrite realizes the challenges of varying network setups in different organizations. Therefore, we have provided recommendation for three prominent network setups:

Scenario 1

Installing Seqrite Endpoint Security on a network with subnets configured using static IP address.

Network Setup Description

The entire network is configured using static IP addresses and the network comprises of subnets connected to the main server. Seqrite Endpoint Security is installed on the server and Seqrite client agents are deployed on the endpoint systems in the subnet.



Seqrite Recommendation

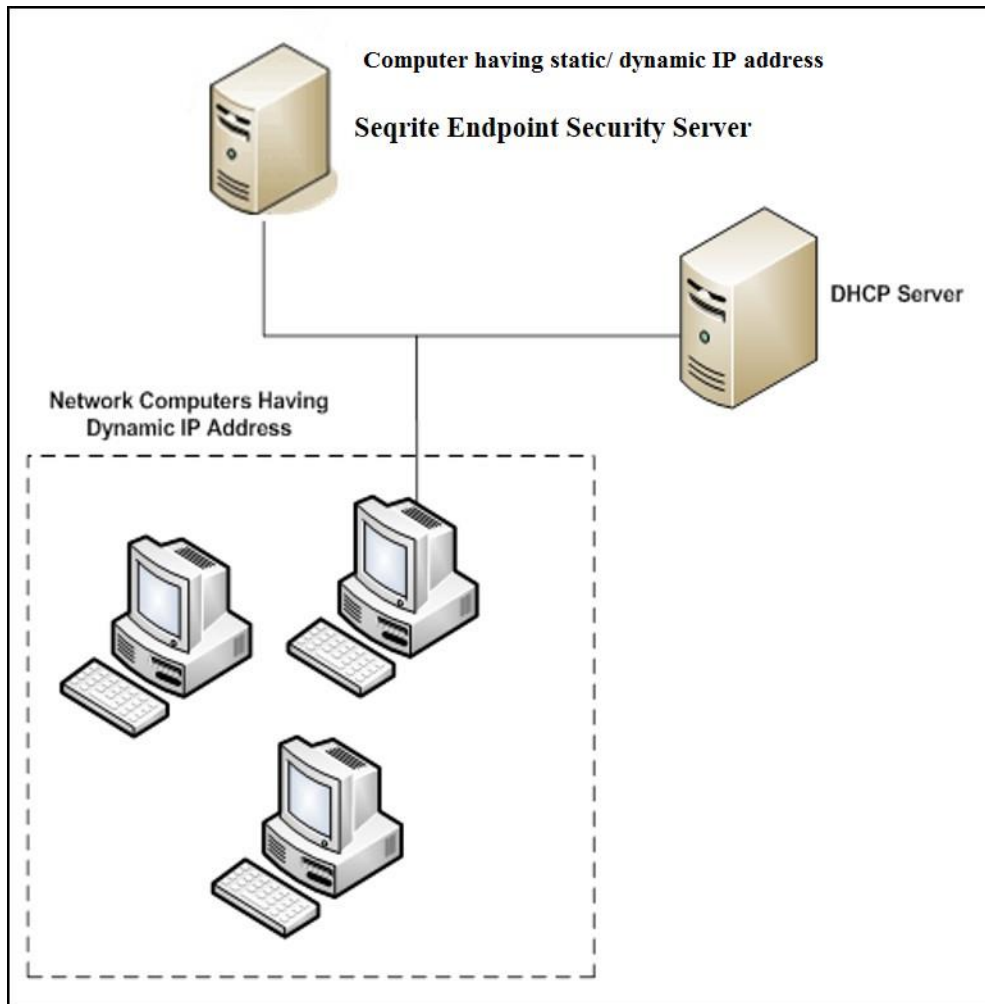
- Before installation, ensure that the server and endpoints are connected. Verify this by pinging server to the endpoints and vice versa.
- The server system should be configured using static IP address.
- During installation of Seqrite Endpoint Security, select IP Address in the Server Information screen.

Scenario 2

Installing Seqrite Endpoint Security on a network with endpoints configured using DHCP server.

Network Setup Description

The entire network is configured using a DHCP server. Seqrite Endpoint Security is installed on server system and the Seqrite endpoint agents are deployed on the endpoint systems.

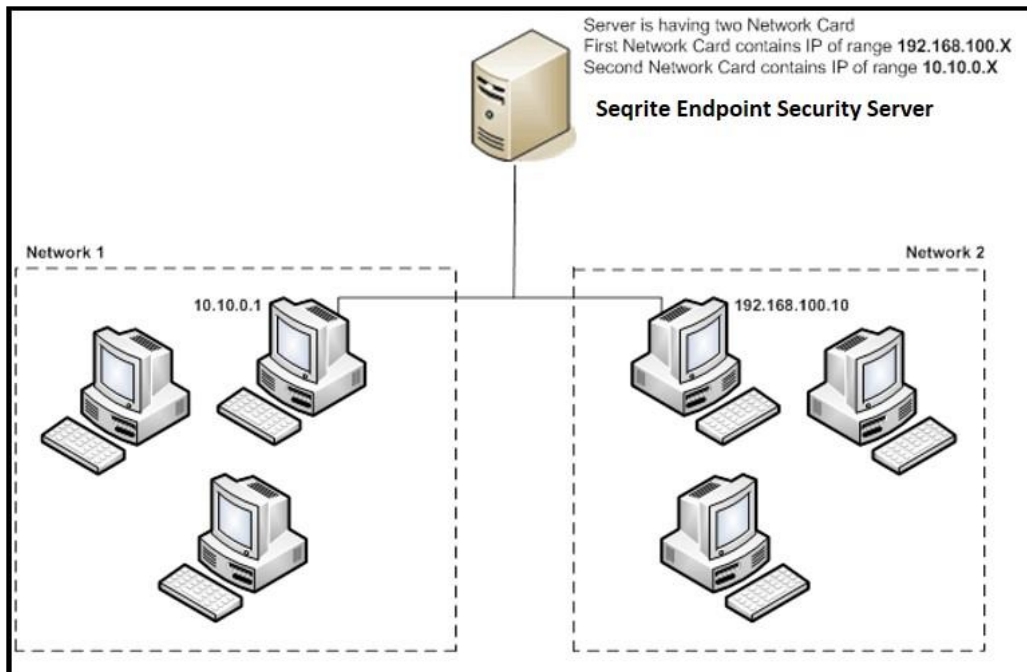


Scenario 3

Installing Seqrite Endpoint Security on a server using two network cards.

Network Setup Description

The server consists of two network cards, each catering to a network of different IP ranges (Example: One network has the IP range of 10.10.0.1 and the other network has the IP range of 192.168.100.10). Seqrite Endpoint Security is installed on the server with two network cards and Seqrite clients are installed on all endpoint systems of both the networks.



Seqrite Recommendation

- Before installation, ensure that the server and endpoints are connected. Verify this by pinging server to the endpoints and vice versa. Try to ping using IP address and computer name.
- The server system should be configured using static IP address.
- During installation of Seqrite Endpoint Security, select Domain Name in Server Information screen. Provide the target server domain name. You can also use Fully Qualified Domain Name (FQDN) of the server if the endpoint has access to a DNS server, which can resolve the FQDN with the endpoint's IP address.

Getting Started

Seqrite Endpoint Security (SEPS) is simple to install and easy to use. During installation, read each screen carefully and follow the instructions.

Prerequisites

Remember the following guidelines before installing SEPS on your computer:

- Remove any other antivirus software/hardware from your server and endpoints before installing Seqrite EPS. A computer system with multiple antivirus programs installed may result in system malfunction.
- Close all open programs before proceeding with installing Seqrite EPS.
- Network should be configured with TCP/IP protocols.
- File and printer sharing for Microsoft Networks must be installed.
- To install Seqrite EPS server, you must have administrator or domain administrator rights.
- To use the Login Script setup, Windows Server 2012 R2 / Windows Server 2012 / Windows 2008 Server R2 / Windows 2008 Server / Windows 2003 Server should be properly configured with Active Directory services.

System requirements for SEPS server

System requirements for Seqrite Endpoint Security server are as follows:

General requirements

The computer where SEPS server is to be installed must meet the following requirements.

Component	Requirements
Processor	Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium or higher
RAM	Minimum:

	2 GB Recommended: 4 GB or more EPS server may require additional RAM as per the requirements of installed applications.
Hard disk space	Minimum: 4800 MB free disk space Recommended: 10000 MB free disk space
Web Browser	<ul style="list-style-type: none"> • Internet Explorer 10 or 11 • Google Chrome 62, 63, 64 or 65 • Mozilla Firefox 56, 57, 58, 59, 62, 64 or 65
Display	1024 x 768



- For more than 25 clients, Seqrite recommends installing EPS Server and Patch Management server on the Windows Server operating system.
- For more than 500 clients, Seqrite recommends a dedicated Web server (IIS).
- Seqrite recommends deploying a separate/dedicated Alternate Update manager for a group of up to 200 clients for proper load balancing.

Operating system requirements

- Microsoft Windows 11
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP 32-bit SP3, 64-bit SP1 and SP2 / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2022 Standard / Datacenter / Essentials
- Microsoft Windows Server 2019 Standard / Datacenter / Essentials
- Microsoft Windows Server 2016 Standard / Datacenter (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials

- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)



The following operating systems support only Master Servers without any Secondary Server,

- Microsoft Windows XP 64-bit SP1 and SP2 / Professional Edition (64-bit)
- Microsoft Windows Server 2003 Web / Standard / Enterprise (64-bit)

Additional software required for SEPS server

Seqrite EPS server needs to have Microsoft IIS Web server as well as Microsoft .NET Framework 4.0 on your computer system.

Web server	Requirements
IIS	IIS Version 10 on Windows 10
	IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2
	IIS Version 8.0 on Windows 8 and Windows Server 2012
	IIS Version 7.6 on Windows 7 and Windows Server 2008 R2
	IIS Version 7.0 on Windows Vista and Windows Server 2008
	IIS Version 6.0 on Windows Server 2003
	IIS Version 5.1 on Windows XP SP3



The EPS installer will install required IIS Components.

Java Runtime Environment (JRE) Requirements

Java Runtime Environment (JRE) required to perform installation through Web page and Add Device functionalities are as follows:

OS versions	Requirements	JRE
32-bit	32-bit	JRE 7, JRE 8
64-bit	32-bit	32-bit JRE 7, 32-bit JRE 8
	64-bit	64-bit JRE 7, 64-bit JRE 8

System requirements for Seqrite EPS clients

System requirements for Seqrite Endpoint Security clients are as follows:

General requirements

The computer where SEPS client is to be installed must meet the following requirements.

Component	Requirements
Processor	Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista or higher
RAM	Minimum: 1 GB Recommended: 2 GB or more
Hard disk space	3200 MB
Web Browser	Internet Explorer 5.5 or later

Operating system requirements

Seqrite Endpoint Security client can be installed on a computer system with any one of the following operating systems:

- Microsoft Windows 11
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Basic/ Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2022 Standard / Datacenter / Essentials
- Microsoft Windows Server 2019 Standard / Datacenter / Essentials
- Microsoft Windows Server 2016 Standard / Datacenter (64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)

- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)



- For Windows 2016 Server and Windows 2019 Server, uninstall Windows Defender before installing Seqrite EPS client.
- If you are upgrading the EPS client to Windows 2016 Server or Windows 2019 Server, uninstall Windows Defender after upgrade.

System requirements for Mac OS

Software and hardware requirements for Seqrite EPS clients on Mac OS are as follows.

Component	Requirements
MAC OS	Mac OS X 10.9, 10.10, 10.11, macOS 10.12, 10.13, 10.14, 10.15, 11 and 12
Processor	Intel or Apple M1 chip
RAM	Minimum: 512 MB Recommended: 2 GB or more
Hard disk space	1200 MB

System requirements for Linux OS

Software and hardware requirements for Seqrite EPS clients on Linux OS are as follows:

Component	Linux OS versions	Requirements
Linux OS	32-bit	<ul style="list-style-type: none"> • RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 • BOSS 6 • Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25 • openSUSE 11.4, 12.2, 12.3, 13.2, 42.2 • Linux Mint 13, 14, 15, 16, 17.3, 18 • Ubuntu 10.10, 11.4, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10, 17.04 • CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9
	64-bit	<ul style="list-style-type: none"> • RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3 • Boss: 7.0, 8.0 • Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25

		<ul style="list-style-type: none"> • openSUSE 11.4, 12.2, 12.3, 42.3 • Linux Mint 13, 14, 15, 16, 17.3, 18 • Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10, 17.04, 17.10, 18.04, 20.04 LTS • CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.4, 8.0, 8.1 • SUSE Linux 11.00, 12.00, 12.2
Processor		Intel core compatible
RAM		Minimum: 512 MB Recommended: 1 GB or more
Hard disk space		1200 MB

The EPS client supports the above-mentioned distribution. The clients also support the other versions if the following prerequisites are met,

For 32-Bit OS:

GNU C Library 2.11 and above

SAMBA version 3.5.x to 4.5.x, 4.10.x, 4.11.x.

For 64-Bit OS:

- GNU C Library 2.5 and above

SAMBA version 3.5.x to 4.5.x, 4.10.x, 4.11.x.

In case of the clients with other than above mentioned Linux operating system, Seqrite recommends to validate the clients in a non-production environment before deploying in the production environment.

To check for more details about system requirements, visit <http://www.seqrite.com>.

Installing Seqrite Endpoint Security server on Windows Operating System

To begin installation of Seqrite Endpoint Security server, follow these steps:

1. Download and execute the setup downloader for Seqrite Endpoint Security from the URL mentioned in the Software License Certificate.
2. Execute the setup.
3. On the Seqrite Setup Downloader screen, do the following:

- i. In the **Select the directory to download setup** box, select the location to download the setup.
 - ii. The **Launch setup when download completes** check box is selected by default. This initiates the installation immediately after the download is complete.
 - iii. If you want to install SEPS later, clear the **Launch setup when download completes** check box. Select the **Open folder location when download completes** check box.
 - iv. Click **Download**. The time and progress of download appears. When the download is complete, a message appears, "Seqrite Endpoint Security setup is downloaded successfully."
4. If the option **Launch setup when download completes** is selected, after the setup is downloaded, the SEPS setup wizard starts immediately.

If the option **Open folder location when download** completes is selected, the folder opens. Select the installer file and double click it. The SEPS setup wizard starts.

5. Read the information about Seqrite Endpoint Security. Click **Next**.
6. The license agreement appears. Read the License Agreement carefully. Installation and usage of Seqrite Endpoint Security is subject to your formal acceptance of the Seqrite Endpoint Security end-user license terms and conditions.

Select **I Agree** to accept the license agreement, and then click **Next**.

7. Seqrite EPS server needs Microsoft .NET Framework 4.0 and Microsoft IIS Web server on your computer system to complete the installation.

If .NET and IIS are both already installed, SEPS setup wizard continues.

If .NET, IIS or any one of the required components is not installed, a Pre-requisites Checks screen is displayed. The screen shows the installed and missing components that are required to proceed with the installation. Click **Next**.

The wizard helps you to install .NET and, then IIS component.

To install .NET Framework, follow these steps,

A screen is displayed to install .NET Framework.

- i. Click **Next** to continue with the installation of .NET Framework.
- ii. In the Microsoft .NET Framework 4 Setup screen, select the **I have read and accept the license terms** check box and click **Install**.

Installation progresses.

- iii. In the Microsoft .NET Framework 4 Setup screen, click **Finish**.
- iv. Restart the system.
- v. Start the Endpoint Security installation again with the installer file.

To install IIS, follow these steps,

- i. A screen is displayed to install IIS.

In the Prerequisite – Internet Information Services (IIS) screen, click **Next**.

IIS will be configured on the system.

- ii. Click **Next** to continue the SEPS setup wizard.

If you want to enable IIS on Windows Server 2003 and XP, see [Enabling IIS on Windows Server 2003 and XP](#).

8. The Proxy Settings screen appears.

If you are using a proxy server on your network or using Socks Version 4 and 5 networks, you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Connection settings. Username and password are mandatory to log on.

The SEPS modules, Registration Wizard, Update Manager, and Messenger uses the following settings to connect to the internet.

To enable and configure proxy settings:

- i. Select the **Enable Proxy Settings** check box.
- ii. Select the Proxy Type as HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings.
- iii. In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
- iv. In the **Port** text box, type the port number of the proxy server (For example: 80).
- v. In the **User Name** and **Password** text boxes, type in your proxy server credentials.
- vi. Click **Next**.

9. The Pre-requisite – MySQL 5.6.42 screen appears.

You need to provide a path for MySQL 5.6.42 setup file. If you do not have MySQL 5.6.42 setup file, download from the given link and provide the path.

Click **Next**.

The file will be verified.

10. Select one of the following server types:

- Master Server - Select this option to make EPS as Master Server. Master Server can manage local clients and Secondary Servers installed at different locations.
- Secondary Server - Select this option to make EPS as Secondary Server. Secondary Server can be installed at different locations, and it reports important statistics to the Master Server.
 - a. Enter **Master Server IP/Name**.
 - b. Enter **Master Server Port** number.
 - c. Click **Verify**. The Master Server details are verified. Only after successful validation, the installation can progress.

The installation steps remain the same for both types of server.

11. Click **Browse** if you want to install Seqrite Endpoint Security server to another folder than the default folder. To proceed with the default installation default path, click **Next**.

The Seqrite Endpoint Security installer scans system memory for virus infection and verify the installed system components.

While installing SEPS, if another antivirus software is already present on your computer, a message appears to uninstall the other antivirus software.

SEPS server installation does not proceed further until you remove the other installed antivirus software.

12. On the Server Information screen, do the following:

- i. In the Server Information section, select one of the following and provide the information:

Domain Name: Select the server **Domain Name** from the list. You can also use Fully Qualified Domain Name (FQDN) of the server if the endpoint has access to a DNS server, which can resolve the FQDN with the endpoint IP address.

If your network is configured using DHCP, select Domain Name.

IP address: Select the **IP Address** of the server from the list.

- ii. Select the **Public Installation** check box if you are installing Seqrite Endpoint Security on a system hosted on the AWS/Azure platforms.

- Recommendation

- If you are planning to deploy the endpoints locally (Private), Seqrite recommends to do Installation on private IP.
- If you are planning to deploy some endpoint locally and some endpoints remotely, then Seqrite recommends do installation on private IP natted to Public IP. In this case while creating a client packager for the remote client, provide alternate IP address or Domain name.

If you are planning to deploy all the endpoints remotely, Seqrite recommends Public Installation.

- iii. In the HTTP section, Port number appears. HTTP Port Number is a port to use as the server listening port. Seqrite Endpoint Security server address is as follows to launch the console,

- For Windows XP: `http://{Seqrite_Endpoint_Security_Server_name}/qhscan760`
- For other OS: `http://{Seqrite_Endpoint_Security_Server_name}:{port number}`

- iv. In the SSL section, by default the **Enable Secure Socket Layer** check box is selected and **SSL Port** number appears.

This port number serves as a listening port for the server. Seqrite Endpoint Security server address is as follows to launch the console,

- For Windows XP: `https://{Seqrite_Endpoint_Security_Server_name}/qhscan760`

- For other OS: https://{Seqrite_Endpoint_Security_Server_name}:{port number}



Do not use the following ports,

- Port Numbers 0-1023
- MySQL port 62222

- v. Click **Next**.
- vi. A message appears for your verification about the Web server settings.

13. To confirm, click **Yes**.

You can make changes in your settings if required.

14. If you select Public Installation, provide the **domain name or IP address** of the target Server which will be used by the remote clients to communicate with the EPS Server.

By default, clients that are installed by the client packager are configured to communicate with the EPS server with this domain name/IP address.

15. Click **Next**.

16. The Client Installation Settings screen appears.

Seqrite client is installed on the endpoint as per the path specified in this screen. The following settings are displayed:

- Default endpoint installation path appears. The Path can be provided using either %PROGRAMFILES% or %BOOTDRIVE% variable. For example: %PROGRAMFILES%\Seqrite\Seqrite or %BOOTDRIVE%\Seqrite.
- The Client Agent Communication Port number appears.

The Seqrite clients communicate with server to fetch important instructions such as, scanning and updates, and submit the log to Seqrite Endpoint Security server using this port number. So, ensure that this port number is not used by any other application in the network.

Click **Next**.

17. A confirmation dialog box appears for your confirmation. You can change the port number if required.

To confirm, click **Yes**.

18. The Authentication screen appears.

Create Seqrite Endpoint Security administrator password to access the Web console and endpoint password to access the endpoint settings at the endpoint side. The password for administrator and endpoint should be different; else the installation will not proceed.

- i. In the Endpoint Security Administrator Password section, type in your password in the **Password** and **Confirm password** text boxes.
- ii. In the Client Password section, type in your password in the **Password** and **Confirm password** text boxes.

This helps prevent unauthorized users from accessing the Web console and make changes in your settings or remove the endpoints.

iii. Click **Next**.

19. The MySQL Authentication screen appears.

- i. In the Username and Password text boxes, type in your MySQL user credentials.
- ii. In the Confirm password text box, retype the password.
- iii. Click **Next**.

20. The installation summary screen appears. You can change your settings if required.

Click **Next**.

21. A confirmation dialog box appears stating that the Network connection on the system will be temporarily disabled if you continue with Seqrite Endpoint Security installation on the system.

To continue with installation, click **OK**.

22. The installation process starts. The **Read me** information screen appears. Read the important information related to Seqrite Endpoint Security.

Click **Next**.

23. The **Things to do** screen appears. All the following options are selected by default,

- Register Seqrite Endpoint Security
- Configure Update Manager
- Automatically delete reports older than ... days. Here you can select number of days to delete the reports. It is recommended to keep older reports for no longer than 90 days. Not removing older reports can impact the performance. This selection is reflected at [Reports > Manage > Settings](#).

24. Click **Next**. If you want to perform these tasks later, clear these options. In case of Secondary Server installation, registration window does not appear as the Master Server activates the Secondary Server.

25. To complete the installation, click **Finish**.

Enabling IIS on Windows Server 2003 and XP

1. Click **Start > Settings > Control Panel**.
2. In Control Panel, double-click **Add or Remove Programs**.
3. In the Add or Remove Programs dialog box, in the left pane, click **Add/Remove Windows Components**.
4. In the Windows Components page, in the Components box, click **Application Server/Internet Information Services (IIS)**, and then click **Next**.
5. Wait for the installation to complete and close the wizard.



For IIS Installation on windows Server 2003 and Windows XP, you may need OS installation CD.

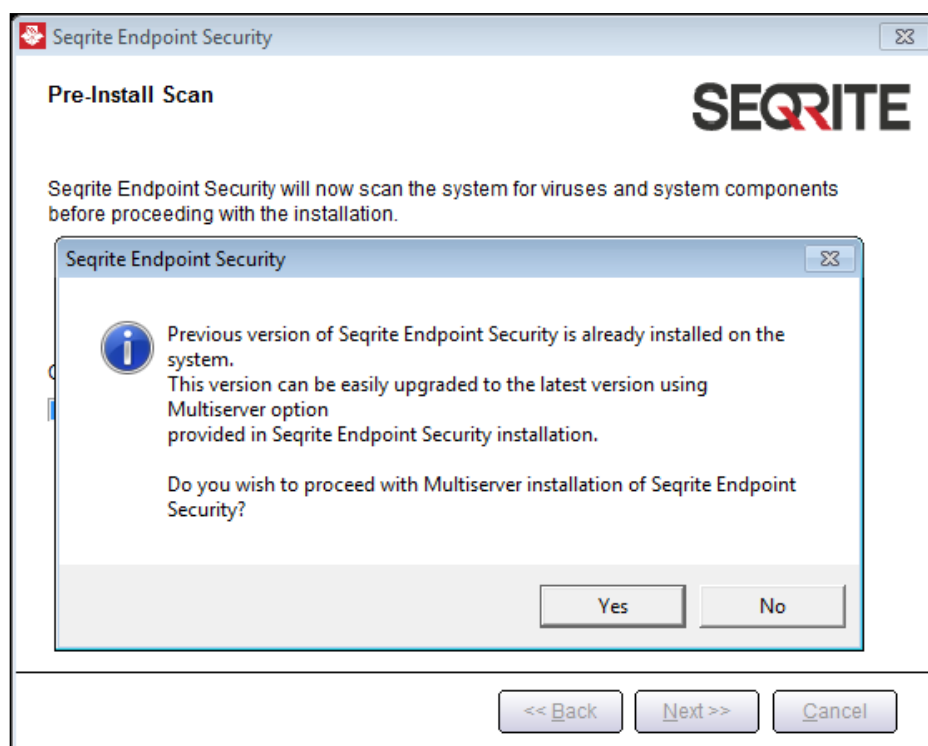
Installing Multiple Seqrite Endpoint Security Servers

Seqrite Endpoint Security multiple server installation is a unique feature of Seqrite Endpoint Security. Administrators can install latest version of Seqrite Endpoint Security where the previous versions are already installed. This feature enables the administrators to easily migrate to the latest version of Seqrite Endpoint Security in simple ways.

Upgrading Seqrite Endpoint Security to the latest version

Seqrite Endpoint Security can be upgraded in the following way:

1. Install Seqrite Endpoint Security on the system where previous version of Seqrite Endpoint Security is installed.
2. Seqrite Endpoint Security will detect the previous version and will show the following message:



3. To proceed with multiserver installation, click **Yes**.

After the installation of the latest version of Seqrite Endpoint Security is complete, open the previous version of Seqrite Endpoint Security and follow these steps:

- i. Go to **Admin Settings > Server > Redirection**.

- ii. In **Server Name/IP** text box, type the server name or IP address of the latest version of Seqrite Endpoint Security.



If the higher version of EPS is installed on DHCP based IP, Seqrite recommends that use server name.

- iii. In Port text box, type the port number of the latest version of Endpoint Security.
- iv. Click **Apply**.

This will send a notification about the latest version of Seqrite Endpoint Security to all Seqrite endpoints and they would be redirected to the latest version.

The latest version of Seqrite Endpoint Security checks if there are any previous versions of SEPS in the network. If detected, the installation process will automatically uninstall the previous version of SEPS and install the latest version.

4. After all the endpoints are upgraded, uninstall the previous version of Seqrite Endpoint Security server.

Before uninstallation, note down the Product Key of your Seqrite Endpoint Security server that will be required for reactivation of the latest version of Seqrite Endpoint Security.

5. After uninstallation of the previous version of Seqrite Endpoint Security, reactivate the latest version of Seqrite Endpoint Security with your existing product key.



****** You can upgrade all the endpoints with the latest version of SEPS within 30/60/90 days. The Default is set to 60 days. These settings can be configured from Admin Settings > Server > General > Multi server migration period, on higher version EPS server when in multi-server mode.

Best cyber security practices for Enterprises to stay cyber secure

In wake of the rising incidences of targeted attacks on enterprises, there is no way organizations can afford to ignore the importance of cyber security. Regardless of the size and type of enterprise, even a small data breach or cyber-attack could mean millions of dollars of loss, crippling the economy of enterprise.

It is for this reason that as a thumb rule, enterprises start following these good cyber security practices, in order to be cyber secure against known and unknown threats:

- Invest in Security Solutions – An enterprise may be subjected to various kinds of threats and thus, to ensure enterprise-wide security, it is a good practice to invest in a variety of security solutions that cover the changing needs of an organization.
- Use Complex & Unique Password – As a thumb rule, enterprises must encourage employees to use strong and unique passwords and prohibit them from sharing their credentials.

- Invest in Training – Educate and train employees about cyber security so that they are absolutely cautious about clicking suspicious links, sharing sensitive data and responding to security alerts.
- Backup Your Data – Follow the 3-2-1 rule when it comes to data backup, meaning that maintain 3 varying copies of your crucial data in 2 different formats, where at least 1 of the data storage locations should be offline.
- Disabling remote access - It is advisable that, the Administrator should disable remote access for all users. If remote access is given to all users, an unauthorized user may gain control of your system to steal, change or destroy information, by installing malware. Disable remote access will help protect your computers from any current or future attempts to exploit your data.
- In case remote access is enabled for some specific users, ensure to use strong and unique passwords for remote access. Also, provide limited access to the user.
- Robust Security Policies – In order to ensure that both employees and third parties follow the security policies, it is important to strictly convey the enterprise security policies and expectations.
- Use Updated Software – Using an expired software is as good as counting on a dead security solution. Thus, it is a good practice to keep your software updated to the latest version, to safeguard your organization against evolving threats.
- Data Encryption – It is advisable to encrypt all the saved and backed up data, while providing access rights to only limited and specific personnel.
- Two-Factor Authentication – An additional and reliable login procedure is to use two-factor authentication that uses a secondary device like mobile for access authentication.
- Have an MDM Plan – It is important to monitor and regulate the mobile device usage of employees since, they often use it for accessing sensitive data and company Emails, while using company's wireless network. This may serve as a soft vulnerability for attacks.
- Change Default Credentials – There are several IoT devices that come with default passwords that make it easy for malware to target such IoT devices. Thus, it is a good practice to change these default credentials.
- Secured Wi-Fi – A device can connect to only those Wi-Fi networks which have a known SSID. Thus, to prevent an unknown device from connecting to the Wi-Fi network of your enterprise, a good security mechanism is to use a hidden SSID to prevent it from getting broadcast.
- Limited Access Right Grant – Anyone who requests access to a resource, should be provided with minimum access rights and that too for the shortest duration necessary. Such restricted delegation of access right can limit attackers from intruding systems.

- Server OS Hardening – In order to address the security of your enterprise adequately, it is advisable to configure and harden the operating system. This typically involves removing all the unnecessary applications, services, and network protocols.

Post Installation Tasks

Seqrite Endpoint Security must be registered immediately after installation to activate the copy, otherwise endpoint deployment will not start.

Registration

Seqrite Endpoint Security is simple to register.

Registering Online

If your system is connected to the Internet, you can register Seqrite Endpoint Security online in the following way:

1. Go to **Start > Programs > Seqrite EPS Console > Activate Seqrite EPS Console**.
2. On the Registration Wizard, type the product key and then click **Next**.
3. Type relevant information in the Purchased from, Register for, and Name text boxes.
4. Click **Next**.
5. Type your personal details such as organization's email address, administrator email address, contact number, and location details.
6. Click **Next**.

A confirmation screen appears with the information that you have entered. You can change your information if required. To change your information, click **Back** to go to the previous screen and make the required changes.

7. To confirm, click **Next**.

It takes few seconds to register and activate your copy. Please stay connected to the Internet during this process.

After the activation completes successfully, a message appears with the License validity information for your reference.

8. To close the Registration Wizard, click **Finish**.



You can find the Product Key on the User Guide or inside the box. If you have purchased the software online using credit card, you will find the Product Key in the email confirming your order.

Internet Settings

When you open the registration wizard, the system tries to connect to the direct Internet connection. If the default Internet connection is not found, it shows the message, **System is not connected to the Internet. Please connect to Internet and try again.**

If you have alternative ways to connect to the Internet, follow these steps to connect to the Internet and register online:

1. Click the **Internet Settings** button.

The Configure Proxy Settings screen appears.

2. To set the proxy setting for Internet, select **Enable Proxy Setting**.

The proxy settings details are activated.

3. In the Sever text box, type the sever name.
4. In the Port text box, type the port number.

You can also set authentication rule if you use Firewall or proxy server. For this, type the User Name and Password in the Authentication section.

5. To save your setting, click **OK**.
6. Click **Retry to connect to the Internet**.

If you are connected to the Internet, the online activation wizard opens, and you can activate your product online.

Reactivation

This section includes the following:

Reactivating Seqrite Endpoint Security

Reactivation is a facility that ensures that you use the product for the full period until your license expires. If you uninstalled Seqrite Endpoint Security and now you want to install it again or you want to install Seqrite Endpoint Security on the other endpoint. In such cases, you need to reactivate Seqrite Endpoint Security.

The reactivation process is similar to the activation process, with the exception that you need not type the complete personal details again. On submitting the product key, the details are displayed. Complete the process by verifying the details.

Disabling remote access

Administrator should disable remote access for all users. If remote access is given to all users, an unauthorized user may gain control of your system to steal, change or destroy information, by installing malware. Disable remote access will help protect your computers from any current or future attempts to exploit your data.

Configuring Update Manager

Update Manager is a tool integrated with Seqrite Endpoint Security. This tool is used to download and manage the updates for Seqrite Endpoint Security. Update Manager provides you the flexibility to download the updates on any endpoint. All the Seqrite Endpoint Security clients fetch the updates from the centralized location. Update Manager automatically updates Seqrite Endpoint Security for new enhancements or bug fixes.

Accessing Update Manager

To access Update Manager, select **Start > Programs > Seqrite EPS Console > Update Manager**.

Features of Update Manager

Update Manager includes the following features:

- Status
- Configuration
- Connection Settings
- Reports

Status

Status includes information about the latest updates downloaded by Update Manager. It displays the product version, service pack, and virus database date of your Endpoint Seqrite Security.

Configuration

Configuration helps you customize and configure Update Manager.

To access configuration, follow these steps:

1. Select **Start > Programs > Seqrite EPS Console > Update Manager**.
2. Click **Configuration**.
3. Type the Super Administrator Password and then click **OK**.
4. If you want to take the updates automatically, select the **Enable Automatic Updates** check box.

This feature is enabled by default. Seqrite recommends that you do not disable this feature.

5. Select the updating mode from the following options:

- **Internet Center:** Helps you download the updates to your system from the default Internet Center.
- **Specified URL:** Helps the endpoint obtain the updates from a specified endpoint that has the updates downloaded by the connected system.
 - In the Server text box, type the URL.
 - In the Port text box, type the port number.



The msg32.htm file should be present at the update location in the system with Internet connection.

To create the msg32.htm file, rename a text file as msg32.htm file.

- **Specified path:** Helps you pick the updates from a specified local folder from your computer without Internet connection. You can specify the path of the local folder from where the updates are to be copied.

For example, if you have downloaded the updates on other system, you can copy them into a CD/DVD or pen drive and then paste in the local folder. Update Manager will fetch the updates from this local folder path.

- i. Select the **Pick from specified Path** option.
- ii. Type or browse the path to the folder from where the updates need to be copied.

6. Select the **Download Seqrite Endpoint Security Service Pack** check box. This feature is enabled by default.

7. Select the **Restrict download speed (kbps)** check box if you want to restrict the download speed. Enter the speed in the text box.

8. Verify the path mentioned in **Download updates to** box. All the Seqrite Endpoints Security products will take the updates from this centralized location.

9. Select the following check boxes:

- **Always take backup before downloading new update:** Helps you take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. This feature is enabled by default.
- **Delete report after:** Helps you delete the reports as per the time interval selected by you. This feature is enabled by default. The default value of time interval is 10 days.

10. To prevent unauthorized access to the Seqrite Endpoint Security settings, you should enable password protection. Select the **Enable password protection** check box. Type password and click **Ok**.

11. To save your changes, click **Apply**. In the Confirmation dialog box, click **Yes**.

If you want to restore the default settings, click the **Default** button.

The following are the two buttons that are accessible always:

- Update Now
- Rollback

Fields	Definitions
Update Now	Helps you download the new updates for Seqrite Endpoint Security.
Rollback	<p>Helps you rollback Update Manager to the previous state. The latest updates are removed. This feature will work only if the Always take backup before downloading new update option is selected in the Configuration section of Update Manager. The steps to rollback Update Manager are as follows:</p> <ul style="list-style-type: none"> • Click the Rollback button. The Seqrite product for the Endpoint Security is displayed. • Confirm the product that you want to roll back and then click the Rollback button on the displayed screen. You may click Close to exit the dialog.

Schedule Scan in Update Manager

With Schedule Scan, you can define the scheduled scans for the Update Manager at certain frequency.

To configure Update Manager Schedule Scan, follow these steps:

1. Select **Start > Programs > Seqrite EPS Console > Update Manager**.
2. Click **Configuration**.
3. Type the Super Administrator Password and then click **OK**.
4. Click **Settings**.

The Update Manager Scheduler dialog appears.

5. Select the **Custom** option and configure the following options:
 - i. In **Frequency**, select either the Daily or Weekly option.
If you select Weekly option, select the weekday from the list.
 - ii. In **Start At**, set time in hours and minutes.
 - iii. If you want to repeat scanning of the Update Manger, select the **Repeat Update** check box and set the frequency in days to repeat the scan.
6. Click **Apply**.

Connection Settings

If a proxy server is being used on the network, you need to provide the IP address (or domain name) and the port number of the proxy server in the Connection Settings.

To access Connection Settings, follow these steps:

1. Select **Start > Programs > Seqrite EPS Console > Update Manager**.
2. Click **Connection Settings**.
3. Type the Super Administrator Password in the **Password** box and click **OK**. The Connection Settings page appears.
4. To enable HTTP proxy settings, follow these steps:
 - i. In the **Connection Type** list, select HTTP.
 - ii. Select the **Enable Proxy** check box.
 - iii. Select **Proxy Type** from the list.
 - iv. In the **Server** text box, type the IP address of the proxy server or domain name (Example: proxy.yourcompany.com).
 - v. In the **Port** text box, type the port number of the proxy server (Example: 80).
 - vi. If required, for firewall or proxy server section, type your logon credentials in the **User Name** and **Password** boxes to authenticate.
 - vii. To save the changes, click **Apply**. In the Confirmation dialog, click **Yes**.

If you want to restore the default settings, click the **Default** button.

Reports

The Reports section records a log of updates or rollback activities. Reports provide the details such as; Date, Time, and Status of the updates or rollback activity.

To access reports, follow these steps:

1. Select **Start > Programs > Seqrite EPS Console > Update Manager**.
2. Click **Reports**.

You can perform the following actions on reports:

Fields	Description
View	To get the complete details of the downloaded update or rollback, select a report and click View .
Delete	To delete the report, select a report and click Delete .
Delete All	To delete all the reports in the section, click Delete All .
Previous	Helps you view the previous report.
Next	Helps you view the next report.
Save As	Helps you save a copy of the report in text format on your local computer.
Print	Helps you print a copy of the report.
Close	Helps you exit from the report window.

Configuring ports on the Azure or AWS Cloud machine

You should configure the ports to establish communication between the EPS server and the clients. Allow the ports of EPS server, Database, Patch Server, and Update Manager in the cloud machine where EPS will be deployed.

Allow the following ports from the Azure or AWS machines:

- EPS Console - 9111
- CGI - 6805
- Download - 8101
- Communication - 5057
- MySQL - 62228
- Patch Server HTTPS - 6201
- Patch Server HTTP - 3698

Uninstalling Seqrite Endpoint Security server

Uninstalling Seqrite Endpoint Security may expose your systems and valuable data to virus threats. However, if you need to uninstall Seqrite Endpoint Security, follow these steps:

1. Go to **Start > Programs > Seqrite EPS Console > Uninstall EPS Console**.
2. Seqrite Endpoint Security uninstaller will prompt for the password.

Type Super Administrator **Password** in the Password box.

3. Click **Next**.

After the uninstallation, the product key is displayed.

Note down the product key as you might require it when you reinstall Seqrite Endpoint Security. Select **Restart System Now** to restart the system immediately or **Restart system later** to restart the computer after sometime.

4. To complete uninstallation of Seqrite Endpoint Security, click **Finish**.



- If you have assigned a script to install endpoint by Login Script Setup to domain servers, clear it through the Login Script Setup before proceeding with uninstallation.
- Before proceeding with uninstallation, ensure that all other running programs are closed.

You can also uninstall Seqrite Endpoint Security through the Control Panel. Uninstallation will remove Seqrite Endpoint Security client from the endpoint.

About Seqrite Endpoint Security Dashboard

Seqrite Endpoint Security has a Web-based graphical console that displays the current status of the health of endpoints and highlights critical security situations that need immediate attention.

This section explains how to navigate the Web console.

Log on the Seqrite Endpoint Security Web console

To log on the Web console, follow these steps:

1. Select **Start > Programs > Seqrite EPS Console**

Alternatively, you can do the following to log on:

Open the browser on a computer in your network, and do one of the following:

- In the address bar, type the SEPS server name or IP address in the following URL format:
 - For XP: `http://{Seqrite_Endpoint_Security_Server_name or IP address}/qhscan760`
 - For other OS: `http://{Seqrite_Endpoint_Security_Server_name or IP address}:{port number}`
- If your system uses SSL, type the SEPS server name or IP address in the following URL format in the address bar:
 - For XP: `https://{Seqrite_Endpoint_Security_Server_name or IP address}/qhscan760`
 - For other OS: `https://{Seqrite_Endpoint_Security_Server_name or IP address}:{port number}`

Seqrite Endpoint Security Account Login window appears.

2. Type the user name as **administrator** in the **User Name** text box and administrator password in the **Password** text box.
3. Click the **Login** button.

The Web console is displayed with a summary of the current health status of the network.

Resetting the Web console password

You can reset the web console password using any of the following methods:

- Use the 'Forgot Password' link
- Use the Password Reset tool

Resetting the Web console password with Forgot Password link

To reset the Web console password, follow these steps:

1. In the Account Login window, click **Forgot Password** link.
2. In the Reset Password window, enter username.
3. Click the **Send Recovery Email** button to generate temporary password. The Temporary Password will be sent to your registered email ID.
4. In the **Temporary Password** text box, enter the temporary password.
5. Click **Submit**.
6. In the new window, in the **New Password** and **Confirm Password** boxes, type the password to reset your password.
7. Click **Submit**.

You can log on the Web console with new password.



If SMTP settings are not configured, user can reset the password using the Password Reset tool.

Resetting the Web console password with Password Reset tool

To reset the Web console password with Password Reset tool, the user should have administrative privilege on the machine where EPS is installed.

To reset the Web console password, follow these steps:

1. Go to < installation directory>/ Admin/resetpwd.exe. <installation directory> indicates the path where Seqrite Endpoint Security has been installed.
2. Execute the file resetpwd.exe.
3. In the Console Password Reset Tool window, either enter Windows Host name\administrator user and password or you can select hostname\administrator from the drop down list.
4. Click **Next**.
5. In the new window, in the **New Password** and **Confirm Password** boxes, type the password to reset your password.
6. Click **Change Password**.

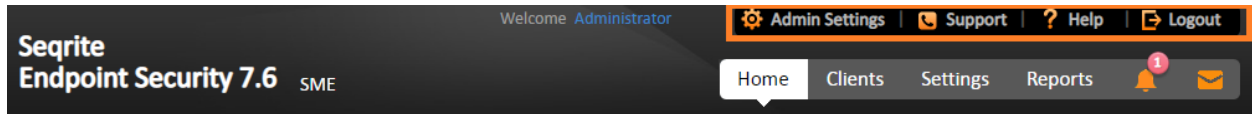
You can log on the Web console with new password.



Number of login attempts allowed are limited to 6. After 6 unsuccessful attempts, the user account will be locked for 6 hours.

Areas on the Web console

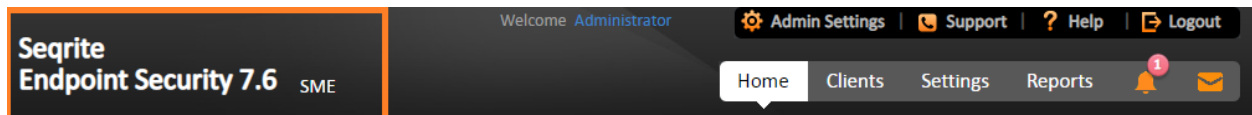
When you log on to Seqrite Endpoint Security console, the Home page is displayed by default. The options that appear on the console are as follows:



The menu bar on the upper-right corner, highlighted in yellow, includes the following options that are common to all pages:

Menus	Description
Admin Settings	Helps you configure the settings related to the features, such as Server and Endpoints.
Support	Helps you find out all the support options that Seqrite provides.
Help	Includes the Help file that provides information about all the features, how they work, and how to configure them.
Logout	With this button, you can log out from the current session.

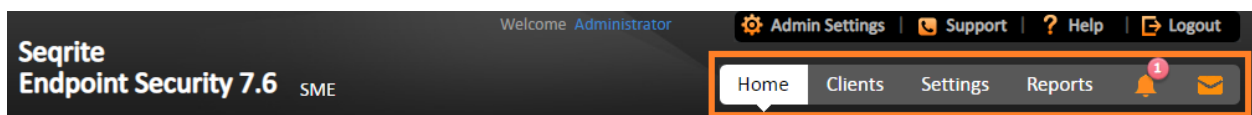
Product name:



The product name section includes the following:

Menu	Description
Product Name and Version	Displays the product name and its current version. The edition name is also displayed.

Tabs:

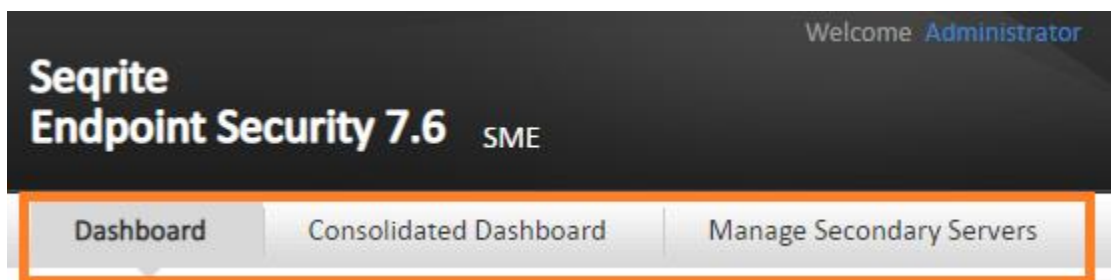


The user interface of the Web console also includes the links to the following pages:

Pages	Description
Home	Helps you visit the Home page, which is the Seqrite Endpoint Security Dashboard.

Clients	Helps you configure the settings related to Endpoint Status and Endpoint Action.
Settings	Helps you configure the settings related to Endpoint Settings and Schedule Settings.
Reports	Helps you generate reports on all the features that you need.
Alerts (Bell icon)	Displays alert messages for the following critical situations: <ul style="list-style-type: none"> • Update Manager not updated • License expired • License limit exceeded • License about to expire • New service pack available • SMS credit limit has been reached to maximum
Messenger	Displays the messages related to security information, new service pack released, new SEPS version released etc.

Ribbon

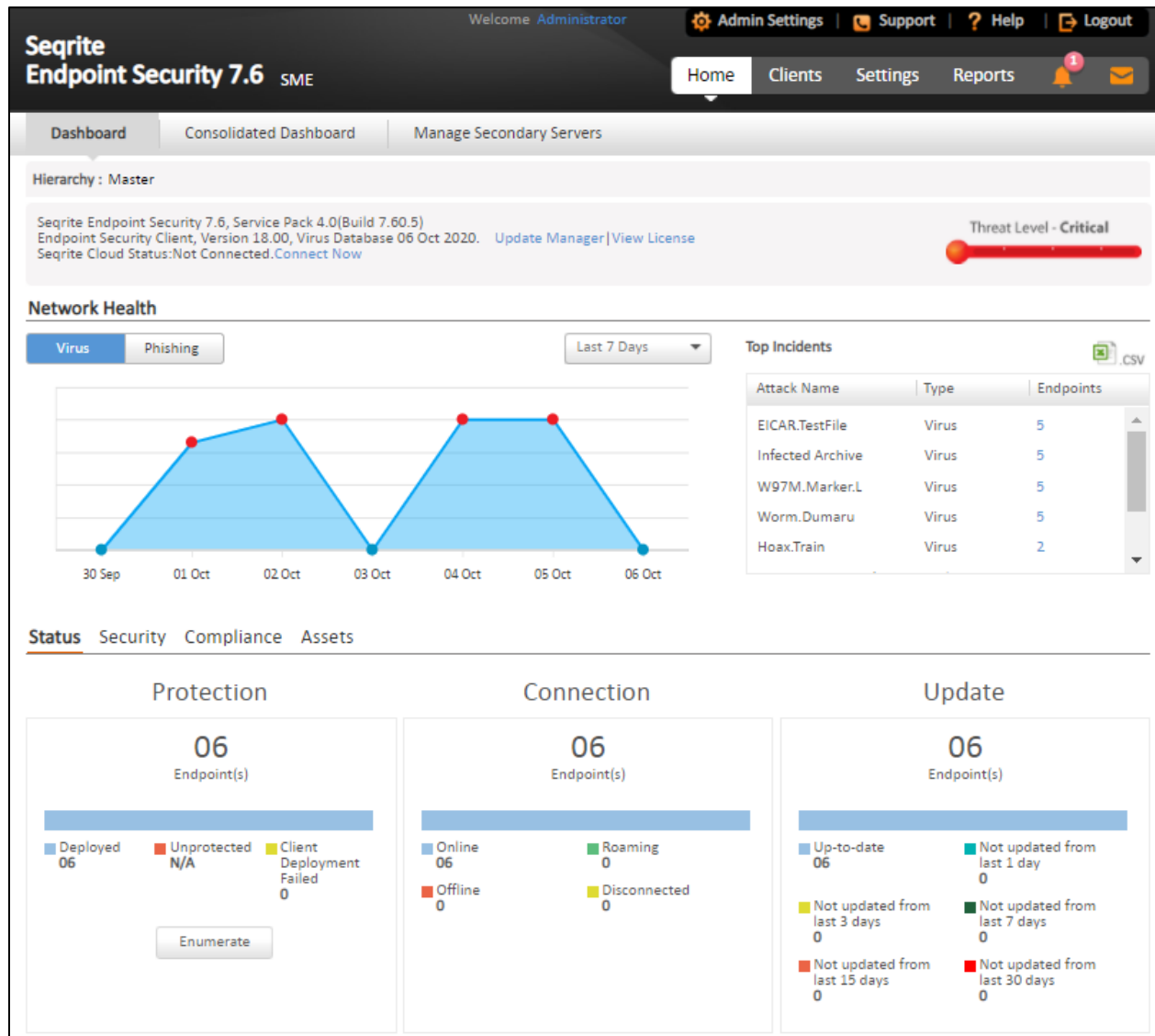


The ribbon on the Web console includes the tabs to the following pages.

If the EPS server is not connected to any Secondary Server, Consolidated Dashboard and Manage Secondary Servers tabs are not visible.

Pages	Description
Dashboard	Helps you visit the Home page, which is the Seqrite Endpoint Security Master Server Dashboard.
Consolidated Dashboard	Helps you visit the Home page, which is the consolidated Dashboard of Seqrite Endpoint Security Master Server and Secondary Servers.
Manage Secondary Servers	Helps you visit the page, to manage all the Secondary Servers.

Dashboard



The Dashboard area on the Home page has widgets for the following:

Overview

Feature	Description
Hierarchy	On the Master server, "Hierarchy" name will be represented as "Master". On the Secondary Server, displays the hierarchy of the Server you have logged on. This shows the names of the parent servers up to Master. Example: Master / Primary001 / Secondary020. In this case, the logged-on Server name is Secondary020 and the parent Server is Primary001, which is reporting to the Master.

Feature	Description
Product version	Displays the product version along with the build number. The build number is useful for troubleshooting purposes. The SEPS service pack information is also available. The virus database date included helps in understanding if your version is updated or whether it needs updates.
Update Manager	Link for running the Update Manager. For more information, see Update Manager .
View license	Displays the links for: <ul style="list-style-type: none"> • Status: Displays currently held licensee information, installation number, product key, product type, validity and the maximum number of the Endpoints permitted. • License order form: Displays the License order form to order new feature/license. • License History: Displays the license history details.
Seqrite Cloud Status	Displays whether the EPS server is connected or not connected to the cloud. If not connected, use the Connect Now link if required. Seqrite Cloud is a different product and is only available for the users who have purchased it additionally.
Threat Level	Displays current threat level of your network. The threat levels include: <ul style="list-style-type: none"> • Normal: Indicates that 12% of the endpoints detected viral infection in last 24 hours. • Elevated: Indicates that 24% of the endpoints detected viral infection in last 24 hours. • High: Indicates that 36% of the endpoints detected viral infection in last 24 hours. • Critical: Indicates that more than 36% of the endpoints detected viral infection in last 24 hours. <p>Important: Thorough scanning of the entire network is recommended if the threat level alert is High or Critical.</p>
Alert	An alert appears if the health of the network needs an immediate action. Click the More link to see all the alerts. (The More link is displayed only if multiple alerts are available.) You can take appropriate action to fix the issue.
Seqrite Encryption Manager	Seqrite Encryption Manager (SEM) is a different product. If SEM server is installed on the same system, then only this option appears. Displays the name of Seqrite Encryption Manager with version. Click the View Console link to access the Seqrite Encryption Manager console.

Network Health

Feature	Description
Network Health	<p>Graphical representation of the network health for the categories of Virus and Phishing. Click the respective tab to get the details of that category. It shows how secure your system is currently. This status is displayed over a 4-level grid by colored dots that are in ascending level with green at the lowest level and red at the highest level. These colored dots indicate the following:</p> <ul style="list-style-type: none"> • Green (Normal): Indicates endpoint is not infected and is secure. • Yellow (Elevated): Indicates low level of endpoint infection. • Orange (High): Indicates high level of endpoint infection that requires immediate action. • Red (Critical): Indicates critical level of endpoint infection that requires immediate action. <p>The right pane carries a table with Top Attacks, the type and the total number of endpoints affected.</p>
View for drop down list	<p>Gives a graphical representation of the network health for the selected time period. The graphs can be viewed for the following time periods:</p> <ul style="list-style-type: none"> • Past 7 Days: Displays the report of the last seven days. • Today: Displays the report of the today's infection. • Past 15 Days: Displays the report of the last 15 days. • Past 30 Days: Displays the report of the last 30 days.
Top Incidents	<p>Displays the top 10 incidents on computers by Attack Name, type, and number of endpoints infected. Clicking on the endpoint count, opens a window with details of the actual endpoint infected. You can save the top incidents report of Virus and Phishing in the csv format.</p> <p>If the client is removed or uninstalled after the incident, the updated Endpoint count is reflected after next Client-Server communication cycle.</p>

Status

Feature	Description
Status Tab	<p>Displays the information for the following categories:</p> <ul style="list-style-type: none"> • Protection • Connection • Update
Protection	<p>Displays the number of endpoints deployed in the network, unprotected endpoints across your network, and the endpoints on which deployment of any client has failed.</p>

Connection	Displays the total number of connections registered to the system with the break-up for online, offline, disconnected, and roaming endpoints. It also displays information about offline, disconnected, roaming endpoints, and when they were last connected to the computer.
Update	Displays the number of endpoints on which the virus definitions are not updated from last 1, 3, 7, 15 and 30 days. Click the number under the category. An update Status dialog appears showing a list of the Endpoint name, Domain, IP address, and Virus Database date. You can select the number of days to view the list of endpoints which are not updated. This filter helps you to select in between days of the categories. This status can be exported in the csv format.
Enumerate	Click Enumerate to generate a list of all the unprotected endpoints connected to the network. Note: This may take some time and a link to a list of all these endpoints with their endpoint name, domain name, and operating system platform name will be displayed.

Security

Feature	Description
Security Tab	Displays the protection status for the following: <ul style="list-style-type: none"> • Virus protection • Phishing protection • Browsing Protection
Web Security	Displays the information for top 5 Web site categories, which were blocked in past 7 days in graph and a list of the top 5 Web sites, which were blocked in past 7 days in a table with URL, Type, and Count columns. Note: This feature is optional and will be visible only if you have purchased the license for Web Security feature. For more information, see Web Security .
Data Loss Prevention	Displays the number of data leak attempts over the last 7 days and a list of the top users who were trying to leak the data. Note: This feature is optional and will be visible only if you have purchased the license for DLP feature. For more information, see Data Loss Prevention .
Vulnerabilities	Displays the number of affected endpoints and a comparative list of the top vulnerabilities, severity level, and the total number of vulnerabilities detected. Also, displays a graphical widget for the listed data.
Patch Management	Displays the number of missing patches by severity. In Patch scan overview section, you can view status of patch scan for the selected date. Select the date from the calendar and click Submit . This gives

	<p>a doughnut chart which displays the number of endpoints with missing patches, endpoints not scanned, and up to date Endpoints.</p> <p>The Number of endpoints with missing patches as per application family section gives a doughnut chart which displays the number of endpoints with missing patches of top 5 application families. Clicking the count, opens a window with details of patch scan result.</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Compliance

Feature	Description
Advanced Device Control	Displays the information for top device types that breached the policies in the past 7 days and a list of top 5 users, who breached the policy, specifying their user name, endpoint name, and the count of breaches.
Application Control	Displays the information for top applications that were blocked in the past 7 days and a list of top 5 users who attempted to access the blocked applications specifying their user name, endpoint name, and count.

Assets

Feature	Description
Hardware changes	Displays the number of hardware changes detected on SEPS 7.6 endpoints.
Software changes	Displays the number of software changes detected on SEPS 7.6 endpoints. Clicking the count, opens a window with details of software changes, i.e. Software installed, uninstalled and updated.
Platforms	Displays the total number of endpoints installed on a platform. Click the columns in the bar graph to display extended information related to a specific category. The endpoint IP address is displayed along with the platform on which it was installed.
Software Installed	Displays the number of endpoints on which software have been installed. This display is also in the form of a bar graph which can be toggled to display the number of software least installed v/s the number of software most installed. Click the columns in the bar graph to display more information related to the category. The endpoint IP address is displayed along with the software name.

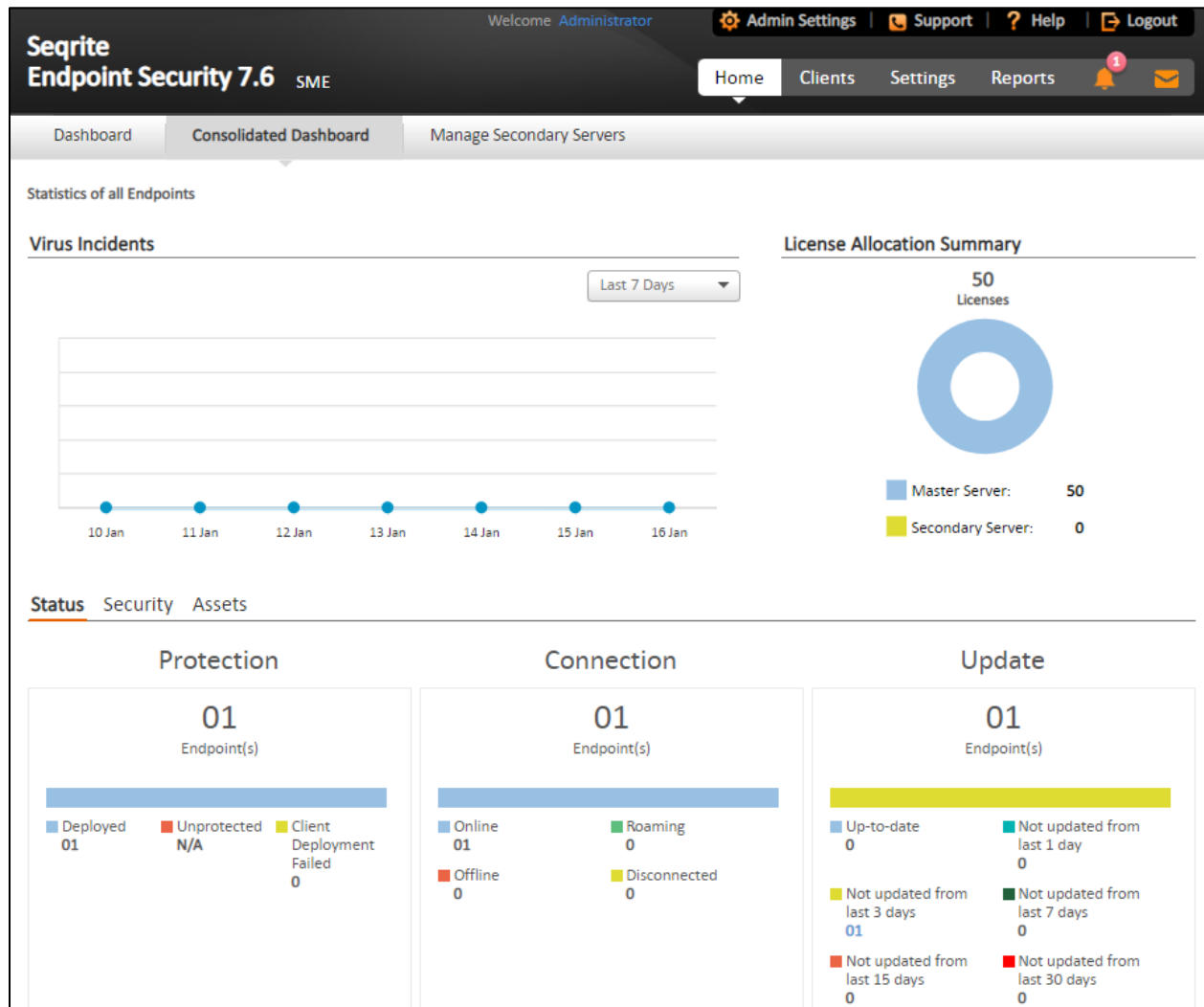
CTA Banner - GoDeep.AI

A Call to Action (CTA) banner of GoDeep.AI is displayed in the footer of the page. GoDeep is Artificial intelligence (AI) enabled Deep Predictive Malware Hunting Technology using Advance Machine Learning. Click **KNOW MORE** on the banner for more information.

Consolidated Dashboard

The data on this page is consolidated, data of the main server and data of all the secondary servers.

If the EPS server is not connected to any Secondary Server, Consolidated Dashboard page is not visible.



Virus Incidents

Feature	Description
Virus incidents	<p>Gives a graphical representation of the virus incidents for the selected time period. The graphs can be viewed for the following time periods:</p> <ul style="list-style-type: none"> Past 7 Days: Displays the report of the last seven days. Past 15 Days: Displays the report of the last 15 days. Past 30 Days: Displays the report of the last 30 days.

	<p>This status is displayed over a 4-level grid by colored dots that are in ascending level with green at the lowest level and red at the highest level. These colored dots indicate the following:</p> <ul style="list-style-type: none"> • Green (Normal): Indicates endpoint is not infected and is secure. • Yellow (Elevated): Indicates low level of endpoint infection. • Orange (High): Indicates high level of endpoint infection that requires immediate action. • Red (Critical): Indicates critical level of endpoint infection that requires immediate action. <p>The Virus Incidents summary does not change if the client is removed or uninstalled after the incident.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

License Allocation Summary

License Allocation Summary	Gives a doughnut chart which displays the total number of licenses held by the Master Server and the Secondary Servers.
----------------------------	-------------------------------------------------------------------------------------------------------------------------

Status

Feature	Description
Status Tab	<p>Displays the information for the following categories:</p> <ul style="list-style-type: none"> • Protection • Connection • Update
Protection	Displays the number of endpoints deployed in the network, unprotected endpoints across your network, and the endpoints on which deployment of any client has failed.
Connection	Displays the total number of connections registered to the system with the break-up for online, offline, disconnected, and roaming endpoints. It also displays information about offline, disconnected, roaming endpoints, and when they were last connected to the computer.
Update	<p>Displays the number of endpoints on which the virus definitions are not updated from last 1, 3, 7, 15 and 30 days.</p> <p>Click the number under the category. An update Status dialog appears showing a list of the Endpoint name, Domain, IP address, and Virus Database date. You can select the number of days to view the list of endpoints which are not updated. This filter helps you to select in between days of the categories. This status can be exported in the csv format.</p>

Security

Feature	Description
Security Tab	Displays the protection status for the following for last 7, 15 and 30 days: <ul style="list-style-type: none"> • Virus protection • Phishing protection • Browsing Protection
Web Security	Displays the information for top 5 Web site categories, which were blocked in past 7 days in graph and a list of the top 5 Web sites, which were blocked in past 7 days in a table with URL, Type, and Count columns. Note: This feature is optional and will be visible only if you have purchased the license for Web Security feature. For more information, see Web Security .
Data Loss Prevention	Displays the number of data leak attempts over the last 7 days and a list of the top users who were trying to leak the data. Note: This feature is optional and will be visible only if you have purchased the license for DLP feature. For more information, see Data Loss Prevention .
Vulnerabilities	Displays the number of affected endpoints and severity level in the percentage format. It also displays a graphical widget for Vulnerability Severity. A link View details helps you to view Vulnerability Severity details.
Patch Management	Displays the number of missing patches by severity.

Assets

Platforms	Displays the total number of endpoints installed on a platform. Click the columns in the bar graph to display extended information related to a specific category. The endpoint IP address is displayed along with the platform on which it was installed. Note: This feature is applicable to all endpoints for Windows, Linux, and MAC operating systems.
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Manage Secondary Servers

This page displays status of all the Secondary Servers under the Master Server. You can edit or delete the Secondary Server.

If the EPS server is not connected to any Secondary Server, Manage Secondary Servers page is not visible.

Master and Secondary Server

Master Server is the EPS server that can manage local clients and Secondary Servers installed in different locations.

A Secondary Server is a type of server that serves as an addition to the Master Server. The Secondary Server has the same features and capabilities as the Master Server. It can be installed at different locations. It manages local clients, and it reports important statistics to the Master Server.

Benefits of Secondary Server

With the help of the Secondary Servers, you can manage a large number of endpoints. If the network is distributed in geographical different areas, the Secondary Server plays an important role. For each location, you can have a Secondary Server, which manages all the endpoints at that location. All the Secondary Servers are managed by one Master Server.

In EPS 7.6, Master and multi-level Secondary Server architecture can be used. As per your geographical locations, multiple and multi-level Secondary Servers are possible as per your requirement.

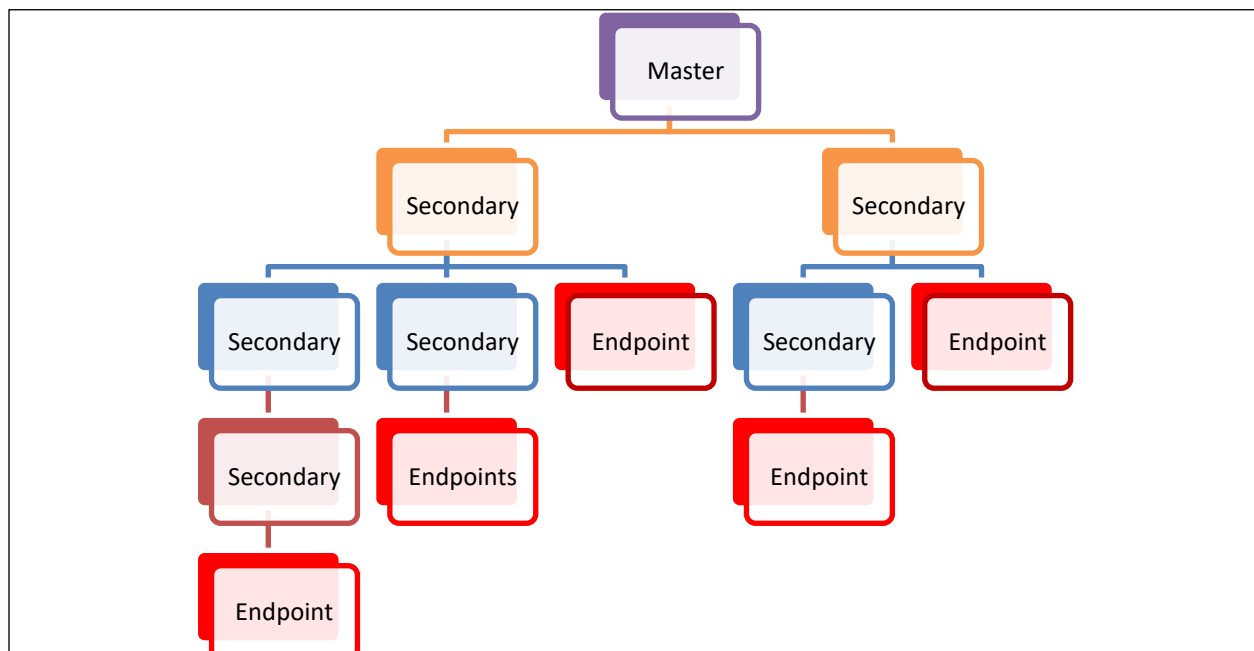


Figure: Example of Master and multi-level Secondary Server architecture

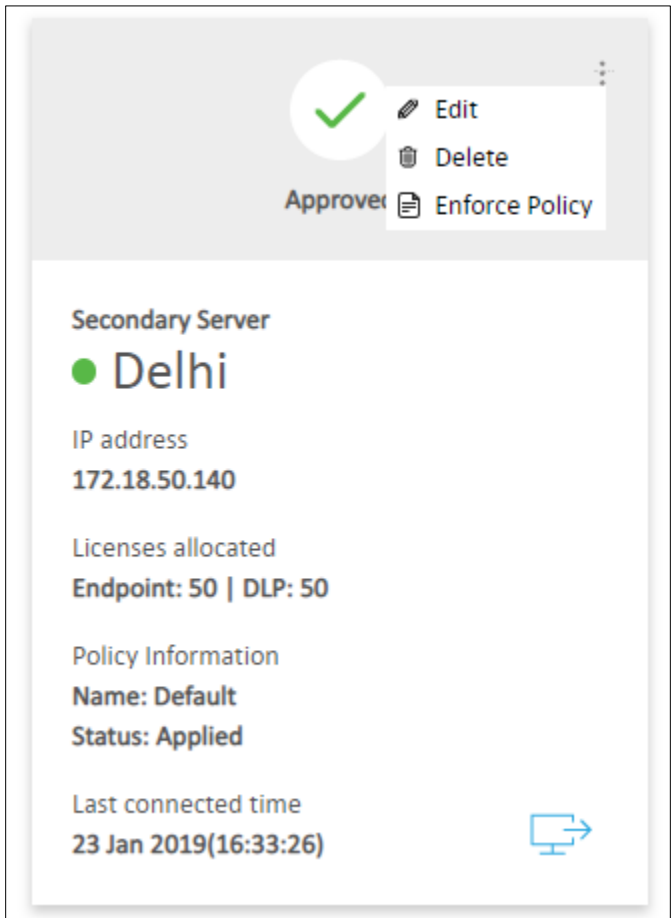
Installing the Secondary Server

1. While installing Seqrite Endpoint Security server, you can select whether you want to install the Master Server or Secondary Server. Remaining installation steps remain the same for both types of server. For more info, see [Installing Seqrite Endpoint Security server](#).
2. After you install the Secondary Server, on the Home page, go to Manage Secondary Servers tab. The cards of the installed Secondary servers appear.
3. Click **Approve** to assign the licenses and policy.
4. The Assign Policy & License dialog opens. Select the policy from the list.
5. Enter number of Endpoints and DLP licenses.

6. Click **Submit & Approve**.

Viewing information of the Secondary Servers

The information of the Secondary Servers is displayed in the card format. Each card represents one Secondary Server.



The card displays the following information,

Feature	Description
Status	Displays one of the following status of the Secondary Server, <ul style="list-style-type: none">• Approved• Approval Pending• Deny• Red dot indicates status is offline. If the last connected time of Secondary server with the Master/parent server exceeds 2 hours, the status is shown as offline.• Green dot indicates online status

Secondary Server	Displays name of the Secondary Server.
IP address	Displays IP address of the Secondary Server.
Licenses allocated	Displays number of EPS licenses and number of DLP (Data Loss Protection) licenses.
Policy Information	Displays the following information about the policy assigned to the Secondary Server: Name – name of the policy Status – status of the policy, either Approved or pending
Last connected time	Displays date and time when the Secondary Server is last connected to the Master Server.
Edit	You can edit the information about the Secondary Server with help of the Edit option in the ellipsis icon.
Delete	You can delete the Secondary Server with help of the Delete option in the ellipsis icon.
Enforce Policy	You can enforce the policy on the Secondary Servers with help of the Enforce Policy option in the ellipsis icon. At the Secondary Server, the enforced policy is applied to the default group and its secondary servers if present.
Go to Server	This icon redirects you directly to the home page of the Secondary Server.

Managing the Secondary Server

You can edit or delete the secondary server with help of the options in the ellipsis icon. You can also enforce a policy on the Secondary Server.

Editing the Secondary Server

To edit the Secondary Server, follow these steps:

1. On the Home page, go to **Manage Secondary Servers** tab. The cards of the installed Secondary servers appears.
2. Click **Edit** from the ellipsis icon at the right corner.
3. The Edit Server Details dialog opens. You can edit the following,
 - Name of the Secondary Server
 - Assigned policy to the Secondary Server –
If you change the policy, a confirmation message is displayed. Click **Yes** to enforce the policy on the Secondary Server.
 - Number of Endpoint licenses or DLP licenses

4. Click **Submit**.

To delete the Secondary Server, follow these steps:

1. On the Home page, go to **Manage Secondary Servers** tab. The cards of the installed Secondary servers appears.
2. Click **Delete** from the ellipsis icon at the right corner.
A confirmation message is displayed.
3. Click **Yes**.

The Secondary Server is deleted.

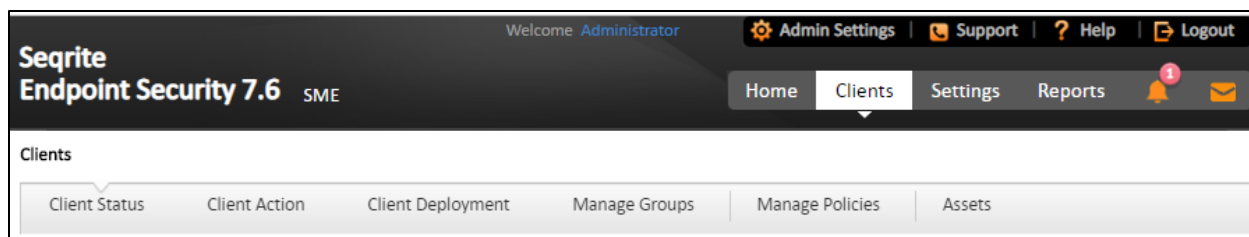
To enforce the policy on the Secondary Server, follow these steps:

1. On the Home page, go to **Manage Secondary Servers** tab. The cards of the installed Secondary servers appears.
2. Click **Enforce Policy** from the ellipsis icon at the right corner.
A confirmation message is displayed.
3. Click **Yes**.

The policy is enforced on the Secondary Servers.

Clients

The Clients page includes features that help you manage and control all the clients deployed in the network. You can verify the current status of the clients and carry out various activities. You can scan endpoint computers, update the software application, improve system performance, install, and uninstall Seqrite Endpoint Security Client remotely. You can also manage endpoint groups, create and apply scanning policies, etc.



The following features are available in the Clients tab as shown in the above screen:

- Client Status
- Client Action
- Client Deployment
- Manage Groups
- Manage Policies
- Assets

Client Status tab

Client Status tab gives the current status of all the endpoints in the network. The status includes information such as the endpoint name, group name, domain name, IP and MAC addresses. The tab also shows protection status, installation status, product version, virus database date, last scan date, protection policies among others, and the enabled security features.

To view the Client Status, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Status**.
3. In the left pane, under EPS Console, select a group name.

In the right pane, all the endpoints of a relevant group are displayed.

4. Select an endpoint and click **View Status**.

The status of the selected endpoint appears.

The View Status window appears. The status of the selected endpoint is shown. If client is not installed on any endpoint, the **View Installer Log** link appears in Product name row.

Click the **View Installer Log** link to view the Client Installer log. You may find the reason why a client is failed to deploy.

You can select multiple endpoints at a time to remove offline clients.

You can either export the status or take a print if required.

Terms	Definition
Show endpoints within subgroup	Helps you view endpoints that are in a subgroup.
View Status	Helps you view the status of the clients.
Remove Client	Helps you remove an offline client from a group.
Search	Helps you search the client by endpoint name.
CSV	Helps you save the report in csv format.

Client Action tab

Using the features on the Client Action tab you can scan endpoints remotely, update virus definitions, and improve performance of the endpoints. You can also verify the compliance to security policies, for e.g. identifying unauthorized applications installed on any of the endpoints in the network.

You can remotely scan individual endpoints or endpoints in a group, customize scan settings, and stop scanning as per your preference. You can improve the performance of your endpoints by cleaning up disk space, registry entries, and schedule defragmentation at next boot. You can update the SEPS virus database for the endpoints and verify security compliance if any unauthorized applications are installed on any endpoints.

The following table shows a comparison of the features in Client Action that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Scan	✓	✓	✓
Update	✓	✓	✓
Data-At-Rest Scan	✓	✓	X
Temporary Device Access	✓	✓	X
Tuneup	✓	X	X
Application Control Scan	✓	X	X
Vulnerability Scan	✓	X	X

Patch Scan	✓	X	X
Patch Install	✓	X	X
Delete Backup Data	✓	X	X

Scan

This feature allows remote scanning of any endpoint in the network. You can initiate a manual scan with preconfigured policies. This feature reduces the additional task of personally overseeing each target endpoint.

To initiate scanning, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Scan**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to that group.

3. Under EPS Console, select a group.

In the right pane, all the endpoints of a relevant group are displayed.

4. To initiate scanning, click **Notify Start Scan**.

The selected endpoints are scanned for compliance.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps you display the endpoints that are in a subgroup.
Scan Settings	Helps you customize scan settings.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Scan Settings

This feature allows you to customize the scan settings for a client machine.

To configure Scan settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Scan**.
3. On the Scan screen, click **Scan Settings**.

4. On the Scan Settings screen, carry out the following actions:

- i. In How to Scan section, select either Quick Scan or Full System Scan.

Quick Scan includes scanning of the drive where operating system is installed, and Full System Scan includes scanning of all fixed drives.

- ii. The **Scan Priority** is **Normal** by default. You can change the priority if required.
- iii. Select either **Automatic** or **Advanced** scan mode.

Automatic scanning involves optimum scanning and is selected by default.

- iv. When the **Advanced scan mode** check box is selected, all the related attributes get enabled. You can carry out the following actions:
 - a. From the Select the items to scan options, select the files, file types (executable files, packed files, archive files), and the mailboxes that you want to scan.
 - b. In **Archive Scan Level**, set the scan level.

You can set the level for scanning in an archive file. The default scan level is 2. Increasing the default scan level may affect the scanning speed.
 - c. To remove an infected file from your system follow these steps in the Select action tab:
 - If an infected file is found in an archived folder on your system, select whether you want to delete, quarantine, or skip the file.
 - If an infected file is found in your active folder/drives on you system, select whether you want to repair, delete, or skip the file.
- v. Under Antimalware Scan Settings, select **Perform Antimalware scan** if required.
- vi. In Select action to be performed when malware found, select an action from the following:
 - Clean
 - Skip

The action selected here will be taken automatically.
- vii. Under Boot Time Scan Settings, select **Perform Boot Time Scan**.

The Select Boot Time Scan Mode option is activated.
- viii. Select one of the following scan options:
 - Quick Scan
 - Full System Scan

The setting for Boot Time Scan is applied only once and is not saved.

This will schedule boot time scan on the endpoints. Boot time scan will be executed whenever the endpoint system restarts.
- ix. After configuring the scan setting, click **Apply**.

The new setting is applied.



- Scan packed files, Scan mailboxes, Antimalware Scan Settings, and Boot Time Scan Settings are available only in the clients with Windows operating systems.
- Notification for Scan from SEPS Web console will not be sent if the user is not logged on to the Mac system.
- SEPS scan notification, supports only 'ext' file system in the Linux operating system.

Update

Using this feature, you can update the client applications on any endpoint in the network remotely. Seqrite releases updates regularly to fix technical issues and provide protection against new threats. Hence, it is recommended that you update the virus definitions of your software protection regularly. Also, you can rollback Seqrite to previous state.

To take the update, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Update**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to that group.

3. Under EPS Console, select a group.

In the right pane, all the endpoints of a relevant group are displayed.

4. Select an endpoint and then click **Notify Update Now**. The selected endpoints are updated with the latest virus definitions.

To rollback Seqrite to the previous state, click **Notify Rollback Now**.

Terms	Definition
Select endpoints with out-of-date Seqrite	Helps you update endpoints with outdated virus definitions.
Show endpoints within subgroup	Helps you display endpoints that are in a subgroup.
Notify Update Now	Helps you notify endpoints to update Seqrite.
Update All	Helps you update all the endpoints with a single click of the button.
Notify Rollback Now	Helps you notify endpoints to rollback Seqrite to previous state.
Refresh	Updates the status of sent notifications.



- Notification for update from SEPS Web console will not be sent if the user is not logged on to the Mac system.

- The Rollback feature is applicable only for the clients with Microsoft Windows operating system.

Tuneup

This facility improves the performance of the endpoints by defragmentation and by cleaning unwanted and junk files and invalid and obsolete registry entries. While you work in applications, computers write junks on the drives or when you visit Websites, temporary files are created on your computer. Such junks and files occupy spaces in the memory resulting in slowing down of the endpoints. Tuning up your computers cleans up these files improving their performance.



- The Tuneup feature is available only in the clients with Windows operating systems.
- The Tuneup feature is not available for Windows Server operating system.

To tune up the endpoints, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Tuneup**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to the group.

3. Under EPS Console, select a group for which you want to perform the tune up process.

By default, it shows all the endpoints present under the EPS console.

In the right pane, all the endpoints of a relevant group are displayed.

4. Select an endpoint and then click **Notify Start Tuneup**.

Tuneup notifications are sent to the selected endpoints and tune up is performed on those endpoints.

You can stop Tuneup activity by clicking Notify Stop Tuneup at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps you display those endpoints that are in a subgroup.
Tuneup Settings	Helps you customize Tuneup settings.
Notify Start Tuneup	Helps you notify the clients to start Tuneup.
Notify Stop Tuneup	Helps you notify the clients to stop Tuneup.
Refresh	Updates the status of the sent notifications.
Tuneup All	Helps you tune up all the endpoints with a single click of the button.

Tuneup Settings

These settings allow you to carry out different types of cleanups such as; disks, registry entries, or schedule a defragmentation at next boot.

To customize Tuneup settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Tuneup**.
3. On the Tuneup screen, click the **Tuneup Settings** button.
4. On the Tuneup Settings popup, select any of the following:
 - Disk Cleanup
 - Registry Cleanup
 - Defragment at next boot

However, all these options are selected by default.

5. To save your settings, click **Apply**.

Disk Cleanup: Helps you find and remove invalid and unwanted junk files from the hard disk. These files consume hard disk space and slow down the system considerably. Disk Cleanup deletes these files and provide free space that can be used for other applications and helps in improving system performance. This feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files, and empty folders.

Registry Cleanup: Helps you remove invalid and obsolete registry entries from the system, such entries may appear due to improper uninstallation, non-existent fonts, etc. Sometimes during uninstallation, the registry entries are not deleted. This leads to slower performance of the system. The Registry Cleanup removes such invalid registry entries to increase the performance of the system.

Defragment: Helps you defragment vital files, such as page files and registry hives for improving the performance of the system. Files are often stored in fragments in different locations slowing down the system performance. Defragment reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve system performance.

Application Control Scan

Allows you to check whether security compliance policies framed by your organization are being followed on each endpoint. It also helps you in verifying whether endpoints have any unauthorized applications other than the authorized ones running on them.



The Application Control Scan feature is available only in the clients with Windows operating systems.

To scan endpoints for compliance control, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.

2. Go to **Clients > Client Action > Application Control Scan**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to the group.

3. Under EPS Console, select a group.

In the right pane, all the endpoints of a relevant group are displayed.

4. With the Scan Settings button, select your scan setting.

5. Select an endpoint and then click **Notify Start Scan**.

The selected endpoints are scanned for compliance.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for application control.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Scan Settings

This feature helps you customize your scan preference.

To customize Scan Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Application Control Scan**.
3. On the Application Control Scan screen, click the **Scan Settings** button and then select one of the following:
 - **Unauthorized applications:** Helps you initiate scanning only for the unauthorized applications present on a client machine.
 - **Unauthorized and authorized applications:** Helps you initiate scanning for both, unauthorized and authorized applications present on the client machine.
 - **All installed applications:** Helps you initiate scanning for all applications installed on a client.

You can select any one of the options for application control scan.

Scanning by first two options may take longer time.

4. The Scan Priority is Normal by default. You can change the priority if required.
5. To save your settings, click **Apply**.

Vulnerability Scan

This feature allows you to scan the known vulnerabilities in the installed applications of various vendors such as; Adobe, Apple, Mozilla, Oracle etc. and the operating systems on the endpoints in your network and assess their security status. You can probe the endpoints for applications and operating system patches for possible vulnerabilities. This is helpful to create security measures against the known vulnerabilities and secure the endpoints against data outage.

To enable Vulnerability Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Vulnerability Scan**.
3. On the Vulnerability Scan page, click the **Scan Settings** button.

The Scan Settings dialog appears.

4. Under Scan for vulnerability against following software vendors, select one of the following options:
 - Microsoft applications and other vendor applications
 - Microsoft applications only
 - Other vendor applications only
5. To save your settings, click **Apply**.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for Vulnerability Scan.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Data-At-Rest Scan

Using Data-At-Rest Scan, you can scan and detect any confidential data present in your endpoints and removable devices. You can scan the desired location such as; drive, folder, or removable devices on the endpoints and detect the confidential or sensitive information

present. You can view the information related to the detected confidential data such as; the file path, threat type, and matched text.



To perform Data-At-Rest scan, you must enable DLP on the endpoints. To enable DLP on the endpoints, see [Enabling DLP feature](#).

Scan Settings

To enable Data-At-Rest Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Data-At-Rest Scan**.
3. Enter the endpoint name or IP address that you want to scan or select from the default list.

You can also select an endpoint from a particular group.

You may also select the required check box provided at the end of the page if you want to select an offline client or endpoint within a subgroup or both.

4. Click the **Scan Settings** button and select one of the following:
 - **Quick Scan:** Select this option to scan the drive on which your operating system is installed.
 - **Full System:** Select this option to scan all the drives.
 - **Scan Specific Folder(s):** Select this option to scan a particular folder(s).
 - i. Click **Configure**.
 - ii. Enter the path of the folder that you want to scan.
 You can also choose to scan the subfolders by selecting the **Include Subfolder** check box.
 - iii. Click **Add**.
 You can also remove a path from the list by clicking **Remove**.
 - iv. Click **Apply**.
5. The Scan Priority is Normal by default. You can change the priority if required.
6. From the File Types list, select the file format that you want to search for the data.
7. Select either **Confidential Data** or **User Defined Dictionaries** or both for the type of data that you want to scan.
8. Click **Apply**.

Clicking **Cancel**, closes the dialog box and clicking **Default**, clears all the selections.



- Email Notifications are not supported for Data-At-Rest Scan feature.
- Data-At-Rest Scan feature will be available only if DLP feature pack is enabled for that EPS server.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for Data-At-Rest Scan.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Exclusion

You may exclude or include a path for scanning.

- To exclude, enter the path in the text box and click **Add**.
- To include, select the path in the text box and click **Delete**.

Patch Scan

This feature allows you to scan the missing patches in the network.

To enable Patch Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Patch Scan**.
3. Click the **Scan Settings** button and select one of the following options:
 - **Online (Recommended)**
The client accesses latest data from the patch server during missing patch scan.
 - **Offline**
The client accesses data from the local system during missing patch scan.
4. Click **Apply**.
5. Enter the endpoint name or IP address that you want to scan or select from the default list.
You can also select an endpoint from a particular group.
You may also select the required check box provided at the end of the page if you want to select an offline client or endpoint within a subgroup or both.
6. Select an endpoint and then click **Notify Start Scan**.
The selected endpoints are scanned for missing patches.



Seqrite recommends to select 100 endpoints at a time for patch scan to have optimal performance.

You can stop scanning by clicking **Notify Stop Scan** whenever you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for the patch scan.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.

Patch Install

This feature allows you to install the missing patches on the selected endpoints.

To install the missing patches, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Patch Install**. Patch Install page appears. A list of the missing patches appears.
3. You can filter the list with the help of the four filters described in the following tables:

Severity options:

Severity	Description
Critical	Vulnerability may allow code execution without user interaction.
Important	Vulnerability may result in compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	Vulnerability may result in random malfunctions.

Category options:

Category	Description
Security Updates	A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
Update Rollups	A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product, such as Internet Information Services (IIS).
Applications	Application (software) is a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.
Service Packs	A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.
Feature Packs	New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
Updates	Updates are code fixes for products that are provided to individual customers when those customers experience critical problems for which no feasible workaround is available.
Definition Updates	A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.
Critical Updates	A widely released fix for a specific problem that addresses a critical, non-security-related bug.
Drivers	Software that controls the input and output of a device.

Restart Required options:

Restart Required	Description
All	Display result for all the options.
Not Required	The patch does not require the system restart.

Required	The patch requires the system restart. Restart the system to take the patch effect.
May Require	The patch may require the system restart.

EULA Status options:

EULA Status	Description
All	Display result for both the options, Accepted and Not Accepted.
Accepted	End User License agreement is accepted.
Not Accepted	End User License agreement is not accepted.

You can provide endpoint name or an application name to generate the specific result. You can search the patches by entering KB ID or Bulletin ID.

To generate the result with help of filters and/or record details, click **Generate**.

4. Select the **Show patches within subgroup** check box to display the name of the patches that are in the subgroup from the list of the endpoints without actually exploring the network.
5. To change the restart setting, click **System Restart Settings** button. Restart settings are applicable only if the patch requires the system restart.
6. Select the **Allow auto-restart the system** check box to restart the system automatically. Clear the check box to restart the system manually.
7. From the missing patches list, select the patches that you want to install.
 - i. In the list, click the number in the column **No. of Endpoint Affected**. Endpoint(s) affected dialog appears.
 - ii. Select the endpoints where you want to install the missing patch.
 - iii. Click **Apply**. The list of endpoints is saved. The count in the column **No. of Endpoint selected** is updated.
8. Click **Start Install**. To cancel the selection, click **Refresh**.
9. To exclude endpoints from installing patches, click the **click here** link. Exclusion for Patch Install dialog appears.
10. Select the **Exclude endpoints having Server OS in an EPS network** check box if required.
11. Select the **Exclude below endpoints** check box.
12. To exclude a particular endpoint, enter the endpoint name or IP and then click **Add**.
13. Click **Apply**.

To remove the exclusion, select the endpoint and then click **Remove**.

Temporary Device Access

This feature allows you to permit temporary access to a device on the client for a specific period. If a user wants temporary access to a device on the client, he can send a request to the Administrator for temporary access. An OTP is generated and shared. The client uses this OTP to access the device for the specific period.

To enable Temporary Device Access, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Temporary Device Access**.
3. On the Temporary Device Access page, select the endpoint client which requires temporary access. Only one endpoint can be selected at a time.
4. Click **Allow Temporary Access**. The Generate OTP dialog appears.
5. In the **Allow temporary access for** list, select minutes.
6. In the **Use OTP within** list, select minutes.
7. Click **Generate**. The OTP appears. When the client is online, click **Notify** and the OTP is automatically received by the client. Temporary access is allowed as per the settings effective from that minute.
8. If the client is offline or roaming, Notify is disabled. To send the OTP manually, by Email to the client, do the following:
 - i. Click **Notify By Mail**. Mail dialog appears.
 - ii. In the **To** text box, enter Email ID.
 - iii. Click **Send Mail**. Default mail client of the system opens and displays a mail specifying the details of the OTP.
 - iv. Click **Send**.

At the client side, after successful validation of the OTP, temporary device access is enabled for the specific period.

Delete Backup Data

Seqrite EPS takes a backup of all your important and confidential files present on the endpoint automatically and periodically (multiple times a day). For more information, refer [General Settings>Data backup](#).

Here you can delete the old or current data backup of the selected endpoints.

To delete backup data, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Delete Backup Data**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to that group.

3. Under EPS Console, select a group.

In the right pane, all the endpoints of a relevant group are displayed.

4. To delete backup data taken to protect from a ransomware attack for the selected group, click **Notify Delete Backup**.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps you display the endpoints that are in a subgroup.
Delete Settings	Helps you customize settings to delete the backup data.
Notify Delete Backup	Helps you notify the clients to delete old backup data.
Refresh	Updates the status of sent notifications.

Delete Settings

This feature allows you to customize the settings to delete the backup data for a client machine.

To configure delete settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Action > Delete Backup Data**.
3. On the Scan screen, click **Delete Settings**.
4. On the Delete Settings screen, select either **Old Backup Data** or **Current Backup Data**. By default, Old Backup Data is selected.
5. Click **Apply**.

Client Deployment

The Client Deployment tab on the Clients page helps you to deploy the Endpoint Security client. Select one of the following methods to deploy the Endpoint Security client as applicable. A brief about each method is mentioned below.

- Through Active Directory: Sync with Active Directory groups to deploy Endpoint Security client.
- Remote Install: Install Endpoint Security client remotely.
- Notify Install: Send e-mail notification containing URL to client Installation.
- Client Packager: Create client installer for manual installation.
- Login Script: Assign login script for client installation.
- Disk Imaging: Deploy Endpoint Security clients through imaging.

The following table shows support of different operating systems related to client deployment methods:

Features	Clients		
	Windows	Mac	Linux
Through Active Directory	✓	X	X
Remote Install	✓	✓	X
Notify Install	✓	✓	X
Client Packager	✓	✓	✓
Login Script	✓	X	X
Disk Imaging	✓	X	X
Remote Uninstall	✓	✓	✓

Through Active Directory

This feature helps you synchronize the SEPS server with Active Directory groups. After you synchronize the group, the clients will get installed on all the endpoints which come under your domain network. A periodic check is carried out to find if any new endpoint is added to your

network. When a new endpoint is added, the client gets automatically installed on that endpoint.

You can also exclude certain endpoints from the Active Directory group so that the client is not installed on these endpoints.



- This installation method is available only with Microsoft Windows operating system.
- To synchronize the server with Active Directory, the console should be installed on the domain machine or should be a member of the domain.
- Synchronization cannot be done with Default group.
- Groups shown in red color are already synchronized with Active Directory.
- The user should have permissions of Domain Admins to synchronize with Active Directory.
- The default synchronization time interval is GLOBAL.

Synchronizing with Active Directory

To synchronize Active Directory groups, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Through Active Directory**.

A window appears with all the groups.

3. Under EPS Console, select a group.

In the right pane, Active Directory Container and Synchronization Interval of the selected group are displayed, if already synched.

4. Right-click a group and select **Synchronize with Active Directory**.

The Select a Domain screen appears.

5. Select a domain and click **Next**.

The Authentication screen appears.

6. Specify the user name in the format of "domain name\username" and enter a valid password and then click **Next**.

The Select Active Directory Container screen appears.

7. Select **Domain Name** or **Active Directory Container** or Organizational Units (OU) for synchronization.

If you select a Domain Name, the whole Active Directory gets synched.

If you select any Active Directory Containers or OU then only the selected containers get synched.

You can select maximum 500 Active Directory Containers or Organizational Units at a time for synchronization.

8. Click **Next**.

The Settings screen appears.

9. Select the **Automatically install client on newly detected computer** check box.

The **Restrict Download Speed** check box is selected by default. You can edit the speed if required. Enter speed limit in the range of 64 to 10,000 kbps.

10. Click **Next**.

The Synchronization screen appears.

11. In Synchronization Interval, type the time interval when a periodic check is to be performed for this group and then click **Finish**.

Time should be specified between 1 to 24 hours.

The SEPS server will be synchronized with the Active Directory as per specified interval.

Editing Synchronization

This feature gives you the flexibility to edit the time interval for carrying out periodic checks to find if a new endpoint is added to the network.

The frequency can be changed depending on how many and how often new endpoints are added.

To edit the time interval, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.

2. Go to **Clients > Client Deployment > Through Active Directory**.

A window appears with all the groups.

3. Under EPS Console, right-click an already synched group and click **Edit Synchronization**.

The authentication screen for Synchronization with Active Directory appears.

4. Type the password and click **Next**.

The Settings screen appears.

5. Select the **Automatically install client on newly detected computer** check box.

The **Restrict Download Speed** check box is selected by default. You can edit the speed if required. Enter speed limit in the range of 64 to 10,000 kbps.

6. Click **Next**.

The Synchronization screen appears.

7. In the Synchronization interval text box, type the time interval.

Time should be specified between 1 to 24 hours.

8. To save the new setting, click **Finish**.

New synchronization setting is saved successfully.

Removing Synchronization

With this feature, you can remove the synchronization of a group in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Through Active Directory**.
A window appears with all the groups.
3. Under EPS Console, right-click a group that has already been synchronized and click **Remove Synchronization**.

The synchronization of the selected group is removed successfully.

Exclusion

You can exclude endpoints from installation of EPS client when Active Directory is synchronized. EPS client will be not installed on the excluded endpoint. You can exclude endpoints by Host Name, IP Address or by IP Range.

To exclude an endpoint, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Through Active Directory**.
3. On the Through Active Directory page, click the **Exclusion** button.
A popup appears with the options about how you want to exclude an endpoint.
4. On the Exclude Endpoints screen, select one of the following:
 - **Exclude by Host Name:** If you select this option, type the **Host Name** and click **Add**. The endpoint is added to the Excluded Workstations list.
 - **Exclude by IP Address:** If you select this option, type the **IP address** and click **Add**. The endpoint is added to the Excluded Workstations list.
 - **Exclude by IP Range:** If you select this option, type the **Start IP Address** and **End IP Address** and click **Add**. The endpoints are added to the Excluded Endpoints list.
5. To save your settings, click **Save**.



You can delete an endpoint from the exclusion list whenever you prefer.

Remote Install

This feature allows you to deploy Seqrite client on all supported Windows operating systems (OS). You can also install Seqrite client on multiple endpoints at a time. Before proceeding with

Remote Install, it is recommended that you go through the following requirements and changes:

Exception Rules

- On Windows Vista and later operating systems, remote installation is possible only with 'Built-in Administrator' account. To enable 'Built-in Administrator' account on endpoints running Windows Vista (or later), follow these steps:
 1. Open Command Prompt in administrative mode.
 2. Type 'net user administrator /active: yes' and press **Enter**.
 3. Change the password of 'Built-in Administrator' from **Control Panel > User Accounts**.
- For remote installation of Seqrite Endpoint Security Client on Windows XP Professional Edition, follow these steps:
 1. Open My Computer.
 2. Go to **Tools > Folder**.
 3. Click the **View** tab.
 4. Clear the option **Use simple file sharing**.
 5. Click **Apply** and then click **OK**.
- Remote installation of Seqrite is not supported on Windows XP Home Edition. To install the Seqrite client on Windows XP Home Edition, other methods of installation can be used, such as; Notify Install, Login Script, and Client Packager provided in Seqrite Endpoint Security.
- Remote Install is not supported with the users having blank passwords on Windows XP and later operating systems.
- To install Seqrite Client on the computers which are under Domain Controller, specify the user name in 'DOMAINNAME\User Name' format where DOMAINNAME is the name of the Domain Controller and User Name is the name of the Domain Administrator.

For Remote Install, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Remote Install**.

The Remote Install page opens.

3. You can initiate remote installation in any one of the following ways:
 - Remote Installation by computers

- i. Under Network Places, select an endpoint, and then click **Add**. You can select multiple number of endpoints. You can also search an endpoint by the Find computer utility.

Any endpoint in your network can be searched without enumerating the network.

For adding an endpoint, you are required to provide the user credentials of the target endpoint, having administrator rights.

- ii. On the Enter Network Password dialog, type the user credentials of the target endpoint and then click **OK**.

Repeat these steps for all the endpoints that you have selected.

If the entered user credentials are correct, the target endpoints appear in the endpoints selected to protect list.

In case, if you forget or provide an incorrect user credentials of an endpoint, you can click the Skip button and move to the next endpoint and provide its user credentials.

- Remote Installation by IP Address

- i. Click the **Add by IP Address** button (you need not select any computer from the Network Places list).
- ii. On the Add Computer by IP Address dialog, select either of the following options:
 - **Add by IP Address Range:** If you select this option, you must provide a range of IP Addresses in the Start IP Address option and the End IP Address option. This is helpful if you want to install the Seqrite client on a number of endpoints which are available in serial IP Address range at one go.
 - **Add by IP Address:** If you select this option, you need to provide the IP Address of the target endpoint.

4. Select a group under which the client will be managed after installation. By default, default group is selected.

5. Click **Next**.

For all the endpoints on which you want to install the client, you must provide the user credentials using the User Accounts option.

6. For User Accounts under Add Computer by IP Address, click **Add**.

The Add User dialog appears.

7. On the Add User dialog, type the user credentials and then click **OK**.

Repeat this for all the computers on which you want to install the client.

8. On the User Accounts list, click **Finish**.

All the endpoints are added to the Endpoints selected to protect the list.

9. Click **Install**.

The installation status of Seqrite client agents can be viewed through View Installation Status link.



- The Remote Install feature is available only in the clients with Windows operating systems.
- Remote Install is not supported through roaming service.

Viewing installation status

When deploying Seqrite client with help of remote installation process, you can keep track of client installation with the help of View Installation Status link. You can get more information about installation from Results column. At any instance, you can visit Remote Installation Status page and refresh the page to get latest installation status of multiple endpoints.

This page also provides an option to stop the installation. The installation can be stopped for those endpoints, on which installation has not yet started and is in pending state. You cannot stop the installation which is in progress state.

To view installation status, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Remote Install**.

The Remote Install page appears.

3. Click **View Installation Status** link.

Remote Installation Status page appears.

The page shows following columns:

- Endpoint Name: Shows names of the endpoints.
- Domain: Shows domain names.
- Date/Time: Shows the installation status date and time.
- Group Name: Shows the group name.
- Result: Shows installation status. If any installation fails, its reason is also displayed.

The page also shows different buttons as follows:

- Refresh: On refresh, the latest result of client installation on multiple endpoints is displayed.
- Stop Installation: Stops the pending installation, which is not actually started. You cannot stop the installation which is in progress.
- Reinitiate Install: Reinitiates the installation in case of failed, pending or stopped client installation.
- Clear: This option helps to clear the installation information from the Result column about successful, failed, and stopped client installation.
- Close: It closes the installation status page.

Notify Install

This facility allows you to send email notification to the endpoints in the network to install the Seqrite Endpoint Security client. The message can be typed and saved for future notifications. This can be edited whenever required.

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

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Notify Install**.

The Notify Install screen appears.

3. In the To field, type the email address. In case of multiple recipients, insert a semicolon (;) between email addresses.

Modify the subject line of the message if necessary.

4. Click **Send Notification**.

The default email program on your system opens. Send the email using the email program. Users should click the link provided in the email that will redirect to Seqrite client installation Web page.

5. Click the **Download** button and download the client installation utility. Execute the cainstlr.exe file.

Windows Defender SmartScreen prompt may appear. Click **Run Anyway** to continue the installation.

After Seqrite client installation is finished, the Seqrite Antivirus installation will be initiated by the Seqrite client.



- The Notify Install feature is available only in the clients with Microsoft Windows and Mac operating systems.
- To download the Notify Install utility, few Internet Explorer settings should be configured as follows:
 - **Internet Explorer Settings for Windows Server 2008:**
 - With the help of Server Manager, configure IE ESC and turn off for both Administrators & Users.
 - From Internet Explorer, go to Tools > Internet Options > Advanced tab. Clear the following check box, **Check for signature on downloaded programs**.
 - **Internet Explorer Settings for Windows Server 2003:**

From Internet Explorer, go to Tools > Internet Options > Advanced tab. Clear the following check boxes, **do not save encrypted pages to disk**, and **Empty Temporary Internet Files folder when browser is closed**.
 - **Other Security Settings for Internet Explorer:**

Other Internet options which are to be enabled are;

- Enable **File download** feature in Custom level security settings.
- Enable advanced security settings by selecting **Allow software to run or install even if signature is invalid** check box.
- Once Notify client utility is downloaded on your system then you can revert the settings done in Internet Explorer to previous state.

Client Packager

Client Packager can compress the Seqrite client setup and update files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media. It also includes an email function that can open your default email client and allow you to send the package from the Client Packager tool. The Client Packager can also be created for the Clients outside the organizational network using the Minimal option.

In Seqrite Endpoint Security 7.6, Client Packager can be created with or without the Seqrite installer and also with MSI-based Client Packager. The Client agent installer including Seqrite installer is helpful in situations where there are network bandwidth limitations to download the Seqrite installer from the Endpoint Security server. In such cases, you can create the Client agent installer including the Seqrite installer and burn into a CD/DVD or copy it to a USB removable disk for deployment on endpoints. But the Client Packager with the installer cannot be distributed through email.

When users receive the package, they should double-click the setup program to start the installation. The Seqrite clients installed through Client Packager starts communicating with the Seqrite Endpoint Security server.



The Seqrite clients installed through Client Packager out of organizational network, communicate with Seqrite Endpoint Security server by using roaming service.

Creating the Windows Seqrite Client Packager

To create a Windows Seqrite Client package, follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In Client Agent Package list, select **Custom**.

If **Minimal** is selected, then the Validity period check box is enabled, but other options on the page gets disabled. The validity period check box helps you to provide a stipulated number of days to use the installer. After the validity period, the installer expires.

The Minimal option is selected to send the Client Packager outside the organizational network through email. For more details see, [Sending a minimal Client Packager](#). The Client Packager created with installer cannot be sent through email because of the email attachment size limitation.

3. In OS platform list, select **Windows**.

4. Select the setup type from Setup type list as per requirement.

EXE/32-bit for 32-bit Client Packager EXE/64-bit for 64-bit Client Packager	Select EXE/32-bit or EXE/64-bit options to create the packager as an executable file.
MSI/32-bit for 32-bit Client Packager MSI/64-bit for 64-bit Client Packager	Select MSI/32-bit or MSI/64-bit options to create the packager as a Microsoft installer package. These packages are useful in deploying the Seqrite clients through the following: <ul style="list-style-type: none"> • Active Directory group policies • Microsoft SMS server

5. Specify if you want to include antivirus setup in Client Packager by selecting Yes or No.

- Select **Yes**, if you want to include the antivirus setup in Client Packager. But you cannot distribute this packager through email.
- Select **No**, if you do not want to include the antivirus setup in Client Packager. This packager can be distributed through email.

6. A Default group is allocated to the Client Packager from the EPS Console groups list.

The selected group gets assigned to the Client Packager and the installed client through that Client Packager will move to the selected group of EPS Console.

7. Click **Browse** to specify the folder path where you want to save Seqrite Client Packager.

8. Select the **Select this check box to specify public IP address/Hostname of EPS server for deployment of clients at remote locations** check box.

Type the Public IP address or Hostname of the EPS server.

9. Click **Create**.

10. Specify if you want to create a password protected Client Packager by selecting Yes or No.

- If you select Yes, password dialog appears. Do the following:
 - Type the password and then click **OK**.
Use a password that has at least 6 characters and maximum 18 characters. While creating the password use combination of number, uppercase letter, lowercase letter and special symbol.
 - In the **Confirmation Password** box, enter the password.
 - Click **OK**. A password protected Client Packager is created.
 - Provide the password while extracting the client packager.
- If you select No, Client Packager without password protection is created.



Password Protection is applicable only for EXE setup types for the Windows client.

Creating the Mac Seqrite Client Packager

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

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Custom**.
3. In the OS platform list, select **Mac**.
4. Specify whether you want to include antivirus setup in Client Packager by selecting Yes or No from Antivirus setup included list.
 - Select Yes if you want to include the antivirus setup in Client Packager. However, you cannot distribute this installer through email.
 - Select No if you do not want to include the antivirus setup in Client Packager. This installer can be distributed through email.
5. A Default group is allocated to the Client Packager from the EPS Console groups list.
The selected group gets assigned to the Client Packager and the installed client through that Client Packager will move to the selected group of EPS Console.
6. Download the Mac Client build from one of the following links:
<http://dlupdate.quickheal.com/builds/seqrite/760/en/mclsetp.7z>
<http://download.quickheal.com/builds/seqrite/760/en/mclsetp.7z>
7. To provide path of downloaded build, click **Browse**.
8. Select folder in which the mclsetp.7z is downloaded. By default, the mclsetp.7z is downloaded in the Downloads folder. Click **Ok**.
9. Click **Create**.
 - If you select **Yes** to include antivirus in the client packager, a MCCLAGAV.TAR file is created in the acmac folder.
 - If you select **No** to create the client packager without antivirus, a MCCLAGNT.TAR file is created in the acmac folder.
10. On the Mac endpoint you need to copy and extract any of the above created TAR file 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 SEPS server.



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

Creating the Linux Seqrite Client Packager

To create a Linux Seqrite Client packager, follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Custom**.
3. In the **OS platform** list, select **Linux**.
4. Select **Setup type** as 32 bit or 64 bit from the drop-down list as per the endpoint configuration.

The window displays the 32 bit or 64 bit links to download tar file as per your selection.

5. Download the tar file from any of the following links,

For 32-Bit,

<http://dlupdate.quickheal.com/builds/seqrite/760/en/epslin32.tar.gz>

<http://download.quickheal.com/builds/seqrite/760/en/epslin32.tar.gz>

For 64-Bit,

<http://dlupdate.quickheal.com/builds/seqrite/760/en/epslin64.tar.gz>

<http://download.quickheal.com/builds/seqrite/760/en/epslin64.tar.gz>

6. Click **Browse** and select the downloaded folder.
7. Click **Create** to create the client packager.

The packager will be created as per your selection of Setup type in the following folders:

For 32 bit -

" Seqrite\Endpoint Security 7.60\Admin\web\build\epslin32"

For 64 bit -

" Seqrite\Endpoint Security 7.60\Admin\web\build\epslin64".

To install the Client Agent:

1. Copy and extract the client packager on the Linux system.
2. For 32 bit, LinuxSetup32 is created.
For 64 bit, LinuxSetup64 is created.
3. Linux Client packager, LinuxSetup32/LinuxSetup64 contains the following files as per the endpoint configuration:
 - readme.txt
 - install
 - clagnt.ini
 - epslin32.tar.gz or epslin64.tar.gz

4. On the command prompt, type `chmod 777 install` command to grant execute permission to “install” script.
5. Execute install script.

Sending the package through email

You need to have the default email client installed to use the Client Packager email function.

Sending a minimal Client Packager

To send Client Packager from the server through an email for out of network usage, follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Minimal**.
Few options on the page become disabled.
3. Default group is selected by default under which the client will be managed after installation.
4. Click **Browse** to specify the folder path where you have saved the Seqrite Client Packager.
5. Click **Send Mail**.

The default email client will open. The email with the default subject and message appears. However, you can make changes to the subject and message, if required.

6. In the To field, specify the recipients of this package.

If required, you can also mark your email to other recipients in your organization in the Cc or Bcc recipients.

7. Click **Send**.

Sending a custom Client Packager

To send Client Packager from the server through an email for internal network, follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Custom**.
3. Default group is selected by default under which the client will be managed after installation.
4. Click **Browse** to specify the folder path where you have saved the Seqrite Client Packager.
5. Click **Send Mail**.

The default email client will open. The email with the default subject and message appears. However, you can make changes to the subject and message, if required.

6. In the To field, specify the recipients of this package.

If required, you can also mark your email to other recipients in your organization in the Cc or Bcc recipients.

7. Click **Send**.



The Send Mail button will remain disabled for Mac Client Packager and Client Agent installer including Seqrite installer option.

Login Script

This section includes the following.

Installing Login Script

This feature allows you to assign a login script to the users so that they can deploy Seqrite Client on remote systems when they log on to the selected domain. You can assign a script called QHEPS.BAT to the selected users in the domain. This script will install Seqrite endpoint protection on the system when the user logs on to the concerned domain.



The Login Script feature is available only in the clients with Windows operating systems.

Opening Login Script Setup

To open the Login Script Setup, follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console**.
2. Click **Login Script Setup**.
3. Type the Super Administrator Password of Seqrite Endpoint Security and click **OK**.

The Login Script Setup application opens. The left panel of the application includes a tree-like structure that displays all the domains in your network.

Assigning Login Script

To assign Login Script, follow these steps:

1. Open Login Script Setup; follow the steps mentioned in the Opening Login Script Setup section.
2. In the new screen, double-click the **Domain**.
3. Click the **Domain Name**.
4. Type the User Name and Password of the user having administrative privileges of the selected domain. A list of all users of the selected domain is displayed in the right panel.

- i. Select a user or multiple users from the list to assign login script.
 - ii. To select all users, click **Check All**.
 - iii. To deselect all the selected users, click **Uncheck All**.
5. Select Overwrite existing Login Script if you want to overwrite the existing assigned login script of the selected users.
6. To assign login script to the selected users, click **Apply**.

When a user logs on to the domain server, the assigned login script will deploy the Seqrite client on the user system.



- Users who do not have administrative privileges under the domain are shown in red color.
- The Result for a user can either be Assigned or Not Assigned. If the Result of a user is Assigned, it indicates that a script is assigned to that user. If the Result of a user is Not Assigned, it indicates that no scripts are assigned to that user.
- The Seqrite client will get deployed only by the users having administrative privileges on Windows XP and later operating systems.

7. To exit the Login Script Setup application, click **Close**.

Installing Seqrite Endpoint Security on Mac Operating Endpoints

Before continuing, create a Mac Client Packager (See [Creating Mac Seqrite Client Packager](#))

After the Mac Client Packager has been created, the administrator can install EPS client using Notify Install method.

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

To notify clients to install the Seqrite client, see [Notify Install](#).

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

To install Seqrite Endpoint Security, follow these steps:

1. To install SEPS Client on a Mac system, type the link in the browser (sent to you in the email).

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

2. Click the **Download Mac Client** link.

A file, MCCLAGNT.TAR, 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).

Run the installer to start the Seqrite Endpoint Security installation.

Seqrite Endpoint Security is installed successfully.



Installation of Standalone Seqrite Total Security for Mac build will proceed even if SEPS client is installed.

Remote Installation of Seqrite Endpoint Security on Mac System

You can install Seqrite Mac Client Agent in any 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)

Remote installation 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 10.9 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 [Creating the Mac Seqrite 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 above, do the following on your Mac system,
 - a. Open System Preferences.
 - b. Go to **Security & Privacy > Privacy** tab.
 - c. Click the lock icon and provide password if it is locked.
 - d. Select **Full Disk Access** in the left pane.

- e. 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

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 7.60\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.

If the Client Packager is failed to create on macOS Catalina and above, 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.

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, do the following,
 - i. In System Preferences, go to **Security and Privacy**.
 - ii. Click the **Lock** icon and provide password if it is locked.
 - iii. Select **Firewall > Firewall Options**.
 - iv. Clear the **Enable stealth mode** check box if it is selected.
 - v. Click **OK**.
- Mac Seqrite Client installer must be created on the Seqrite Endpoint Security server. To know about how to create client installer, see [Creating the Mac Seqrite Client Installer](#).

Installing Seqrite Mac Client Agent

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

1. On Seqrite Endpoint Security server, browse to the folder "<installation directory>\Seqrite\Endpoint Security 7.60\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.

- 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, do the following,
 - vi. In System Preferences, go to **Security and Privacy**.
 - vii. Click the **Lock** icon and provide password if it is locked.
 - viii. Select **Firewall > Firewall Options**.
 - ix. Clear the **Enable stealth mode** check box if it is selected.
 - x. Click **OK**.
- Mac Seqrite Client installer must be created on the Seqrite Endpoint Security server. To know about how to create client installer, see [Creating the Mac Seqrite Client Installer](#).

Installing Seqrite Mac Client Agent

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

- On the Seqrite Endpoint Security server, open **cmd.exe** and go to the folder "<installation directory>\Seqrite\Endpoint Security 7.60\Admin\web\build\acmac".

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

- Enter the following command:

```
.\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.

Creating the Mac Seqrite client installer

To create the Mac Seqrite Client installer (.TAR file), follow these steps:

1. On the Seqrite Endpoint Security server, go to **Start > Programs > Seqrite EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Custom**.
3. In the OS Platform list, select **Mac**.
4. Specify whether you want to include antivirus setup in Client Packager by selecting Yes or No from the Antivirus setup included list.
 - Select Yes if you want to include the antivirus setup in Client Packager. However, you cannot distribute this installer through email.
 - Select No if you do not want to include the antivirus setup in Client Packager. This installer can be distributed through email.
5. A Default group is allocated to the Client Packager from the EPS Console groups list.
The selected group gets assigned to the Client Packager and the installed client through that Client Packager will move to the selected group of EPS Console.
6. Download the Mac Client build from one of the following links:
<http://dlupdate.quickheal.com/builds/seqrite/760/en/mclsetp.7z>
<http://download.quickheal.com/builds/seqrite/760/en/mclsetp.7z>
7. To provide path of downloaded build, click **Browse**.
8. Select folder in which the mclsetp.7z is downloaded. By default, the mclsetp.7z is downloaded in the Downloads folder. Click **Ok**.
9. Click **Create**.

- If you select Yes to include antivirus in the client packager, a MCCLAGAV.TAR file is created in the acmac folder.
 - If you select No to create client packager without antivirus, a MCCLAGNT.TAR file is created in the acmac folder.
10. On Mac endpoint you need to copy and extract any of the above created TAR file 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 SEPS server.



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

Installing client on Linux-based Endpoints

Seqrite clients need to be manually installed by the Administrator on Linux endpoints.

To install the Seqrite client on Linux endpoints, follow these steps:

1. Follow the steps according to your endpoint's configuration:

- For the 32-bit Linux Endpoint, download the 'epslin32.tar.gz' file from one of the following links:

<http://dlupdate.quickheal.com/builds/seqrite/760/en/epslin32.tar.gz>

<http://download.quickheal.com/builds/seqrite/760/en/epslin32.tar.gz>

For 64-Bit,

<http://dlupdate.quickheal.com/builds/seqrite/760/en/epslin64.tar.gz>

<http://download.quickheal.com/builds/seqrite/760/en/epslin64.tar.gz>

2. Click **Browse** and select the downloaded folder.
3. Click **Create** to generate a package using Client Packager.
4. Create the Client Packager (according to the configuration).
5. Copy the Client Packager on your Linux endpoint.
6. Open the terminal on your Linux endpoint and log in as a root user.
Trace the path where the Client Packager is saved.
7. Extract the Client packager and trace the path of extracted folder.
8. Type the command `./install` to execute the installation script of Seqrite.

The installation script will do the following:

- It will copy the necessary files to `/usr/lib/Seqrite` folder.
- It will install Seqrite client successfully.

This completes the Seqrite client installation.



- Online Protection is dependent on Dazuko which is compatible with Linux 2.6 kernels.
- Online Protection is compatible on 32-bit operating systems of kernel version 2.6.*.
- Seqrite GUI Scanner is available on 32-bit and 64-bit endpoints.

After installation:

- If Online Protection is not installed by ./install script, you can install online protection by running ./install script with --online parameter. If automatic installation of Dazuko fails, it prompts for the dazuko file. Seqrite Online Protection (qhdaemon) requires Dazuko, a free software project providing access control. To use qhdaemon, you will need to compile Dazuko as kernel module or compile into the kernel. For more details, visit <http://dazuko.org>.
- Configure Seqrite Online Protection. You can configure Seqrite Online Protection later by running "configqhonline" from /usr/lib/Seqrite/Seqrite.

Disk Imaging

You can also deploy Seqrite Endpoint Security client through disk imaging like Sysprep.

To deploy clients through Disk Imaging, follow these steps:

1. Disconnect the endpoint from the network that will be used as a source for disk imaging, or ensure that this endpoint is not able to communicate with Seqrite Endpoint Security server.
2. Install operating system and other applications.
3. Install Client.

To install Client, follow these steps:

- i. Create a Client Packager without AV Build.
- ii. Create a Client Packager with AV Build.

4. Create a disk image.

Note: All Seqrite Endpoint Security clients have GUID (Globally Unique Identifier). If Seqrite Endpoint Security client (after installation on the endpoint that is the source for disk imaging) communicates with the Seqrite Endpoint Security server, the server will automatically assign GUID to this client. If such a client is Disk Imaged, then Seqrite Endpoint Security server will not be able to uniquely identify the clients after deployment of the image on multiple endpoints. To avoid this, ensure that the Seqrite Endpoint Security client does not communicate with the Seqrite Endpoint Security server when it gets installed on the computer that is the source for disk imaging.



The Disk Imaging feature is available only in the clients with Windows operating systems.

Firewall Exception Rules

Operating systems such as Windows and Linux have their own Firewall bundled with them. If the user prefers to retain the firewall bundled with the operating system, then exceptions can be created with Seqrite Endpoint Security for such systems. These exception rules are created during installation of Seqrite Endpoint Security. For the computer on which Seqrite Endpoint Security is installed, the exceptions will be automatically created during installation. For the Seqrite client the exception will automatically be created during deployment of Seqrite clients.

The system with Seqrite Endpoint Security will require three exception rules: one for the server, one for its own client, and one for the Endpoint Security site configured on it.

The following are the exception rules for server:

- Agent Server 7.6
- Client Agent 7.6
- Endpoint Security Site Port 7.6

The computer with the Seqrite client will require one exception rule to be created. The following is the exception rule for clients:

- Client Agent 7.6

If the client system is a Linux-based system, the exception rule will be created in its Firewall as a port number.

Remote Uninstall

With Remote Uninstall, you can remove Seqrite client along with the antivirus program from the computers on your network remotely.



The Remote Uninstall feature is available in the clients with Microsoft Windows, Mac, and Linux operating systems.

To remove the client through Remote Uninstall, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Client Deployment > Remote Uninstall**.

The Remote Uninstall dialog appears that displays all the groups. Each group includes the name of the endpoints belonging to the group.

3. Select the endpoint from which you want to uninstall the Seqrite client. To uninstall Seqrite Client from all endpoints, select the check boxes available to the endpoint name columns.

You can also schedule uninstallation from endpoints that are not online or not present in the network by selecting Show offline clients. Select the Show Endpoints within subgroup to display the name of the endpoints that are in the subgroup from the list of the endpoints without actually exploring the network.

4. Select **Start Uninstall Notification**.

The uninstallation starts.

Stop Uninstallation Notifications

If you want to send notifications to stop uninstallation to the endpoints that have not yet started uninstallation, follow these steps:

1. Select the endpoints from which you want the clients should not be removed.
2. Click **Stop Uninstall Notification**.
3. Clients that have not yet started the client uninstallation will skip the uninstallation request. However, clients that are already running the uninstallation program cannot stop the uninstallation procedure.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.



Notification for Remote Uninstall from SEPS Web console will not be sent if the user is not logged on to the Mac system.

Manage Groups

This feature helps you create groups and subgroups and apply a policy to a group (or a subgroup). A group includes a number of endpoints and all the endpoints within a group share the same policy. You can delete or rename a group or set different policies for different groups. You can also move endpoints from one group to another. You can export or import groups from one EPS server to another along with policies assigned to them.

Adding a Group

To add a new group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Select the root node, for example Endpoint Security, and then right-click it.

A submenu list appears. Only Add Group option is enabled.

4. Select **Add Group**.

The Add Group screen appears.

5. In the Enter Group Name text box, type a group name.
6. Click **OK**.

The new group is added.

Terms	Definition
Show endpoints within subgroup	Helps you display the endpoints that are in a subgroup.
Search	Helps you search an endpoint by its name or IP Address.
CSV	Helps you save the report in csv format.



No subgroup can be created under the Default group.

Adding a Subgroup

To add a subgroup, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select a group and then right-click it.

A submenu list appears.

4. Select **Add Group**.

The Add Group screen appears.

5. In the Enter Group Name text box, type a group name.
6. Click **OK**.

The subgroup is added.

Deleting a Group

To delete a group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select a group and then right-click it.

A submenu list appears.

4. Select **Delete Group**.

A confirmation message is displayed.

5. Click **OK**.

The selected group is deleted.



If you delete a group that includes subgroups, then all the connected subgroups are also deleted.

Renaming a Group

To rename a group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select a group and then right-click it.

A submenu list appears.

4. Select **Rename Group**.

The Rename Group screen appears. The old group name is also displayed.

5. In the Enter New Name text box, type a new group name.
6. Click **OK**.

The group name is modified. However, the policy applied earlier to this group does not change. To change a policy, you have to apply a new policy.

Importing from Active Directory

This feature allows you to import Active Directory Structure in the console. This is helpful when you need to have group structure in the console that is already available in the Active Directory.



- To import from Active Directory, your console must be installed on the domain machine, or it should be a member of the domain.
- “Import From Active Directory” cannot be done with the default group.

To import Active Directory Structure, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select a group and then right-click it.
A submenu list appears.
4. Select the **Import from Active Directory** option.
The Active Domain Controller dialog appears.
5. Select a domain and then click **Next**.
The authentication screen appears.
6. Type the user name in the format "domain name\user name" and then enter your password.
7. Click **Next**. Depending upon number of Active Directory Containers or Organizational Units selected, delay can be observed while loading the Organizational Units list.
8. On the Select Active Directory Container screen, select a Domain Name or Active Directory Container to import.

If you select a Domain Name, the whole Active Directory is imported and if you select any Active Directory Container, only the selected container is imported.
9. Click the **Finish** button.

Setting Policy to a Group

Policies may include different client settings for different groups in an organization.

To set a policy to a group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select and right click a group.
A submenu list appears.
4. Click the **Set Policy** option.
A list of policies appears.
5. Select the policy that you want to apply.
The applied policy is displayed in the right panel along with the endpoint name, group, and other details.

Assigning Group Administrator

To assign the Group Administrator to a group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select and right click a group to assign the Group Administrator.
A submenu list appears.
4. Select Assign Group Administrator.
A submenu list of Group Administrators appears.
5. Select the Group Administrators that you want to assign.
6. Click Yes on the confirmation dialog box.
The Group Administrator is assigned to the group.
When you log on to Seqrite Endpoint Security console as Group Administrator, the Clients page is displayed by default.

Unassigning Group Administrator

To unassign the Group Administrator for a group, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select and right click a group to unassign the Group Administrator.
A submenu list appears.
4. Select Unassign Group Administrator.
5. Click Yes on the confirmation dialog box.

The Group Administrator is unassigned for the group.

Changing Group of an Endpoint

Using this feature, you can check if an endpoint should be in a certain group, or the group has to be changed because of policy change at your organization. In case a change is incorporated, the protection policy of the new group will be applied.

To change the group of an endpoint, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Under EPS Console, select a group.

A list of all endpoints of the selected group is displayed in the right panel.

4. Select an endpoint and drag it to a desired group where you want.

The endpoint is included in the new group.

Exporting groups and policies

This feature allows you to export groups and policies assigned to them from one EPS server to another. This is helpful when you need to move groups from one EPS server to another or in case of reinstallation. The data is downloaded to a .db file. You must copy that file to another server and use the import option to import groups and policies assigned to them.

To export groups and policies assigned to them, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Click **Export**.
4. If the USB device is added and encrypted in Admin Settings > Server > Manage Devices, Manage Groups dialog appears. Click **Yes** or **No**.

If you click **Yes**, all customized settings along with USB device authorization will be exported. You will be able to use exported authorized USB devices on another EPS Server clients.

Please note, this will deny access to previously authorized devices on the server, on which the policy will be imported.

If you click **No**, all customized settings except USB device authorization will be exported.

5. Select the drive and folder in which you want to store the policy.
6. Click **Save**.

The file containing groups and policies assigned to them is saved.

Importing groups and policies

This feature allows you to import entire groups and policies assigned to them from one EPS server to another. The groups' data is downloaded to a .db file when you export the groups. You must copy that file to another server and use the import option for groups.

To import groups, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Groups**.
3. Click the **Import** button.
4. Select the file which is exported previously.

The Import Setting dialog appears. Select policies you want to import. You can select all policies also.

5. Click **Import**.
6. While exporting the policy, if you have clicked Yes in the Manage Groups dialog, the Import dialog appears. Click **Yes** or **No**.

If you click **Yes**, all customized settings along with USB device authorization will be imported. You will be able to use imported authorized USB devices on these EPS Server clients.

Please note, before importing, ensure to unauthorize all previously authorized USB devices. If you do not unauthorize, the devices will be unusable.

If you click **No**, all customized settings except USB device authorization will be imported.

The groups and policies assigned to them are imported and a message is displayed as follows: **File imported successfully**.



The policy is not imported if the inherited policy with the same name exists.

Policies which are not assigned to any group are not exported or imported from Manage Groups page. Those policies can be exported or imported by using Export or Import option on Clients > Manage Policies page.

Manage Policies

Each organization prefers to enforce a policy that regulates its users. Seqrite Endpoint Security allows the administrators to create policies that help centrally control and manage the users belonging to a group.

You can create a policy about permission to visit only certain Web sites, scan their systems regularly and implement policy for email communication. You can also restrict usage of certain applications and USB-based devices. The Manage Policies feature gives you the flexibility and control over creating new policies and modifying or removing an existing policy. Different protection policies can be created for different groups for better control.

Policies may include different client settings and scan schedules. Once a policy is created, it can be easily applied to a group. The users under a group or a subgroup will inherit the same policy. A group is nothing but a department in an organization. You should create groups before you create a policy setting. You can also view the policy status i.e. Applied, Pending or Failed on each client, this status can also be exported in csv format.

To learn about how to create a group, see [Adding a Group](#).

Understanding Security Policy Scenario

The following example illustrates how different security policies can be created within an organization for different departments. Two departments namely Marketing, and Accounts have been taken as an example.

Policy Settings for Marketing and Account Departments Compared			
Client Settings	Policy Features	Marketing Dept.	Accounts Dept.
Scan Settings	Scan mode	Automatic	Advanced
	Virus Protection Setting	Enabled	Enabled
	Block suspicious packed files	Enabled	Enabled
	Automatic Rogueware scan	Enabled	Enabled

	Disconnect Infected Endpoints from the network	Not Enabled	Enabled
Email Settings	Email Protection	Enabled	Enabled
	Trusted Email Clients Protection	Enabled	Enabled
	Spam Protection Level	Soft	Strict
External Drives Settings	Scan External Drives	Enabled	Enabled
	Autorun Protection	Enabled	Enabled
	Mobile Scan	Not Enabled	Enabled
IDS/IPS	IDS/IPS	Enabled	Enabled
	Disconnect system from the network (only in case of DDOS and Port Scanning attack)	Not Enabled	Enabled
Firewall	Firewall	Enabled	Enabled
	Level	Low	High
Web Security	Browsing Protection	Enabled	Enabled
	Phishing Protection	Enabled	Enabled
Web Categories	Business	Allowed	Denied
	Social Networking	Denied	Denied
Application Control	CD/DVD Applications	Authorized	Unauthorized
	Games	Unauthorized	Unauthorized
Advanced Device Control	Enable Advanced Device Control	Enabled	Enabled
	Device Types	No devices enabled	Devices selected and enabled
	Exceptions	Not enabled	Enabled and appropriately added
Data Loss Prevention	Enable Data Loss Prevention	Enabled	Enabled
	Select Data Transfer Channels	Monitor Network Share, Monitor Clipboard, Disable Print screen	Monitor Transfer through Application, Monitor Removable devices
	Select Data to be monitored	File Types, Confidential Data, User Defined Dictionaries	File Types, Confidential Data

	Actions	Block and Report	Report only
File Activity Monitor	Enable File Activity Monitor	Enabled	Enabled
	Removable Drives	Enabled	Enabled
	Network Drives	Enabled	Enabled
	Local Drives	Not Enabled	Enabled
Update Setting	Automatic update	Enabled	Enabled
	Download from Internet	Enabled	Not Enabled
	Download from Endpoint Security Server	Not Enabled	Enabled
Internet Settings	Proxy Settings	Enabled	Not Enabled
Patch Management	Scan and Install missing patches	Enabled	Enabled
General Settings	Authorize access to the client settings	Enabled	Enabled

Creating Policies

Policies help you manage client settings for different groups. You can create policies with client settings, and schedule settings to apply to different groups.

Creating a new policy

To create a new policy, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.
3. To create a new policy, click **Add**.

The new policy settings screen appears.

4. In the Policy Name text box, type the policy name.

After naming the new policy, you need to configure the client settings and schedule settings.

5. In the Description text box, enter brief details about the policy.
6. To save your settings, click **Save Policy**.

While creating a new policy, you can allow the clients to configure their own settings by selecting the **Let clients configure their own settings** option.



If you enable this option, the Advanced Device Control and Data Loss Prevention features are disabled.

Copying a policy

To copy a policy, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.
3. Select the policy that you want to copy and click **Copy Policy** icon.

The selected policy appears with its settings.

4. In the Policy Name text box, type the policy name.

You can also change the policy settings.

5. To save your setting, click **Save Policy**.

Renaming a policy

To rename a policy, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.
3. Click the policy that you want to rename.

The selected policy appears with its settings.

4. In the Policy Name text box, rename the policy.

You can also change the policy settings.

5. To save your setting, click **Save Policy**.

Deleting a policy

To delete a policy, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.
3. Select the policy that you want to delete, and then click **Delete**.

A confirmation message appears.

4. If you are sure to delete the selected policy, click **YES**.

If the selected policy is applied to a group/secondary server, it cannot be deleted and a message about Failed to delete policies appears.

If the selected policy is an inherited policy, it cannot be deleted and a message about Failed to delete policies appears.



If a policy is applied to a group and you want to delete it, apply a different policy to that group so the target policy is not applied to any group and then delete such a policy successfully.

Importing and Exporting Policies

This feature allows you to import or export the policies of Seqrite Endpoint Security. If you need reinstallation or have multiple endpoints and want the same settings, you can simply export the settings configured on your current endpoint and easily import them on the endpoint(s). Both the default settings and the settings made by you can be exported.



The settings must be exported before you uninstall Seqrite Endpoint Security. Importing or exporting the settings can be done in the same way.

Exporting a policy

To export the policy settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.
3. Select a policy that you want to export and then click the **Export** button.
4. If the USB device is added and encrypted in Admin Settings > Server > [Manage Devices](#), **Manage Policies** dialog appears. Click **Yes** or **No**.

If you click **Yes**, all customized settings along with USB device authorization will be exported. You will be able to use exported authorized USB devices on another EPS Server clients.

Please note, this will deny access to previously authorized devices on the server, on which the policy will be imported.

If you click **No**, all customized settings except USB device authorization will be exported.

5. Select the drive and the folder in which you want to store the policy.
6. Click **Save**.

The policy settings file is exported to the selected location.

Importing a policy

To import the policy settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Manage Policies**.

3. Click the **Import** button.
4. Select the Import Settings file from the location where it exists.
The Import Setting dialog appears. Select policies you want to import. You can select all policies also.
5. Click **Import**.
6. While exporting the policy, if you have clicked **Yes** in the Manage Policies dialog, the Import dialog appears. Click **Yes** or **No**.

If you click **Yes**, all customized settings along with USB device authorization will be imported. You will be able to use imported authorized USB devices on these EPS Server clients.

Please note, before importing, ensure to unauthorize all previously authorized USB devices. If you do not unauthorize, the devices will be unusable.

If you click **No**, all customized settings except USB device authorization will be imported.

The policy settings file is imported.

Policy Fetch Utility

This utility is used to fetch policy from the EPS Server using pull method to apply the policy to the EPS clients within the same network.

To fetch policy from the EPS server, follow these steps from EPS Client:

1. Go to Program files\Seqrite\Client agent 7.60.
2. Execute the file clpolfetch.exe.

The utility dialog opens.

The status of policy fetching and applying on the clients is displayed with date and time on the utility.

3. Click **Close** button to close the Policy Fetch Utility.

If policy is failed to apply, the error message appears. Click **Retry** button to apply the policy again.



Policy Fetch Utility supports only EPS clients within the same network of EPS Server. This utility is not supported for Roaming clients

Assets

Assets feature helps you keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes, if any, that are made to the configuration of the systems in your network. You can also keep a tab on the list of the endpoints where the changes have been carried out and export the above information to a .csv file. You can download the complete report of Asset details of all the endpoints in one go.

Enabling Asset Management

You can enable the Asset Management reporting by the following procedure:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients > Asset Management**.
3. To enable asset management, select the **Enable Asset Management** check box.
4. Select the **Display Windows Product key** check box to view the complete product key at [Clients > Assets > View Details](#). If you don't select this check box, only partial product key will be displayed.
5. Click **Apply**.



- The details of some software may not be displayed in Assets.

Viewing the details for Endpoints

To view the details for all the endpoints, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Assets**.

The Assets view displays the following details of all the clients:

Fields	Description
Endpoint Name	Displays the name of the endpoint.
Group	Displays the group name to which the selected client belongs.

Domain	Displays the domain to which the selected client logs in.
IP Address	Displays the IP address.
Operating System	Displays the name of the operating system of the endpoint.
System Manufacturer	Displays the name of System Manufacturer.
Main Circuit Board	Displays the number of Main Circuit Board.
BIOS	Displays BIOS serial number.

To view the details for a particular endpoint, follow these steps:

1. Do one of the following:

- In the Assets page, enter the endpoint name/IP in the search text box and click the Search icon.
- Select an endpoint from the displayed list.

2. Click **View Details**.

The View Details screen appears.

- The System Information tab displays the system information in detail. OS Product key of the Windows OS appears according to the settings done at [Admin Settings > Clients > Asset Management](#).



The OS Product key is available only in the clients with Windows Vista and above operating systems.

- The Hardware Information tab displays the hardware information in detail.
- The Software Installed tab displays the details of software installed on the system.

The MS Office Product key is available only for MS Office 2010 and above.



The Product key of MS Office is not available in the clients with MAC operating system.

The license status of MS Office appears.

The following table mentions possible License status and their description for MS Office.

License status	Description
Unlicensed	The product is not licensed.
Licensed	The product is licensed.
OoBGrace	The MS Office license is in the grace period.
OoTGrace	The MS Office license requires reactivation.
NonGenuineGrace	The MS Office license has failed online validation and is in the grace period.
ExtendedGrace	The grace period of the MS Office license is extended.

Notification	The MS Office license is either out of the grace period or failed validation.
--------------	-------------------------------------------------------------------------------

You can save the details of the endpoint in csv format.

Downloading Complete Asset Details Report

To download the complete Asset details report for all the endpoints, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Clients > Assets**.
3. In the upper right corner of the page, Click icon with label **Download complete Asset Details**.
4. The complete Asset report is downloaded with the following information of all the endpoints.
 - System information
 - Hardware information
 - Software installed

Settings

This feature allows the administrators to see and customize the settings of the default policy. The default policy is available as soon as you install the product on your system. The default policy includes both the client settings and schedule scan settings and is optimal for security that you can apply to a group. However, you can customize the settings according to the requirement, but its name cannot be changed. The default policy is also available in the Manage Policies option (Seqrite Endpoint Security > Clients > Manage Policies) from where you can customize its settings.

Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Default button.

Client Settings

This section includes the following:

Scan Settings

This feature allows you to define a policy on how to initiate the scan of the client systems in your organization. The policy can be refined to enable Virus Protection or DNA scanning or include blocking of any suspicious packed files, and other settings.

The following table shows a comparison of the features in Scan Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Automatic scan mode	✓	✓	X
Scan executable files	✓	✓	X
Scan all files (Takes longer time)	✓	✓	X
Scan packed files*	✓	X	X
Scan mailboxes*	✓	X	X
Scan archives files*	✓	✓	X

To create a policy for Scan Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Scan Settings**.
3. Under Scanner Settings, select the scan mode.

The Scan Mode includes Automatic and Advanced.

You can enable Virus Protection, Advanced DNAScan, Block Suspicious Files, Automatic Rogueware Scan, Disconnect Infected Endpoints from the network, Exclude files and folders, and exclude extensions from being scanned.


4. To save your setting, click **Save Policy**.

Scanner Settings

Under Scanner Settings, you can select either of the following scanning options:

- **Automatic***: This is the default scan setting that ensures optimum protection to the clients.
- **Advanced**: If you select this option, you may further need to customize the configuration of scanning options as per your requirement. When you select this option, other features are activated that are described as follows:

Features	Description
Select items to scan	Select either of the options to scan: Scan executable files: Includes scanning of executable files only. Scan all files: Includes scanning of all files but takes longer time for scanning.
Scan Packed Files*	Scans packed files inside an executable file.
Scan Mailboxes*	Scans emails inside the mailbox files.
Scan Archive Files*	Scans compressed files such as ZIP and ARJ files including other files.
Archive Scan Level	You can set the level for scanning in an archive file. The default scan level is set to 2. You can increase the default scan level, however, that may affect the scanning speed.
Select action to be performed when virus is found in archive file.	You can select an action that you want to take when a virus is found in archive file during an on-demand scan. You can select any one of the following actions: <ul style="list-style-type: none"> • Delete – Deletes the entire archive file even if a single file within the archive is infected. • Quarantine – Quarantines the archive containing the infected files. • Skip – Takes no action even if a virus is found in an archive file.

Select action to be performed when a virus is found.	<p>You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:</p> <ul style="list-style-type: none"> • Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. • Delete – All the infected files are deleted automatically. • Skip – Takes no action even if a virus is found in a file.
	To know for which clients the features marked with asterisk are applicable, see the comparison table .

Virus Protection Settings

This feature helps you continuously monitor the client systems against viruses that may infiltrate from sources such as email attachments, Internet downloads, file transfer, and file execution. It is recommended that you always keep Virus Protection enabled to keep the client systems clean and secure from any potential threats.

This feature gives signature-based protection to all endpoints in the network.

The following table shows a comparison of the features in Virus Protection Settings that are applicable for different flavors of Seqrite Endpoint Security clients:

Features	Clients		
	Windows	Mac	Linux
Load Virus Protection at Startup	✓	✓	✓
Display alert messages	✓	✓	X
Report source of infection	✓	X	X
Select action to be performed when a virus is found	✓	✓	X

With Virus Protection, you can configure the following:

Features	Description
Load Virus protection at Startup	Enables real-time protection to load every time the system is started.
Display Alert messages	Displays an alert message with virus name and file name, whenever any infected file is detected by the virus protection.
Report source of infection	Displays the source IP address of the system where the virus is detected.

Select the action to be performed when a virus is found	<p>You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:</p> <ul style="list-style-type: none"> • Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. • Delete – All the infected files are deleted automatically. • Deny Access – Access to an infected file is blocked.
---------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Advanced DNAScan Settings

Helps you safeguard the client systems even against new and unknown malicious threats whose signatures are not present in the virus definition database. DNAScan is an indigenous technology of Seqrite to detect and eliminate new types of malware in the system. DNAScan technology successfully traps suspected files with very less false alarms.

Advanced DNAScan Settings also includes the following:

Features	Description
Enable DNAScan	Helps in scanning the systems based on Digital Network Architecture (DNA) pattern.
Enable Behavior detection system	Helps in scanning the files and processes (host based) on their behavior. If the files or systems behave suspiciously or their behavior changes by itself is considered as suspicious. This detection can be categorized based on their criticality level as Low, Moderate, and High. You can select the detection criticality level depending on how often suspicious files are reported in your systems. BDS
Submit suspicious files	Helps in submitting suspicious files to the Seqrite research lab automatically for further analysis.
Show notification while submitting files	Displays a notification while submitting DNA suspicious files.



- The Advanced DNAScan Settings feature is available only in the clients with Windows operating systems.
- The 'Behavior detection system' scan setting is not applicable for Windows XP 64-bit and Windows Server platforms.

Block suspicious packed files

This feature helps you identify and block access to the suspicious packed files. Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the endpoint systems.

It is recommended that you always keep this option enabled to ensure that the clients do not access any suspicious files and thus prevent the spread of infection.



The Block suspicious packed files feature is available only in the clients with Windows operating systems.

Automatic Rogueware Scan Settings

This feature automatically scans and removes rogueware and fake antivirus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.



The Automatic Rogueware Scan feature is available only in the clients with Windows operating systems.

Disconnect Infected Endpoints from the network

This disconnects the infected endpoints from the network. The following options are available:

- **When non-repairable virus found:** Disconnects the endpoint, if a non-repairable virus is found running in the memory.
- **When suspicious file found by DNAScan:** Disconnects the endpoint, if any suspicious file is found running in the memory.



The Disconnect Infected Endpoint from the network feature is available only in the clients with Windows operating systems.

Exclude Files and Folders

This feature helps you decide which files and folders should be omitted from scanning for known viruses, Advanced DNAScan, and Suspicious Packed files. It is helpful in case you trust certain files and folders and want to exclude them from scanning.

The following table shows a comparison of the features in Exclude Files and Folders that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Exclude from: Known Virus Detection	✓	✓	X
Exclude from: DNAScan	✓	X	X

Exclude from: Suspicious Packed Files Scan	✓	X	X
Exclude from: Behavior Detection	✓	X	X

To add a file or a folder, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Scan Settings**.
3. Under Exclude File and Folders, click **Add**.

For Mac OS, use only forward slash (/) in the folder path. Example:
/Users/Admin/ExcludeList.

4. On the Exclude Item screen, select either of the following:
 - **Exclude Folder:** If you select Exclude Folder, type the folder path in the Enter folder path text box.

If you want a subfolder also to be excluded from scanning, select **Include Subfolder**.

- **Exclude File:** If you select Exclude File, type the file path in Enter file path text box.
- **Exclude MD5 checksum:** If you select Exclude MD5 Checksum, type the checksum in Enter MD5 Checksum text box.

MD5 checksum is a 32-character hexadecimal number which is the fingerprint of the file. With MD5 checksum, you can verify whether your downloaded file got corrupted or not in transit.

5. Under Exclude from, select any one option as per your requirement:

- Known Virus Detection
- DNAScan
- Suspicious Packed Files Scan
- Behavior Detection
- Anti-Ransomware



When you select the **Exclude MD5 checksum** option, all the above options are selected, by default. Anti-Ransomware option is available only in the **Exclude MD5 checksum** selection.

6. To save your settings, click **OK**.



- If you select Known Virus Detection, DNAScan and Suspicious Packed File Scan will also be enforced, and all the three options will be selected.
- If you select DNAScan, Suspicious Packed File Scan will also be enforced, and both the options will be selected.
- However, you can select Suspicious Packed File Scan or Behavior Detection as a single option.

Exclude Extensions

This feature helps you exclude the files from scanning by real-time virus protection by their extensions. This is helpful in troubleshooting performance related issues by excluding certain categories of files that may be causing the issue.

To exclude a file extension from scanning, follow these steps:

- Under Exclude Extensions, type an extension in the file extension name text box, and then click Add.

The file extension should be without any dots in the following format: xml, html, zip etc.



The Exclude Extensions feature is available only in the clients with Windows and Mac operating systems.

Email Settings

This feature allows you to customize the protection rules for receiving emails from various sources. You can set rules for blocking spam, phishing, and virus infected emails.

The following table shows a comparison of the features in Email Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Enable Email Protection	✓	✓	X
Enable Trusted Email Clients Protection	✓	X	X

To configure Email Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Select the options that you want to enable.

The Email Setting options include: Email Protection, Trusted Email Clients Protection, Spam Protection, Spam Protection Level, white list, and black list.

4. To save your settings, click **Save Policy**.

Email Protection

With this feature, you can apply the protection rules to all incoming emails. These rules include blocking infected attachments (malware, spam, and viruses) in the emails.

This feature is turned on by default which provides the optimal protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection. Once the feature is enabled, all incoming emails will be scanned before they are sent to Inbox.

To configure Email Protection, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.

The **Enable Email Protection** check box is selected by default.

3. The **Block attachments with multiple extensions** check box is selected by default. This option helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
4. The **Block emails crafted to exploit vulnerability** check box is selected by default. This option helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
5. The **Enable attachment control** option helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are enabled:
 - Block all attachments: Helps you block all types of attachments in emails.
 - Block user specified attachments: Helps you block email attachments with certain extensions. If you select this option, the **Configure** button is activated. For further settings, click **Configure** and set the following options:
 - a. In the User specified extensions dialog, select the extensions so that the email attachments with such extensions are blocked.
 - b. If certain extensions are not in the list that you want to block, type such extensions in the **Extension** text box and then click **Add** to add them in the list.
 - c. Click **OK** to save changes.
6. Select the **Enable Email scanning over SSL** check box to enable incoming mail scanning for mail accounts configured over SSL. Ensure that you perform the [procedure](#) to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.



The Email Protection feature is available only in the clients with Microsoft Windows and Mac operating systems.

Configuring Email Clients

For MS Outlook mail client, Seqrite Email Scanner certificate is imported automatically. No action required.

For your reference, procedure to import Seqrite Email Scanner certificate for Mozilla Thunderbird mail client is quoted here,

1. Launch Thunderbird mail client.
2. Select **Options** menu > **Advanced > Certificates** tab.

3. Click **View Certificates**.
4. In Certificate Manager dialog, select **Authorities** tab, click **Import**.
5. Select **Seqrite Email Scanner CA.der** certificate from
 <installation directory>\Seqrite\Seqrite.
6. Click the **Trust this CA to identify websites** check box and click **Ok**.
7. In Certificate Manager dialog, click **Ok**.
8. In Options dialog, click **Ok**.

Similarly, for other mail clients, to import Seqrite Email Scanner certificate, refer their technical documentation.

Trusted Email Clients Protection

Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.

Trusted Email Clients Protection is an advanced option that authenticates email-sending application on the system before it sends the emails. This option prevents new worms from spreading further. It includes a default email client list that is allowed to send emails. Email clients in the default list includes Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator.

Trusted Email Clients Protection supports most of the commonly used email clients such as; Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator. If your email client is different from the ones mentioned, you can add such email clients in the trusted email client list.

Configuring Application Path

To configure Application Path, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Follow the steps for [Enable Email Protection](#).
4. Select **Enable Trusted Email Client Protection**.
5. In the Application Path text box, type the path and name of the application (including .exe extension) and then click **Add**.

You can delete the added Application Path with **Delete** button.



The Trusted Email Clients Protection feature is available only in the clients with Windows operating systems.

Spam Protection

This feature allows you to differentiate genuine emails and filter out unwanted email such as; spam, phishing, and adult emails. We recommend you to always keep Spam Protection enabled. If you enable Spam Protection, the Spam Protection Level, White list, and Black list options are also activated.

The following table shows a comparison of the features in Spam Protection that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Spam Protection	✓	✓	X
Spam Protection Level	✓	X	X
Enable White list	✓	✓	X
Enable Black list	✓	✓	X



The Spam Protection feature is not supported on Apple's M1 chip.

Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Follow the steps for [Enable Email Protection](#).
4. Select **Enable Spam Protection**.
5. Under Spam protection level, set the protection level from the following:
 - **Soft**: Applies soft filtering spam protection policy.
 - **Moderate**: Ensures optimum filtering. It is recommended to have moderate filtering enabled. However, this is selected by default.
 - **Strict**: Enforces strict filtering criteria. However, it is not ideal as it may even block genuine emails. Select strict filtering only if you receive too many junk emails.
6. Select **Enable white list** to implement protection rules for whitelisted emails.
7. Select **Enable email black list** to implement the protection rules for blacklisted emails.
8. To save your settings, click **Save Policy**.

Setting spam protection rule for Whitelist

Whitelist is the list of trusted email addresses. The content from the whitelisted email IDs is allowed to skip the spam protection filtering policy and is not tagged as SPAM.

This is helpful if you find that some genuine email IDs are detected as SPAM or if you have blacklisted a domain but want to receive emails from certain email addresses from that domain.

To add email addresses in the whitelist, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Select the **Enable White List** check box.

Check whether Spam Protection is enabled. If Spam Protection is enabled only then the whitelist option is activated.

4. In the Email ID text box, type an email address or a domain and then click **Add**.

You can import email addresses or domains from text file using the Import button.



- An email address should be in the format: abc@abc.com.
- A domain name should be in the format: *@mytest.com.
- The same email ID cannot be entered in both blacklist and whitelist.

Setting spam protection rule for Blacklist

Blacklist 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 is useful particularly if your server uses an open mail relay, which is used to send and receive emails from unknown senders. This mailer system can be misused by spammers. With blacklist, you can filter incoming emails that you do not want or are from unknown senders both by email IDs and domains.

To add email addresses in the blacklist, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Select the **Enable black List** check box.

Check whether Spam Protection is enabled. If Spam Protection is enabled only then the blacklist option is activated.

4. In the Email ID text box, type an email address or a domain and then click **Add**.

You can import email addresses or domains from text file using the Import button.



- An email address should be in the format: abc@abc.com.
- A domain name should be in the format: *@mytest.com.
- The same email ID cannot be entered in both blacklist and whitelist.

Configuring Port Settings

To configure port settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Follow the steps for [Enable Email Protection](#).
4. In the Configure Port Settings section, do the following:
 - i. Enter POP3 and IMAP ports for incoming mails.
 - ii. Enter POP3 and IMAP ports for incoming mails over SSL.
 - iii. Enter SMTP ports for outgoing mails.

External Drives Settings

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them. This feature allows you to set protection rules for external devices such as; CDs, DVDs, and USB-based drives.

The following table shows a comparison of the features in External Drives Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Scan External Drives	✓	X	✓
Autorun Protection Settings	✓	X	X
Mobile Scan Settings	✓	X	X

To configure External Drives Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > External Drives Settings**.
3. Select the options that you want to enable.

The External Drives Settings options include: External Drives Settings, Autorun Protection Settings, and Mobile Scan Settings.

4. To save your setting, click **Save Policy**.

External Drives Settings includes the following:

External Drives Settings

With External Drives Settings, you can scan the USB-based drives as soon as they are attached to your system. The USB-based drives should always be scanned for viruses before accessing it from your system, as these devices are convenient mediums for transfer of viruses and malwares from one system to another.

Autorun Protection Settings

Autorun Protection protects your system from autorun malware that tries to sneak into the system from USB-based devices or CDs/DVDs using the autorun feature of the installed operating system.

Mobile Scan Settings

This feature scans for viruses, spywares, and other malwares in mobile devices. To scan your mobile device, you need to connect it to PC using any of the following methods:

- USB Cable
- Bluetooth



The Mobile Scan feature is not supported on server operating systems.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

When you create a network where numerous machines are deployed, security is of paramount concern. With host-based IDS/IPS, you can detect attacks from various sources such as IDS/IPS, Port scanning attack, Distributed Denial of Service (DDOS), etc. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or network attacks. You can also take actions like blocking the attackers for certain time, disconnecting the infected system from the network, and also send an alert message to the administrator.



The IDS/IPS feature is available only in the clients with Microsoft Windows.

You can create different policies with varying IDS/IPS settings and apply them to the groups so that each has separate policies based on the requirement.

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > IDS/IPS**.
3. Enable one of the following options by selecting the check box:
 - Enable IDS/IPS
 - Detect Port Scanning Attack
On selecting this check box, Customize link is enabled.
 - Detect DDOS (Distributed Denial of Service) Attack
On selecting this check box, Customize link is enabled.
4. From the following options, select an action to be performed when attack is detected:
 - Block Attackers IP for ... Minutes.
Enter time here.

- Disconnect endpoint from the network (only in case of DDOS and Port Scanning attack).
- Display alert message when attack is detected.

This helps you take an appropriate action when attack is detected.

5. To save your settings, click **Save Policy**.

Customizing Port Scanning

You can customize settings for Detect Port Scanning Attack and Detect DDOS (Distributed Denial of Service) Attack as follows:

1. Log on to the Seqrite Endpoint Security Web console.

2. Go to **Settings > Client Settings > IDS/IPS**.

3. Select the **Detect Port Scanning Attack** check box.

The Customize link gets enabled.

4. Click the **Customize** link.

Settings –Port Scanning dialog appears.

5. Select one of the following levels:

- **Soft:** Detects attack if many ports are scanned.
- **Normal:** Detects attack if multiple ports are scanned.
- **Strict:** Detects attack even if a single port is scanned.
- **Custom:** Helps you customize the attack condition and number of scanned ports exceeds than field.

6. To exclude an IP address that you do not want to be scanned, click **Add** in Excluded IP Addresses section.

7. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.

8. To exclude port that you do not want to be scanned, click **Add** from the Excluded Ports section.

9. On the Add Port screen, type a Port or Port range and then click **OK**.

Customization for Distributed Denial of Service

Further customization settings for Distributed Denial of Service Attack are as follows:

1. Log on to the Seqrite Endpoint Security Web console.

2. Go to **Settings > Client Settings > IDS/IPS**.

3. Select the **Detect DDOS (Distributed Denial of Service) Attack** check box.

The Customize link gets enabled.

4. Click the **Customize** link.

The Settings – Denial of Service dialog appears.

Select one of the following levels:

- **Soft:** Detects if many attacks occur.
 - **Normal:** Detects if multiple attacks occur.
 - **Strict:** Detects attack even if a single attack occurs.
 - **Custom:** Helps you customize the attack condition and number of attack sources exceeds than the specified limits.
5. To exclude an IP address that you do not want to be scanned, click **Add** in the Excluded IP Addresses section.
 6. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
 7. To exclude a port that you do not want to be scanned, click **Add** in the Excluded Ports section.
 8. On the Add Port screen, type a port or port range and then click **OK**.

Firewall

Firewall shields your system by monitoring both inbound and outbound network connections. It analyzes all incoming connections whether it is secure and should be allowed through and checks whether the outgoing communication follows the compliance that you have set for security policies. Firewall works silently in the background and monitors network activity for malicious behavior.

You can create different policies for various groups/departments like enabling Firewall protection, applying Firewall security level with an exception rule and other settings according to the requirements. For example, you can apply security level as High for the Accounts Department and apply an exception rule by entering the policy with additional policy settings. You can also apply the Display alert message when firewall violation occurs and Enable firewall reports options. While for Marketing Department, you can create a policy with security level as Low without an exception rule and apply the Enable firewall reports options only.



The Firewall feature is available only in the clients with Microsoft Windows.

To configure a policy for Firewall setting, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In the Level option, select one of the following:
 - Block all
 - High
 - Medium

- Low
5. By default, the **Monitor Wi-Fi Networks** check box is selected. Because of this option, you get alert messages when connected with unsecured Wi- Fi network and when an attempt is detected to access unsecured client Wi-Fi (hotspot). Also, the reports are generated at the server.
 6. If you want an alert message about firewall violation, select the **Display alert message when firewall violation occurs** check box.
 7. If you want reports for all blocked connections, select the **Enable firewall reports** check box.
 8. In the Exceptions section, a list of default exceptions appears. You can add or manage the exceptions. For more information, see [Managing Exceptions](#).
 9. To restore the default settings, click the **Default** button.
 10. To save your settings, click **Save Policy**.



If the Firewall policy is set as **Block All**, Firewall will block all connections and generate many reports that may impact your network connection.

Security Level

Security Level	Description
Block all	Blocks all Inbound and Outbound connections without any exception. This is the strictest level of security.
High	Blocks all Inbound and Outbound connections with an exception rule. The exception policy can be created for allowing or denying connections either for inbound or outbound through certain communication Protocols, IP address, and Ports such as TCP, UDP, and ICMP.
Medium	Blocks all Inbound and allows all Outbound connections with an exception rule. The exception policy can be created for allowing or denying either inbound or outbound connections through certain communication Protocols, IP address, Ports such as TCP, UDP, and ICMP. For example, if you allow receiving data from a certain IP address, the users can receive data but cannot send to the same IP address. To take more advantage of this security level policy, it is advisable that you allow receiving inbound connections and block outbound connections.
Low	Allows all Inbound and Outbound connections. When you apply Low security level, it is advisable that you create an exception rule for denying particular inbound or outbound data with the help of certain Protocols, IP address, and Ports to take more advantage of the security level policy.

Managing the Exceptions rule

With Exceptions, you can allow genuine programs to perform communication irrespective of the Firewall level whether set as High or Medium. With Exceptions, you can block or allow Inbound and Outbound communication through IP Addresses and Ports.

Creating the Exceptions rule

To configure a policy with the Exceptions rule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, click **Add**.
5. On the Add/Edit Exception screen, type a name in the **Exception Name** text box.
6. Select one of the protocols from the following:
 - TCP
 - UDP
 - ICMP
 - i. Under Application, **All Applications that meet the specified conditions** option is selected by default. If you want any specific application, select **Specified Applications path** option and enter the path of application.
 - ii. If you select ICMP Protocol, do the following.
 - a. Click **Next**.
 - b. Under Local IP Address, do one of the following,
 - Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
 - Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.
 You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.
 You can delete the IP address with help of **Delete** button.
 You can also import the IP addresses from a text file using **Import** button. The maximum limit to import valid IP addresses is 25 per exception.
 - Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.
 - c. Click **Next**.
 - d. Configure ICMP Settings.

- e. Click **Finish**.
- iii. If you select TCP or UDP option for Protocol, do the following
 - a. Select one of the following options:
 - All Applications that meet the specified conditions
 - Specified Applications path
Provide full path of the application
 - b. Click **Next**.
 - c. Select one of the Direction from the following and click **Next**:
 - Inbound Connections
 - Outbound Connections
 - Inbound - Outbound Connections
 - d. Under Local TCP/UDP Ports, do one of the following,
 - Select the **All Ports** option to select all ports.
 - Select the **Specific Ports** option and type the port numbers. Use comma in between to add multiple ports.
 - Select the **Port Range** option. Enter **Start Port** Number and **End Port** Number.
 - Click **Next**.
 - e. Under Remote IP Address, do one of the following,
 - Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
 - Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.
You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.
You can delete the IP address with help of **Delete** button.
You can also import the IP addresses from a text file using **Import** button. The maximum limit to import valid IP addresses is 25 per exception.
 - Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.
 - Under Domain Name, type the Domain Name. Click **Add** to add the Domain Name. You can add multiple Domain Names here.
You can add up to 25 Domain Names per exception. However, the combined count of all Domain Names in all exceptions in a policy must be equal to or less than 255.
You can delete the Domain Name with help of **Delete** button.

You can also import the Domain Names from a text file using **Import** button. The maximum limit to import valid Domain Names is 25 per exception.

- Click **Next**.
If you mention remote IP or port, that exception will be for outgoing communications.
- f. Under Remote TCP/UDP Ports, do one of the following,
 - The **All Ports** option is selected by default.
 - Select the **Specific Ports** option and type the port numbers. Use comma in between to add multiple ports.
 - Select the **Port Range** option. Enter **Start Port** Number and **End Port** Number.
 - Click **Next**.
- g. Under Action, select either **Allow** or **Deny**.
- h. Click **Finish**.

The Exception is added at top position in the Exceptions list. The sequence of the exceptions decides the precedence of the rule. The precedence is in descending order. You can move the exception rule with the **Move Up** and **Move Down** buttons.

7. Click **Save Policy**.

Editing the Exceptions rule

You can edit the exceptions rule which are created by you if required. To edit the Exceptions rule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to edit and click the name.
5. On the Add/Edit Exception screen, you can edit the name in the Exception Name text box and edit the protocol.

The protocol includes TCP, UDP, and ICMP.

6. Click **Next**.
7. Edit Local IP Address if required, and then click **Next**.
8. Edit Local TCP/UDP Ports if required, and then click **Next**.
9. Edit Remote IP Address if required, and then click **Next**.
10. Edit Remote TCP/UDP Ports if required, and then click **Next**.
11. Under Action, you can select either **Allow** or **Deny**.

12. Click **Finish**.

13. Click **Save Policy**.

Deleting the Exceptions rule

You can delete the exceptions rule that you created. To delete the Exceptions rule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to delete.
5. Click **Delete**.

The selected exception rule is deleted.

6. Click **Save Policy**.

Exporting the Exceptions rule

You can export the exceptions rule that you created. To export the Exceptions rule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to export.
5. Click **Export**.

The Opening fwexcp.db dialog appears.

6. Select **Save File**.

7. Click **Ok**.

The database file, fwexcp.db is downloaded.

Importing the exceptions rule

You can import the exceptions rule that you created in the earlier versions of EPS. To import the Exceptions rule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. Click **Import**.

The File Upload dialog appears.

5. Select the database file, `fwexcp.db`.
6. Click **Open**.

The database file, `fwexcp.db` is imported.

7. Click **Save Policy**.

Web Security

This feature helps you create security policies for a department or group where Browsing and Phishing Protection can be enabled. This blocks malicious and phishing Web sites based on content filtering capability. You can restrict or allow access to the internet and Web sites as per your requirement.

The following table shows a comparison of the features in Web Security that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Browsing Protection	✓	✓	✓
Phishing Protection	✓	✓	✓
Web Control - Restrict access to particular categories of Web sites /Web Categories	✓	✓	✓
URL filtering - Block specified Web sites	✓	✓	✓

To create a policy for Web Security, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Web Security**.
3. Under Web Security, select either of the following or both the check boxes:
 - Browsing Protection
 - Phishing Protection
4. To get an alert message when a blocked Web site is accessed by a user, select the **Display alert message when website is blocked** check box.
5. Under Web Categories, restrict or allow access to the Web sites based on their categories as per the security policy of your organization. To enable the categories, select the **Restrict access to particular categories of Websites** check box.

Select one of the following options to access the website category:

- Allow All – When you select this option, status of all categories is Allow.
- Deny All – When you select this option, status of all categories is Deny.

- Custom – When you select this option, you can change status of the categories as Allow or Deny as per your requirement in the Status column.

If you block a category, all the Web sites under it will be blocked.

6. In Block specified websites section, enter the Web sites that you want to block. This is helpful if you are sure to block certain Web sites. To enable this section, select the **Restrict access to particular Websites** check box.
7. To schedule the internet access, select the **Schedule Internet Access** check box and do the following:

- i. Select one of the following options:

- Always allow access to the internet
- Restrict internet access

When you select the option, Allow access to the internet, you can add the schedule.

- ii. Click **Add** to add the schedule.

Add Time Interval dialog appears.

- iii. Select the **Weekday** from the list.

- iv. Select the **Start at** and **End at** hours and minutes.

- v. Click **OK**.

You can delete the schedule entry if the entry is not required.

8. You can exclude certain known websites from getting it blocked. Excluded URLs/Websites will not get blocked even if internet is restricted. To exclude the websites, do the following,

- i. Select the **Schedule Internet Access** check box.
- ii. Select the **Restrict internet access** option.
- iii. Click **Exclusions**. The Exclude URLs dialog appears.
- iv. Enter complete URL that you want to exclude.
- v. Click **Add**.
- vi. Click **Ok**.

The list of excluded URLs is displayed in the Excluded URL box.

You can delete the URL entry if the entry is not required.



SSL versions earlier than 3.1 are not supported for Schedule Internet Access.

9. Select the **Enable Web Security reports** check box if you want to generate reports for all blocked Web sites.

If you select this option, a large number of reports will be generated depending upon the Web usage.

10. To save your settings, click **Save Policy**.



The Schedule Internet Access feature is available only in the clients with Microsoft Windows and Mac operating systems.

Browsing Protection Settings

While users visit malicious Web sites some files may get installed on their systems. These files can spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious Web sites are blocked while the users in a group are accessing the Internet. Once the feature is enabled, any site that is accessed is scanned and blocked if found to be malicious.

Phishing Protection Settings

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and sites such as banks, companies and services seeking for your personal information such as credit card number, social security number, account number or password.

Administrators can enable Phishing Protection that prevents users from accessing phishing and fraudulent Web sites. As soon as a site is accessed, it is scanned for any phishing behavior. If found fraudulent, then it is blocked to prevent any phishing attempts.

Exclusion for Browsing Protection and Phishing Protection

Exclusion enables you to apply an exception rule to the protection policy for Browsing Protection and Phishing Protection. This helps you exclude the URLs of the sites that are genuine but get erroneously detected either as malicious or phishing sites. You are recommended to exclude only those URLs that you trust to be safe and genuine.

You can exclude the URLs in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Web Security**.
3. In the Web Security section, click the **Exclusion** button.

The Exclude URLs dialog appears.

4. In the Enter URL text box, type the URL and then click **Add**.

The Report Miscategorized URL dialog appears. You can report about miscategorization of the URL to the Seqrite lab if the URL is detected as malicious or phishing site.

5. Select one of the reasons from the following:
 - URL is getting detected as Malicious.
 - URL is getting detected as Phish.

6. To report about miscategorization, click **Yes**. If you do not want to report about miscategorization, click **No**.

The URL is added in the Exclude URL list.

7. To save your settings, click **OK**.

Settings	Description
Add	Helps you exclude a URL from being detected as malicious or phishing.
Delete	Helps you delete a URL from the Excluded URL list.
Report	Helps you report if a URL is miscategorized.

Web Categories

There are certain concerns that most organizations may face:

- System infection by malware.
- Users browsing unwanted Web sites.
- The employees idling away time.

To avoid these concerns the administrators need to have a policy that regulates users and their Web access activities.

The Web Categories feature helps the administrators centrally control and manage the browsing behavior of the users. The administrators can create different security policies for different groups according to their requirements and priorities.

To configure Web Categories, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Web Security**.
3. Under Web Categories, select the **Restrict access to particular categories of Websites** check box.
4. Select one of the following options to access the website category:
 - Allow All – When you select this option, status of all categories is Allow.
 - Deny All – When you select this option, status of all categories is Deny.
 - Custom – When you select this option, you can change status of the categories as Allow or Deny as per your requirement in the Status column.

The Web categories are enabled, and you can allow or deny access to each category.

Exclusion for Web Categories

Exclusion helps you apply an exception rule to the protection policy for Web Categories. This helps you when you want to restrict access to a Web site category, but you want to allow certain Web sites from the restricted category.

You can enlist such Web sites in the Exclusion list in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Web Security**.
3. In Web Categories section, select the **Restrict access to particular categories of Websites** check box.
4. Click the **Exclusion** button.
The Exclude URLs dialog appears.
5. In the Enter URL text box, type the URL and then click **Add**.
The URL is added in the Exclude URL list.
6. To exclude the subdomains, select the **Also Exclude Subdomains** check box.
7. To save your settings, click **OK**.

Settings	Description
Add	Helps you exclude a URL from being restricted even if it belongs to the blocked category.
Delete	Helps you delete a URL from the Excluded URL list.

Block specified websites

This feature is helpful in restricting access to certain Web sites or when a Web site does not fall into an appropriate category. It is also helpful if you have a shorter list of the Web sites that you would prefer to restrict the Web sites than blocking the entire category.

To block Web sites, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Web Security**.
3. On the Web Security screen, under Block specified websites section, select the **Restrict access to particular Websites** check box.
The Block specified websites features (Add, Delete, Delete All) are activated.
4. To add a Web site, click **Add**.
5. On the Add URL screen, type a URL in the Enter URL text box.
6. If you want to block the subdomains, select the **Also Block Subdomains** check box. For example, if you block `www.google.com` and select 'Also block subdomains', all its subdomains such as `mail.google.com` will also be blocked.
7. To save your settings, click **OK**.



The Also Block Subdomains feature is not applicable for the clients with Mac operating systems.

Application Control

Organizations usually face the following concerns while using applications:

- No illegal or fake applications should be installed on client systems.
- Malicious applications should not infect the systems.
- Unnecessary applications should not clog the systems.

With this feature, the administrators can authorize or unauthorize the users to access and work with certain applications, so that no one accesses an unwanted application. If the users try to access an unauthorized application, a notification can also be sent to the users about why they cannot access the application.

The administrators can create various policies based on the requirement of the groups or departments. For example, for the users of the Marketing Department, you can allow access to File Sharing Applications and Web Browser while restrict access to all other applications. For the Accounts Department, you can allow access to Archive Tools and Web Browsers only.



The Application Control feature is available only in the clients with Windows operating systems.

To create a policy for Application Control, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Application Control**.
3. To block access to an application, select the **Block unauthorized application when accessed** check box.
4. If you want to send a notification when a blocked application is accessed, select **Notify clients when an unauthorized application is blocked**.
5. Select either Authorized or Unauthorized to each application category as per your requirement.

You can also customize the setting to the application category by clicking the Custom button.

6. To save your setting, click **Save Policy**.

Custom

You can customize the application settings that would authorize or unauthorize specific applications or categories. If you authorize or unauthorize an application category, all the applications listed under that category are either allowed or blocked.

For example, from the application category 'Email Clients', you can unauthorize access to 'Thunderbird', and 'MailWasher' and authorize access to all the other applications. Similarly, for the application version 'Thunderbird', you can unauthorize access to 'Thunderbird 1' and authorize access to all the other versions of that application.

You can customize the applications in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Application Control**.
3. Under Application Control, click Custom to an application category.

Ensure that the option Block unauthorized application when accessed is selected, only then you can click the Custom option.

A list of applications under the selected application category appears. You can edit the application name, process name and application category by clicking the **Edit** link.

4. In the list of applications, select all application names that you want to mark as unauthorized.
5. To save your setting, click **Save Policy**.

Add Application

This feature allows you to add a new application to the default list. Adding and unauthorized an application or file that belongs to the operating system or other system specific aspects may cause system malfunction. Hence, it is advised to add an application that is not a part of operating system or other system related programs.

You can add an application as follows:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Application Control**.
3. In the Add Application section, click the **Custom Applications** button.
4. On the Custom Applications screen, click **Add Application**.
5. To add an application, select the option to either provide a process name or path of the application executable file.
6. In the Application Name text box, type an application name.
7. In the Application Category list, select a category.

You can also write a reason for adding a new application to the default list of applications. This helps Seqrite to improve the quality of the software product.

You can also submit the application metadata to the Seqrite lab.

8. To add the application, click **Add Application**.

Submit Application metadata to Seqrite lab

With this option, you can send metadata of an application to the Seqrite lab for including it in the application categories. Metadata includes information of application such as its Name, Version, Company Name, and MD5. You can also provide the reason for adding the application. This information will help us to improve the Application Control module.

Application Categories include thousands of applications based on their functionalities. If you block a category, all the applications in that category are blocked.

However, if you have unauthorized an application category but an application is not yet blocked, you can submit that application. Seqrite analyzes the application and then enlists it in the category.



- User may get application blocked prompt even while copying or renaming any unauthorized application.
- Some unauthorized applications may start in case the application executable is updated due to software update. Such applications can be added to Seqrite Endpoint Security Console and you are recommended to submit the Metadata to the Seqrite lab.

Advanced Device Control

While working with data storage devices such as CD/DVDs and USB-based devices such as pen drives, organizations are concerned with the following:

- Autorun feature does not activate any infection.
- Unnecessary data or applications do not clog the systems.

This feature allows the administrators to create policies with varying rights (device authentication capability). 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 admin configured devices. Once the policy is applied to a group, the access rights are also applied. You can use the exception list to exclude the devices from the device control policy.



- On Windows XP SP1 and prior operating systems, you will not be able to block devices other than USB storage devices.
- Advance Device Control feature is not supported on Apple's M1 chip.

Creating policy for Advanced Device Control

To create a policy for Advanced Device Control, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Advanced Device Control**.
3. To enable device control, select the **Enable Advanced Device Control** check box.
4. Under Select Access Policy for Device Types section, select a category from the following options:
 - Storage Device
 - Card Readers
 - Wireless – [Customize Wi-Fi connection](#)

- Mobile & Portable devices
- Interface
- Camera
- Others

5. For the corresponding device under that category select one of the following:

- Block
- Allow
- Read only



Options under any category are available only if you select the main category check box.

6. To save your setting, click **Save Policy**.

This policy is applied to all the devices that are configured in the list. Even if you add a device, the same policy will apply unless you customize the policy.

Authorize Wi-Fi connections

You can add authorized Wi-Fi access points so that only authorized Wi-Fi connection is established.

To add authorized access points, follow these steps:

1. Select the **Wireless** check box.
2. For Wi-Fi, select **Allow** or **Block if wired connection is available** option.

The **Customize** link is enabled.

3. Click the **Customize** link.

The Authorized Wi-Fi connections dialog appears.

4. If you select Allow for all Wi-Fi access points, all Wi-Fi connections can be established.
5. If you select Allow only for authorize Wi-Fi access points, enter network data to create the authorized wi-Fi connection as the following:
 - i. Enter SSID.
 - ii. Enter Mac address in hexadecimal values.
 - iii. Click **Add**.
 - iv. Click **Ok**.

You can delete the access point if not required with help of Delete button.

Note:

For Windows Clients

- Only NTFS is supported for Partial encryption.

- USB Pen Drives with GUID Partition Table (GPT) Partition Style cannot be added for authorization.
- If an authorized and encrypted device is formatted, the device will be treated as unauthorized. Hence, Administrator will need to add the device again in Device Control and configure the policies accordingly.
- USB devices connected to the systems in the network of SEPS 7.6 server will not be enumerated in **Admin Settings > Server > Manage Devices > Add Devices > Network Devices** list.
- Some devices (e.g. Nokia phones, BlackBerry phones) may need system reboot or device reattachment for device access rights to be applied.
- On blocking SATA Controller from Advanced Device Control, you may frequently see SATA Controller blocked prompts even when actual blocking is not performed.
- While any ongoing session of Webcam or Bluetooth is in progress, changing access right to block will not interrupt this current ongoing session. The device may need reattachment or system reboot for access rights to be applied.
- External CD/DVD reader will not be enumerated in **Admin Settings > Server > Manage Devices > Add Devices > Network Devices** list and also exception rule cannot be created for the same.

For Mac Clients

- If the option Read only is selected in Advanced 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 already attached to the machine and you are installing Mac client, the device may not be shown as mounted for a fraction of seconds.
- If an NTFS USB device is attached to the machine during installation of Mac client, two copies of the attached USB may be visible for a few seconds.
- If a USB device is to be shown as mounted or un-mounted using terminal commands, the Device Control policy will not apply to that device.
- If you are installing Mac client on Mac OSx 10.9 while an FAT USB device is attached to the machine, such a device will not be displayed as mounted. To show the device mounted, you need to disconnect the device and reconnect it.
- iDevices, Internal Card Reader, Webcam, CD-DVD, mobile phones and HFS encrypted devices may need device reattachment for device access rights to be applied.
- Exception functionality will not be applicable for Bluetooth, Wi-Fi, Webcam, External CD-DVD.
- Mobile phones except iDevices that are connected in 'USB Mass Storage' mode will be detected under USB storage device category.
- Mobile phones connected in MTP mode will be detected under 'Windows Portable Devices' category.

- Blocking functionality will not work for Blackberry mobile if the mobile is connected to Mac system in Sync Media.
- USB storage device won't be formatted with Mac OS extended (Journaled, Encrypted) file format.
- The 'Authorized Wi-Fi connections' feature is not supported on Mac operating system.
- Bluetooth blocking functionality does not work on macOS Monterey 12, though Device Control Blocked prompt appears.

For Linux clients

- MTP/PTP based phones are not supported, whereas UMS based phones are supported.
- The Read only option set for internal CD/DVD on the EPS server, is treated as Blocked on the Linux client.
- Wireless adaptors are not supported.
- Bluetooth USB dongle may not be supported on some operating systems.
- In all supported Linux OS, internal CD-DVD tray may open and close itself multiple times if the block mode is set for CD-DVD.
- If DC configuration is changed from Read-only mode to Allow mode, the USB drives may not work accordingly.
- UMS Mobile Phones do not work in Read-only mode. Changing the mode using the option available in the device will connect it to the endpoint. If the device is plugged out, the device in a particular mode does not change the mode automatically.
- Exception functionality will not be applicable for Bluetooth and External CD-DVD.

Adding exceptions to the device control list

You can add exceptions for removable devices that are used by authorized persons so that the devices are excluded from the policy.

To add devices to the exceptions list you must first authorize the devices by adding the device to the server as follows:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Devices**.
3. Click **Add Devices**.
4. Select from Network Devices, USB Devices, or Other Devices.

If you want to add a USB Device, select USB Device and in the Add Device dialog box, add the device name and click OK.

If you want to add a network device, select Network Devices. The list of devices detected in the network is displayed. Select the device and click OK.

If you want to add any other device, select the Other Device option, select device type, and in the Add Device dialog box, add the required details such as; Device name, Device Vendor ID, Product ID, and the serial number. Click OK,

5. Click **Settings > Client Settings > Advanced Device Control**.

Ensure that the option for Enable Advanced Device Control is selected.

6. Click **Exceptions**.

7. Click **Add**.

8. Select one or more devices to add to exception from the devices displayed in the list.

9. Click **OK**.

10. Click **Yes** to the Managed Devices confirmation dialog box.

11. Set the access permissions as required.

12. Click **Save Policy**.



The permissions set for the device added by the USB by Serial Number option has the highest priority.

Adding Device to Server

To know about how to add a device to the server, see [Manage Devices](#).

Data Loss Prevention

You can now prevent unauthorized loss, pilferage, or leakage of confidential company data using the Data Loss Prevention (DLP) feature of SEPS.

It is necessary to enable DLP on endpoints. To do this, see [Enabling DLP feature](#).

You can also view a report of the users who attempted to cause the unauthorized leakage of confidential data. See [Reports for Data Loss Prevention](#).

You can either choose to be notified through email notification when an attempt is made to leak information or prevent the attempt from being carried out successfully.

The DLP feature can stop any such unauthorized activity that is carried out through the following Data Transfer Channels:

- Using the Print Screen option to save the screenshot (Applicable only for Windows platform). The file/data is not monitored.
- Using Removable Devices to copy data (Applicable only for Windows platform). For selected File Types, the Removable Devices go to 'Read Only' mode when 'Monitor Removable Devices' option is selected.
- Using Network Share accessed using UNC Path or Mapped Network Drive (Applicable only for Windows platform).
- Using the Clipboard to paste information from one application to another.

- Using printer activity, printing through local and network printer. The file/data is not monitored. (Applicable only for Windows platform)
- Using online services of third-party Application/Services to send data such as email, file sharing apps, cloud services, Web browsers and other applications using social media.

You can also identify the type of data that you want to monitor such as:

1. File Types

- Graphic Files (Audio, Video, Images)
- Office Files (MS Office, Open Office, Kingsoft Office)
- Programming Files
- Some Other File Types (Compressed files etc.)
- Custom Extension Files

2. Confidential Data

- Confidential data such as Credit/Debit Cards
- Personal information such as Social Security Number (SSN), Email ID, Phone Numbers, Driving License Number, Health Insurance Number, Passport Number, ID, International Banking Account Number (IBAN), Individual My Number, Corporate My Number, Pin Code, Aadhar Number and Vehicle Registration Number.

3. User Defined Dictionary

To specify the words/strings that must be flagged if used in communication.



Confidential Data & User Defined Dictionary Data will not be monitored and blocked if it is in the Subject Line or Message Body of email, instant messenger communication.

Add-on Features

The DLP pack contains the following 2 add-on features.

- File Classification
- Optical Character Recognition (OCR)

File Classification

When a new Microsoft Office file is generated, DLP asks to classify the file as Confidential or Public. You can classify existing files also. Files classified as confidential are treated as sensitive files and any operation to leak is blocked/reported as per DLP policy. This is regardless of the content of the file.

Files classified as Confidential will be monitored only for the following Data Transfer Channels,

- Removable Devices
- Network Share

- Application/Online Services

To classify files, follow the given steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client settings > Data Loss Prevention**.
3. Select the **Enable Data Loss Prevention** check box.
4. In the Add-on Features section, the **File Classification** check box is enabled by default.
5. Select the **Always show pop-up to classify a new file** check box if you want to view pop-up every time when you create a new file.
6. When you create a new MS Office file, save and close it, a Seqrite File Classification dialog appears. The dialog appears only for MS Office files.
7. Select the classification level as **Public** or **Confidential**.
8. Click **OK**.

The overlay icon of classified file appears as per classification.

When you copy a file, classify the copied file as per above procedure.



The overlay icon of classified file appears after system or Windows Explorer is restarted after client is installed.

To classify existing files, follow the given steps:

1. Select the files to be classified. You can select maximum 100 files at a time.
2. Right click the selected files and select **Seqrite File Classification > classification level as Public or Confidential or Unspecified**.

A Seqrite File Classification dialog appears showing result. The lay over icon of classified files appears as per classification.

You can remove the classification, by selecting **Unspecified** option.



Manual classification is supported only on NTFS.

Optical Character Recognition (OCR)

Optical Character Recognition feature is disabled by default.

The confidential/user defined data from image files is identified in case of data leak and action is performed as per policy. The image details are mentioned in the DLP report.

OCR supports the following image formats,

- JPEG (or JPG) - Joint Photographic Experts Group
- PNG - Portable Network Graphics
- GIF - Graphics Interchange Format

- TIFF - Tagged Image File
- BMP - Bitmap image files



OCR is applicable only for the following Data Transfer Channels,

- Removable Devices
- Network Share
- Application/Online Services

Limitations

- OCR does not support embedded images scanning.
- Only Roman (English) alphanumeric script is detected from the images.
- Only clear and high-quality images are detected by OCR. The blur, distorted, too small or too large images may not be detected.

To enable the OCR feature, follow the given steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client settings > Data Loss Prevention**.
3. Select the **Enable Data Loss Prevention** check box.
4. In the Add-on Features section, select the **Optical Character Recognition (OCR)** check box.

You can view list of supported OS versions for OCR by clicking the link.



OCR feature in DLP is available in Microsoft Windows Vista SP2, Windows 7 SP1, and above Personal computer versions and Windows Server 2008 SP2, Windows Server 2008 R2 SP1, and above Server versions.



- Data Loss Prevention feature is not available in both EPS Business and Total flavor. User need to purchase a DLP pack separately to avail this feature.
- Data Loss Prevention feature is not supported with the EPS SME flavor.

Preventing leakage of data

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client settings > Data Loss Prevention**.

Select the **Enable Data Loss Prevention** check box. You can choose to select the option for an Alert message on the endpoint on which an attempt is made at data leakage.

3. Select the channels that you want to monitor from the following options:
 - Print Screen (applicable only in Windows platforms)
 - Monitor Removable Devices (applicable only in Windows platforms)

- Monitor Network Share (applicable only in Windows platforms)
 - Monitor Clipboard
 - Printer Activity (applicable only in Windows platforms)
 - Monitor Data Transfers through Application/Online Services
4. Select the applications that you want to monitor for attempts at data pilferage by clicking on the Applications drop down list. Do one of the following:
- You can select all the applications in the group.
- Select the applications one by one after expanding the group caret.
 - Select all Mac platform applications by clicking the Mac group icon.
 - Select all Windows applications by clicking on the Windows icon.
 - Select all Web Browsers or one by one after expanding the group caret.
 - Select all E-mail applications or one by one after expanding the group caret.
 - Select all Instant Messaging applications or one by one after expanding the group caret.
 - Select all File Sharing/Cloud Services applications or one by one after expanding the group caret.
 - Select All Social Other applications or one by one after expanding the group caret.
 - Select All Custom applications or one by one after expanding the group caret.
5. To configure email SSL settings, select the **Enable Email scanning over SSL** check box. This is applicable only when you select **Email** option in the Application / Online Service. Ensure that you perform the [procedure](#) to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.
6. Configure the settings for File Types, Confidential Data, and User Defined Dictionary.
7. Configure the action to be performed after the attempts is carried out, for example Block and Report or Report only.
- Alert prompts will not be displayed for Report Only action.
8. In the Configure Exceptions section, do the following:
- i. In the Domains tab, select the **Enable domain Exception** check box.
 - ii. Select the domains to exclude from Data Loss Prevention.
 - iii. In the Applications tab, select the **Enable applications Exception** check box.
 - iv. Select the applications to exclude from Data Loss Prevention.
 - v. In the Network Path tab, select the **Enable Network Path Exception** check box.
 - vi. Select the **Network Path** check box to exclude from Data Loss Prevention.
9. Click **Save Policy**.



For Mac Client:

- Confidential & User Dictionary Data will not be blocked in subject line, message body of email or messenger communication.
- Prompts and report will be generated in case if monitored file type is downloaded.
- Certain file types (POT, PPT, PPTX, DOC, DOCx, XLS, XLSX, RTF) containing Unicode data will not be blocked.

Seqrite provides you an advanced scanning feature, Data-At-Rest Scan. With this feature you can search for a particular type of data in various formats.

File Activity Monitor

This feature lets you monitor any suspicious activity related to the confidential files on your computer, a network drive or a removable drive. Apart from a default set of files, you can customize and select the file types that you want to monitor. You can monitor the selected file types for actions such as copy, delete, or rename. You can generate a report for the file activity from the Reports page.



The File Activity Monitor feature is available in the clients with Windows and Mac operating systems.

Enabling File Activity Monitor

To enable file activity monitor, follow the given steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > File Activity Monitor**.
3. Select **Enable File Activity Monitor**.
4. In the "Select File Types and Events to monitor within drives" area, place a check mark to select the drives that you want to monitor for file activity.



Selection of event is not applicable for Removable Drives, Network Drives. You can select to monitor only 'delete' activity for local drives. For Removable Drives you can select 'All Files' to be monitored.

5. In the File types list, select the file types that you want to monitor for all the drive types or you can select all the file types listed by using 'All File Types' check box.
6. In the Custom Files, you can add your own file types that you want to exclude. Click the plus sign (+) to add a new file type extension to be monitored. Use the delete icon to remove a file or folder type.
7. Enter the folder paths that you want to exclude from the monitoring, for example.
C:\JSmith.

For Mac OS, use only forward slash (/) in the folder path. Example:
/Users/Admin/ExcludeList.

To remove a folder path from the exclusions, click on the delete icon which appears when you click the list entry. If you click on the delete icon, a message box is displayed to confirm the delete action.

8. Click **Save Policy**.

Update Settings

When a work environment has a large number of systems installed, the challenge that the administrators usually face is how to update all the endpoints for security patches.

This feature allows you to create policies for taking the updates automatically for the endpoints. You can create policies that help different clients take the updates from different sources. Taking the updates from different sources reduce the load on a single server.

The following table shows a comparison of the features in Update Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Enable Automatic Update	✓	✓	✓
Show update notification window	✓	✓	X
Frequency	✓	✓	X
Update Mode	✓	✓	✓

To create a policy for Update Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Update Settings**.
3. To take the updates automatically, select **Enable Automatic Update**.
4. To display notification window when the updates are taken, select the **Show update notification window** check box.
5. Under Frequency, set the schedule when you want to take the updates.
 - Automatic
 - Custom

If you select **Custom**, Daily Start time and **Repeat after** drop down lists are activated, you can set the schedule as per your requirement.
6. Under Update Mode, when EPS is installed on private IP (Private IP natted to Public IP), the following update settings can be configured:

For local clients

- Download from Internet
- Download from Endpoint Security Server

- Download from Specified Update Servers

For remote clients

- Download from Internet
- Download from Specified Update Servers

For creating different policies, you can select different options for Update Mode.

If you select Download from Specified Update Servers, you should enter the update server locations in the list.

7. To save your settings, click **Save Policy**.



- If you select the option Download from Specified Update Servers, the Linux client will download the updates from the Endpoint Security server.
- If 'Update from Internet' option is enabled (by right clicking on Virus Protection icon at system tray) on client, the client will try to take the updates first from the Endpoint Security Server. If the server is not reachable, the updates will be automatically taken from the Internet Center.
- 'Update from Internet' feature is available only in the clients with Microsoft Windows and Mac operating systems.

Entering update server locations

If you select the Download from Specified Updates Servers option, you are advised to enter the update server location to take the updates. In case of large networks, you can also deploy multiple Update Managers. This helps load balancing as the endpoints can take the updates from different servers. If you have configured multiple Update Managers in your network, specify their URLs in this section. You can configure clients to take the updates from these locations in Client Settings.

To enter a server location, follow these steps:

1. On Seqrite Endpoint Security Dashboard, click **Home**.
2. On the Home page, click the **Update Manager** link, available next to the product name and version details.
3. On the Update Manager screen, click **Alternate Update Managers**.
4. In the Enter Update Manager URL text box, type a URL and then click **Add**.

You can arrange the URLs according to your priority. The URLs added will be available in the update server location list in Update Settings.

Internet Settings

This feature gives the administrators a wider choice of creating policies for the client modules that need Internet connection to function. You can configure different settings for the server and port so that the client modules such as; Quick Update, Spam Protection, Web Security, and Messenger have Internet connection. This is very helpful in allowing the client modules to function in a secure work environment where default Internet connection is not allowed.

To create a policy with Internet Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Internet Settings**.
3. To set the proxy setting for Internet, select **Enable Proxy Setting**.

The proxy settings details are activated.

4. In **Proxy Server**, type the sever name.
5. In **Port**, type the port number.

You can also set authentication rule if you use Firewall or proxy server. For this, type the User name and Password under Authentication.

6. To save your setting, click **Save Policy**.



The Internet Settings feature is applicable for the clients such as Microsoft Windows, Mac, and Linux operating systems.

Patch Server

This feature allows you to configure the patch server to check and install the missing patches.

To create a policy with patch server settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > Patch server**.
3. Select the **Enable Patch Server** check box.
4. Select the patch server from the list that will be used by the endpoint to check and install the missing patches.
5. Select the **Use Microsoft patch server for roaming endpoints to scan missing patches and installing them** check box.
6. To save your setting, click **Save Policy**.



The Patch Server feature is applicable only for the clients with Microsoft Windows OS; does not support Mac, and Linux operating systems.

General Settings

This feature allows you to create a policy that authorizes the clients to access client settings and change their own password, enable or disable Safe Mode Protection, Self Protection, and News Alert.

The following table shows a comparison of the features in General Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Authorize access to the client settings	✓	✓	✓
Enable Safe Mode Protection	✓	✓	X
Enable Self Protection	✓	✓	X
Enable News Alert	✓	X	X
Enable Backup data	✓	X	X
Tray Icon	✓	✓	X

To create a policy for General Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Client Settings > General Settings**.
3. To give access to the client settings, select **Authorize access to the client settings**.

Password setting is activated.

4. In Enter Password, type the password and then re-type the same password in Confirm Password.

The clients will have to use these passwords for accessing the client settings.

5. To activate Safe Mode Protection, select **Enable Safe Mode Protection**.

If you run Windows in Safe Mode, your computer starts with only basic files and drivers and the security features of Seqrite are disabled by default. In such a situation, unauthorized users may take advantage and steal data or modify the settings of the Seqrite features.

To prevent access to your system by any unauthorized users, you can configure Safe Mode Protection. Once you configure it, you need to provide a password to work in Safe Mode.

6. To activate Self Protection, select **Enable Self Protection**.

Self Protection feature helps you protect Seqrite Endpoint Security so that its files, folders, configurations and registry entries configured against malware are not altered or tampered in any way. It also protects the processes and services of Seqrite Endpoint Security. It is recommended that you always keep Self Protection on. However this option is turned on by default.

7. To get the news alert about various incidents, select **Enable News alert**.
8. Backup Data automatically and periodically (multiple times a day) takes a backup of all your important and confidential files present on the endpoint. If you update any file, then this feature automatically takes backup of the latest copy. In the Backup Data section, do the following,
 - i. The **Enable backup data** check box is selected by default.

- ii. Default Backup Location is selected by default. The backup data is stored at the default location, by default. EPS server searches all volumes on the local PC and then selects the drive with maximum free space to store the backup data locally.
- iii. Select **Enter Folder Path** option if you want to store your backup data at other location. Enter the folder path.
- iv. Select **Network Path Location** option if you want to store your backup data of all machines on a particular system in the network. Enter the **Network Path Location**. Enter **Username** and **Password**. Click **Test** to verify the location.
- v. Backup of the following file types is maintained:
 .doc, .odp, .txt, .docx, .ods, .wps, .dps, .odt, .wpt, .dpt, .pdf, .xls, .et, .ppt, .xlsx, .ett, .pptx, .odg, .rtf, .docm, .xlsm and .pptm
 You can view the list of default extensions by clicking the link **Click here to view default extensions**.
- vi. You can add custom extensions to the list as per your requirement. Enter extension and maximum file size in the text boxes.
- vii. Click **Add**. You can delete the extension with **Delete** button.
- viii. To exclude file extension from the data backup, enter the extension in Exclude File Extension box. Click **Add**. You can delete the excluded extension with **Delete** button.

While performing backup, avoid including large size files such as PST, media files to ensure stable system performance and network operations.

After successful client installation, backup starts after 6 hours.

Disable this feature if you have any other provision for data backup (Example: File server backup, Data backup server, etc.)

We have provided a backup facility with EPS. However, we recommend that you take additional backups regularly using third party software.

To restore your data, contact EPS Support Team.

9. In the Desktop Shortcut section, as per requirement, select the check boxes to create shortcuts for the following:
 - Safe Banking
 - Secure Browse.
10. You can configure number of days to change the colour of the tray icon if the client is not updated for a set number of days.
 Select number of days to turn the tray icon to red.
11. To save your setting, click **Save Policy**.

Schedule Settings

Scanning regularly keeps the systems clean and safe. In a large organization the client systems may be installed in physically separated environments.

To centrally manage all the systems about how to scan and when to initiate scanning, the administrator must have a policy. This feature helps you create policies for scheduling scans for the client systems.

You can schedule scanning for the following:

Client Scan

This feature allows you to create policies to initiate scanning the clients automatically at a convenient time. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Full System Scan). You can also enable Antimalware while scanning. This will supplement other automatic protection features to ensure that the client systems remain malware-free.

The following table shows a comparison of the features in Client Scan that are applicable for different Seqrite Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Client Schedule Scan	✓	✓	✓
Antimalware Scan Settings	✓	X	X
Boot Time Scan Settings	✓	X	X

To create a scan schedule policy for Client Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Client Scan**.
3. Configure the following settings: Client Schedule Scan, Scanner Settings, Antimalware Scan Settings, and Boot Time Scan Settings.
4. To save your settings, click **Save Policy**.



You can revert to the default settings whenever you prefer by clicking the Default button.

Client Schedule Scan

This feature helps you define scan schedules for the clients at a certain frequency.

To configure Client Schedule Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Client Scan**.

3. Under Client Schedule Scan section, select **Enable Schedule Scan**.
4. In Frequency, select either the Daily or Weekly option.
5. In Start At, set time in hours and minutes.
6. If you want to repeat scanning of your clients, select **Repeat Scan** and set the frequency after what interval the scan should be repeated.
7. To get notification when a client is offline, select **Notify if client is off-line**.
8. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.

Scanner Settings

This feature helps you define the scan mode that you prefer for scanning the clients or the items you want to scan.

To configure Scanner Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Client Scan**.
3. In Scanner Settings section, Under How to Scan, select a scan mode from the following:
 - **Quick Scan** (Scan Drive where operating system is installed)
 - **Full System Scan** (Scan all the fixed drives)
4. The Scan Priority is Low by default. You can change the priority if required.
5. To set optimal setting, select the **Automatic** option.
6. To set advanced setting, select the **Advanced** option.

If you select the Advanced option, further settings such as, scan items and scan types are activated.

7. Under Select items to scan, select any of the following:
 - Scan executable files
 - Scan all files (Takes longer time)
 - Scan packed files
 - Scan mailboxes
 - Scan archives files
8. If you select the Scan archives files option, you can set the following also:
 - Archive Scan Level: You can set up to level 16.
 - Select action to be performed when virus is found in archive file: You can select one of the actions from Delete, Quarantine, and Skip.

9. In Select action to be performed when a virus is found, select an action from the following: Repair, Delete, and Skip.

Antimalware Scan Settings

This feature helps you enable scanning for malware.

To configure Antimalware Scan Settings, follow these steps:

1. To enable scanning for malware, select the **Perform Antimalware scan** check box.
2. In Select action to be performed when malware found, select an action from the following: Clean and Skip.



Scan packed files, Scan mailboxes, and Antimalware Scan Settings are available only in the clients with Windows operating system.

Boot Time Scan Settings

This feature helps you enable boot time scan settings.

To configure boot time Scan Settings, follow these steps:

1. Under Boot Time Scan Settings, select **Perform Boot Time Scan**.

The Select Boot Time Scan Mode option is activated.

2. Select one of the following scan options:

- Quick Scan
- Full System Scan

This will schedule boot time scan on the endpoints. Boot time scan will be executed whenever the endpoint system restarts.

Application Control

This feature allows you to create policies to initiate scanning of the applications installed on the clients automatically at a convenient time. It also helps you scan all authorized and unauthorized applications present on the clients.

To create a policy for scanning applications, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Application Control**.
3. Configure the following settings: Application Control Schedule Scan and Scan and Report.
4. To save your setting, click **Save Policy**.

You can revert to the default settings whenever you prefer by clicking the Default button.



The Application Control Schedule Scan feature is available only in the clients with Windows operating systems.

Application Control Schedule Scan

This feature helps you define schedules to scan applications at a preferred or specified frequency.

To configure Application Control Schedule Scan, follow these steps:

1. Under Application Control Schedule Scan, select **Enable Schedule Scan**.
2. In Frequency, select either the Daily or Weekly option.
3. In Start At, set time in hours and minutes.
4. If you want to repeat scanning for the applications, select Repeat Scan and set the frequency of interval after which the scan should be repeated.
5. To get notification when a client is offline, select **Notify if client is off-line**.
6. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.

Scan and Report

This feature allows you to initiate scanning of the applications in various ways.

1. Under Scan and Report, select one of the following options:
 - Unauthorized applications
 - Unauthorized and authorized applications
 - All installed applications
2. The Scan Priority is Low by default. You can change the priority if required.

Tuneup

This feature helps you create policies to tune up the clients automatically at preferred time and intervals.

To create a policy for Tuneup, follow these steps:

1. Configure the following settings: Tuneup Schedule Scan and Tuneup Settings.
2. To save your setting, click **Save Policy**.

Note: You can revert to the default settings whenever you prefer by clicking the Default button.



The Tuneup Schedule Scan feature is available only in the clients with Windows Desktop operating systems.

Tuneup Schedule Scan

This feature helps you define schedules to tune up the clients at the preferred frequency.

To configure Tuneup Schedule Scan, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Tuneup**.
3. Under Tuneup Schedule Scan, select the **Enable Schedule Tuneup** check box.
4. In Weekday, select a day of the week.
5. In Start At, set time in hours and minutes.
6. If you want to repeat scanning, select Repeat Scan and set the frequency after what interval the scan should be repeated.
7. To be notified when a client is offline, select the **Notify if client is off-line** check box.
8. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.

Tuneup Settings

This feature helps you define how the tuneup process should run and what should be cleaned. You can select either or all the following options:

- Disk cleanup
- Registry cleanup
- Defragment at next boot

Vulnerability Scan

This feature helps you schedule vulnerability scan for the clients so that the clients are scanned for possible vulnerabilities. This scan helps for vulnerability assessment of the operating system on the client.

To create a policy for Vulnerability Scan, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Vulnerability Scan**.
3. Configure the following settings: Vulnerability Scan and Scan and Report.
4. To save your setting, click **Save Policy**.

You can revert to the default settings whenever you prefer by clicking the Default button.



The Vulnerability Scan feature is available only in the clients with Windows operating systems.

Scheduling Vulnerability Scan

This feature helps you define schedules to initiate vulnerability scan of the clients as per your convenience.

To schedule Vulnerability Scan, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Settings > Schedule Settings > Vulnerability Scan**.
3. Under Vulnerability Scan, select the **Enable Schedule Scan** check box.
4. In Weekday, select a day of the week.
5. In Start At, set time in hours and minutes.
6. If you want to repeat scanning, select **Repeat Scan** and then set the frequency after what interval the scan should be repeated.
7. To get notification when a client is offline, select **Notify if client is off-line**.
8. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.

Scan and Report

Under Scan and Report, select any of the following:

- Microsoft applications and other vendor applications
- Microsoft applications only
- Other vendor applications only

Data-At-Rest Scan

With this feature you can search for a particular type of data in various formats and detect any confidential data that is present in your endpoints and removable devices. To know more, see [Data-At-Rest Scan](#).



To perform Data-At-Rest scan, you must enable DLP on the endpoints. To do this, see [Enabling DLP feature](#).

To create a policy for Data-At-Rest Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console .
2. Go to **Settings > Schedule Settings > Data-At-Rest Scan**.
3. Select **Enable Schedule Scan** and set the frequency and time for the scan.
You can choose to Repeat Scan and Notify if client is offline.
4. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.
5. Select a scan mode from the following:
 - **Quick Scan** (Scan Drive where operating system is installed)
 - **Full System Scan** (Scan all the fixed drives)
 - **Scan Specific Folder(s)**: Select this option to scan a particular folder(s).

- i. Click **Configure**.
 - ii. Enter the path of the folder that you want to scan.
You can also choose to scan the subfolders by selecting the Include Subfolder check box.
 - iii. Click **Add**.
You can also remove a path from the list by clicking Remove.
 - iv. Click **Apply**.
6. The Scan Priority is Low by default. You can change the priority if required.
 7. Configure the settings for File Types, Confidential Data, and User Defined Dictionary.
 8. To save your setting, click **Save Policy**.

Patch Scan

The patch scan checks for the missing patches of the installed products and operating system on the client machine. After the check is complete, the result is generated.

To create a policy for patch scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console .
2. Go to **Settings > Schedule Settings > Patch Scan**.
3. Select the **Enable Automatic Patch Scan** check box and set the frequency and time for the scan.
You may also select **Notify if client is offline**.
4. Select minutes to run the Scheduled Scan only within specified minutes from the scheduled time. The option is selected by default.
5. In the Patch Install Settings section, select the **Automatic Install missing software patches with severity level equal to or more than:** check box and then select the severity level from the list.
6. Select the **Allow auto-restart the system** check box.
7. To exclude endpoints from installing the patches, click the **click here** link.

Exclusion for Patch Install dialog appears.

- i. You can select the Exclude endpoints having Server OS in an EPS network check box if required.
 - ii. Select the **Exclude below endpoints** check box.
 - iii. Enter endpoint name or IP.
 - iv. Click **Add**. The endpoint details appear. You can remove the endpoint. To remove, select the endpoint from the list and click **Remove**.
 - v. Click **Apply**.
8. To save your setting, click **Save Policy**.

Reports

This menu provides the latest information of all clients and keeps comprehensive logs about virus incidents, policies, and updates. It gives the latest status of all the connected online clients and the last update report of the offline clients. Use these logs to assess virus protection policies of your organization and identify clients that are at a higher risk of infection. You can use these logs to verify if the clients have the latest updates. The comprehensive reports help the Administrator to conduct endpoint forensics analysis.

Client

This feature helps you view the reports of all online and offline clients. The reports of clients are available on the following modules: Virus Scan, AntiMalware Scan, Web Security, Tuneup, Advanced Device Control, Application Control, IDS/IPS, Firewall, Vulnerability Scan, File Activity Monitor, and Asset Management.

Viewing Reports of Virus Scan

This feature helps you generate reports about whether any virus is found after scanning the clients through the Virus Protection, Scanner Scheduler, Memory Scan, Email Protection and Anti-Ransomware modules.

To view reports of Virus Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Virus Scan > Virus Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text field. The reports will be generated for that endpoint name.

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

The report can be displayed both in Chart and Tabular forms.

7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
File Name	Displays the file names that are infected with viruses.
Virus Name	Displays the virus names that infect the files.
Action Taken	Displays the actions that were taken against viruses.
View Details	Displays further details for a report. To view the details, click the View Details link.

Viewing Reports of Unscanned Endpoints

You can view the number of endpoints not scanned in the last 1 day to 30 days. This facilitates you to decide on which endpoints the scanning needs to be started.

To view reports of unscanned endpoints, follow these steps:

1. Go to **Reports > Client > Virus Scan > Unscanned Endpoints**.
2. This page gives a doughnut chart and a table which displays the number of endpoints not scanned for the following time periods:
 - Last 1 Day: Displays the report of the last one to two days.
 - Last 3 Days: Displays the report of the last three to six days.
 - Last 7 Days: Displays the report of the last seven to fourteen days.
 - Last 15 Days: Displays the report of the last fifteen to twenty-nine days.
 - Last 30 Days: Displays the report of the last thirty or more days.

You can print the report by clicking the **Print** option.

Clicking on the endpoint count, opens a window with details of the unscanned endpoints. You can save this report in the csv format.

Viewing Reports of AntiMalware Scan

This feature helps you generate reports about whether any malware is found after scanning the clients through the Schedule Scan and On Demand Scan modules (Clients > Client Action > Scan).

To view reports of Antimalware Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > AntiMalware Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

The report can be displayed both in Chart and Tabular forms.

7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Name of Malware	Displays the malware names.
Type of Malware	Displays the malware types.
Action Taken	Displays the actions that were taken against the malware attack.

Viewing Reports of Web Security

This feature helps you generate reports on whether any Web sites were blocked through the Browsing Protection, Phishing Protection, or block Web sites modules (Settings > Client Settings > Web Security).

To view reports of Web Security, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Web Security**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a group name and an endpoint name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.
The report can be displayed both in Chart and Tabular forms.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click **Modify Parameters**.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

Note: In case of SME flavor of Seqrite endpoint Security, only the tabular format report for Web Security is available.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Blocked Web sites	Displays the Web sites that were blocked.
Category	Displays the category of blocked Web sites belong to.

Viewing Reports of Tuneup

This feature helps you generate reports on how many clients were tuned up and how many were not tuned up at all (Clients > Client Action > Tuneup).

To view Tuneup reports, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Tuneup**.
The reports are displayed in chart format.
3. To generate reports for a group, select the Group Name.

4. Enter user name in the **User Name** text box.
5. Select the **Report Type**.

The report can be displayed both in Chart and Tabular forms.

6. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click **Modify Parameters**.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can print it or save it as csv or PDF.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when Tuneup is performed.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Tuneup Status	Displays whether the client was tuned up.
Last Performed	Displays when last Tuneup was performed.

Viewing Reports of Advanced Device Control

This feature helps you generate reports on policies for device control such as, whether removable devices have been blocked and what actions were taken against unauthorized devices (Settings > Client Settings > Advanced Device Control).

To view reports of Advanced Device Control, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Advanced Device Control**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

The report can be displayed both in Chart and Tabular forms.

7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.



Device Control prompts and reports will not be generated for "Network Share".

This report page for Advanced Device Control displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Device Name	Displays the device name that breached the policy.
Device Type	Displays the device type of the device.
Serial Number	Displays the serial number of the device.
Action Taken	Displays the action that was taken against the violation of the Device Control policy.

Viewing Reports for Data Loss Prevention (DLP)

This feature helps you generate, and view reports related to attempts at pilfering or copying data in an unauthorized manner. The report pinpoints the user, endpoint on which the attempt was carried out, the time and channel of operation.

On Access Scan

To receive the data for specific time period with the help of On Access Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Data Loss Prevention > On Access Scan**.
3. Enter the start date and end date for the period for which you want the data.
4. Select the Group name.
5. Enter the endpoint name.
6. Enter user name in the **User Name** text box.
7. Select the Report Type i.e. Chart or Tabular.
8. Select the channel through which the suspected activity might be carried out.
9. Click **Generate**.

After clicking Generate button, a summary is displayed. If you want to change the parameters, click **Modify Parameters**.

The tabular report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the start date of the report.
Endpoint Name	Displays the name of the endpoint.
Group Name	Displays the name of the Group.
Domain	Displays the name of the domain.
User Name	Displays the name of the user.
IP Address	Displays the IP address of the endpoint.
Source	Displays the path of the file from where its data was copied or accessed.
Content Type	Displays the type of content which was accessed.
Matched Item	Displays the subtype of content which was accessed.
File Path	Displays the path of the file from where its data was copied or accessed.
Channel	Displays the channel through which the suspected activity was carried out.
Channel Details	Displays the details of the channel through which the suspected activity was carried out.
Sender	Displays the email ID of the sender.
Receiver	Displays the email ID of the receiver.
Subject	Displays the subject of the email.
Action Taken	Displays the action taken to monitor the suspected activity.

On Demand/Schedule Scan

This scan generates and lets you view a report for confidential information and user defined dictionaries in the selected endpoints. The report also displays matching text as per your search criteria that is found while scanning. For more information about how to scan, see [Data-At-Rest Scan](#).

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Data Loss Prevention > On Demand/Schedule Scan**.
3. Enter the start date and end date for the period for which you want the data.
4. Select the Group Name and enter the Endpoint Name.
5. Enter user name in the **User Name** text box.
6. Select Report Type i.e. Chart or Tabular.
7. Select the type of content to be scanned.
8. Click **Generate**.

You can print or export the report in csv or PDF formats.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the name of the domain.
User Name	Displays the name of the user.
Scan Type	Displays the type of scan, either On Demand or Schedule Scan.
Confidential Data Incidents	Displays the total number of confidential data located when scanning.
Data Dictionary Incidents	Displays the total number of user defined dictionary data located when scanning.
Details	Displays the details of Data-At-Rest scan.

Viewing Reports for Application Control

This feature helps you generate reports on how many applications were accessed or installed or whether they were authorized or unauthorized applications.

The reports on Application Control can be generated for On Access Scan and Application Installed separately.

On Access Scan

To view reports for On Access Scan, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Application Control**.
3. On the General Reports page, click the **On Access Scan** tab to generate reports of the applications that were accessed.
4. Select the start and end dates for the reports.
5. Select a Group Name and an Endpoint Name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text field. The reports will be generated for that endpoint name.

6. Enter user name in the **User Name** text box.
7. Select the Report Type.
The report can be displayed both in Chart and Tabular forms.
8. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
User Name	Displays the user name that belongs to the domain.
Blocked Application	Displays the applications that were blocked.
Application Version	Displays the version of the applications that were blocked.
Application Category	Displays the category of the blocked applications.
Application Path	Displays the path of the blocked applications where they were installed.

Application Installed

To view reports for Application Installed, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Application Control**.
3. On the Generate Reports page, click the **Application Installed** tab to generate reports.
4. Select the start and end dates for the reports.
5. Select a Group Name and an Endpoint Name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

You can take the print of the generated report or can also save the report as csv or PDF using the respective buttons.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.

User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Group Name	Displays the group name that the selected client belongs to.
Module Name	Displays the module name that scanned the applications.
Summary	Displays the summary of the installed applications.
View Details	Displays further details of the installed applications. To view the details, click the View Details link. It also includes information of what authorized and unauthorized applications are present on client machine.

Viewing Reports of IDS/IPS

This feature helps you generate reports on whether there was any Port scanning attack, DDOS (Distributed Denial of Service) attack, or any attempt of intrusion, and what actions were taken.

To view reports of IDS/IPS, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > IDS/IPS**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group name and an Endpoint name.

If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.

5. Enter user name in the **User Name** text box.
6. In Report For, select the attack type for which the report is to be generated.

The report can be generated for the following modules: Intrusions Prevention, Port Scanning, and DDOS Attack.

7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

You can take the print of the generated report or can also save the report as csv or PDF using the respective buttons.

This report page on Intrusion Prevention displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.

System IP	Displays the IP address of the endpoint for which the report is generated.
Attacker IP	Displays the IP address of the attacker.
Vulnerability Detected	Displays the vulnerability detected in a client.
Action Taken	Displays the actions that were taken against the attack.
View Details	Displays further details of the installed applications. To view the details, click the View Details link.

This report page on Port Scanning displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
System IP	Displays the IP address of the endpoint for which the report is generated.
Attacker IP	Displays the IP address of the attacker.
Attacker MAC Address	Displays the MAC address of the attacker.
Scanned Ports	Displays the Ports that were scanned.
Action Taken	Displays the actions that were taken against the attack.

This report page on DDOS displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
System IP	Displays the IP address of the endpoint for which the report is generated.
Attacker IP	Displays the IP address of the attacker.
Attacker MAC Address	Displays the MAC address of the attacker.
Action Taken	Displays the actions that were taken against the attack.

Viewing Reports of Firewall

This feature helps you generate reports on the protection policy for Firewall such as; the blocked connection for communications (Inbound or Outbound) and Firewall security level (Settings > Client Settings > Firewall).

To view reports of Firewall, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Firewall**.
3. On the Generate Reports page, click the **firewall** tab to generate reports.
4. Select the start and end dates for the reports.
5. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page on Firewall displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Local IP	Displays the local IP address.
Remote IP	Displays the remote IP address.
Protocol	Displays the Protocol name.
Direction	Displays the direction of the blocked communication connection.
Firewall Level	Displays the level of the Firewall security policy.
View Details	Displays further details of the installed applications. To view the details, click the View Details link.

Viewing Reports of Wi-Fi

This feature helps you generate reports about the Wi-Fi connection. The reports give details about the endpoints when connected to unsafe Wi-Fi.

To view reports of Wi-Fi, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Firewall**.
3. On the Generate Reports page, click the **Wi-Fi** tab to generate reports.
4. Select the start and end dates for the reports.
5. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

Collapsible Summary appears. Moreover, you can change the parameters by using **Modify Parameters** button.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page on Wi-Fi displays the following details of the clients.

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Wi-Fi Name	Displays the name of the Wi-Fi connection.
Physical Address	Displays the physical address of the endpoint.
Events	Displays the event when connected to unsecured Wi-Fi. Example: Connection to unsafe Wi-Fi detected.

Viewing Reports of Vulnerability Scan

This feature helps you generate reports on vulnerabilities present in the endpoints in the network. Reports can be filtered based on any of the following categories:

- All Vulnerability
- Severity

- Vendor
- Top Vulnerability

To view reports of Vulnerability Scan, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Vulnerability Scan**.
3. On the Generate Reports page, select the start and end dates for the reports.
4. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

5. Enter user name in the **User Name** text box.
6. In Report Type, select the type of report you want to generate.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, collapsible summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page on Vulnerability Scan displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Vulnerability ID	Displays the unique CVE-ID of a vulnerability incident.
Vulnerability Title	Displays the description of a vulnerability incident.
Severity	Displays the criticality of a vulnerability incident.
Vendor	Displays the name of a vendor from where the vulnerability is reported.
View Details	Displays further details of the vulnerability. To view the details, click the View Details link.

Viewing Reports for File Activity Monitor

This feature lets you view reports for suspicious file activity as per the configured settings. You can generate the reports using the following parameters:

- Start date

- End date
- Location
- Group name
- Endpoint name
- Event

Reports are available in a tabular format or a pie chart format. The report also displays the information about the attempts made, the name of the user, the endpoint name and the number of incidents for all the local, network or removable drives. You can click on the link above the charts to view the file type split up against locations. You can also view a summary of the activity for a particular file type such as deleting a file. You can view the file activity related to a person.

Viewing reports for file activity

To view file activity reports, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > File Activity Monitor**.
3. In the Generate Reports section, enter the start date and end dates between which you want to monitor file activity.
4. Select the location, group name, Endpoint name and the type of event you want to monitor.
5. Enter user name in the **User Name** text box.
6. Click **Generate**. The report is generated and displayed on the screen. You can switch between a tabular view and a pie-chart view.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as csv or PDF.

This report page for File Activity Monitor displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
File Name	Displays the file name which is being monitored.
Location	Displays the type of Drive.
User Name	Displays the user name that belongs to the domain.

Details	Displays the details of the event.
---------	------------------------------------

Viewing Reports for Asset Management

The Asset Management tab on the Reports page lets you generate reports related to the assets or the Endpoints. You can generate these reports for a particular period, group-wise, or for a particular Endpoint. Reports are available in a bar and chart format. You can also choose the category of report required, i.e. a hardware changes report or a software changes report. You can print these reports if required.

Viewing reports for asset management

Asset Incidents

To view asset Incidents reports, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Asset Management**.
3. Select the **Asset Incidents** tab.
4. In the Generate Reports area, enter or select the criteria for the required report. You can generate a report for a particular period, or select the type of report required, or look up the report for a particular endpoint by entering the name of the endpoint in the corresponding field.
5. Enter user name in the **User Name** text box.
6. Select the Report type, whether bar chart or tabular.
7. Select the **Category**, Hardware Changes or Software Changes.
8. Click **Generate**. The report is displayed on the screen. Use the Print icon if you want to print the report.

In case of Hardware changes, number of changes for top endpoints are displayed. Clicking the count, opens a window with details of hardware changes.

In case of Software changes, number of changes for top endpoints are displayed. Clicking the count, opens a window with details of software changes i.e., Software installed, uninstalled and updated. When you move the pointer over the Software Name, a tool tip displays the path of the software.

You can save these reports as csv or PDF.

Current Assets

To view current asset reports, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Asset Management**.
3. Select the **Current Asset** tab.

4. In the Generate Reports area, enter or select the criteria for the required report. Select the Operating System, System Manufacturer, Processor, Last Shutdown Before, RAM or Application Name.

Click **Generate**. The report is displayed on the screen. Use the Print icon if you want to print the report. You can also save the report as csv or PDF.

Viewing Reports of Patch Management

This feature helps you generate reports about the patches. The reports display details about the patches installed on the endpoints in the network.

You can generate the reports using the following parameters:

- Start date
- End date
- Group name
- Endpoint name
- Report Type
- Severity
- Patch status

Reports are available client wise or patch wise in a tabular format. The report also displays the information about the domain, name of the patch, name of the application, vulnerabilities targeted, scan type, and patch status. You can also view the details of the patch.

To view reports of patches, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Patch Management**.
3. Select the start and end dates for the reports.
4. Select a Group name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

5. Enter user name in the **User Name** text box.
6. Select **Report Type**, **Severity** and **Patch Status**.
7. To generate the report on the selected parameters, click **Generate**.

A summary report appears. Moreover, you can change the parameters by using **Modify Parameters** button.

You can print the report by clicking the **Print** option. You can also save the report as csv or PDF format.

8. To view the patch details, click the **Patch Title** link.

Patch Details dialog appears. You can print the patch details by clicking the **Print** option. You can also save the patch details as csv or PDF format.

9. Click **Close**.

The patch-wise report page displays the following patch details:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Patch Title	Displays the name of the patch in the hyperlink format. You can click the name to view details of the patch.
Severity	Displays the severity of the missing patch.
Category	Displays the category of the installed patch.
Application	Displays the name of the application. Example, Windows 8
Scan Type	Displays the type of scan.
Patch Status	Displays status of the patch.

The client-wise report page displays the following patch details:

Fields	Description
Endpoint Name	Displays the name of the endpoint for which the report is generated.
Domain	Displays the domain to which the selected client logs in.
Scanned Patches	<p>Displays the count of scanned patches.</p> <ol style="list-style-type: none"> 1. To view the list of scanned patches, click the count. The list of scanned patches appear in a new dialog. 2. To view the patch details, click the Patch Title link. Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format. 3. Click Close to close the window.
Patch Downloaded	<p>Displays the count of downloaded patches.</p> <ol style="list-style-type: none"> 1. To view the list of downloaded patches, click the count. The list of downloaded patches appear in a new dialog. 2. To view the patch details, click the Patch Title link.

	<p>Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format.</p> <p>3. Click Close to close the window.</p>
Installed Patches	<p>Displays the count of installed patches.</p> <ol style="list-style-type: none"> 1. To view the list of installed patches, click the count. The list of installed patches appear in a new dialog. 2. To view the patch details, click the Patch Title link. <p>Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format.</p> <p>3. Click Close to close the window.</p>
Installation Failed	<p>Displays the count of failed installation of patches.</p> <ol style="list-style-type: none"> 1. To view the list of failed installed patches, click the count. The list of failed installed patches along with installation error message appear in a new dialog. 2. To view the patch details, click the Patch Title link. <p>Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format.</p> <p>3. Click Close to close the window.</p>

Viewing Reports of Backup Data

This feature helps you generate reports when backup is failed. The reports display the reason for the failure of backup.

You can generate the reports using the following parameters:

- Start date
- End date
- Group name
- Endpoint name

To view reports of Backup Data, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Client > Backup Data**.
3. Select the start and end dates for the reports.
4. Select a Group name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

5. To generate the report on the selected parameters, click **Generate**.

A summary report appears.

You can print the report by clicking the **Print** option. You can also save the report as csv or PDF format.

Server

This feature helps you check the event logs of all the incidents that took place on server. The OTP generation logs for temporary device access also appears.

To view the event logs on Server, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Server**.
3. Select the start and end dates for the reports.
4. On the Event Logs page, select the category for the reports.

You can print the report or save the report in csv or PDF format using their respective buttons. You can also delete the event logs, if you prefer.

Fields	Description
Delete	Helps you delete the event logs.
Print	Helps you take the print of the event logs.
CSV	Helps you save the report in csv format.
PDF	Helps you save the report in PDF format.

Manage

This feature helps you manage the reports generated on server and client. You can set when the reports can be removed automatically. You can also export the reports and delete them manually.

Settings

This feature helps you set to email the reports in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Manage > Settings**.
3. On the Settings page, set the following:

- In Automatically delete reports older than...days, you can edit the number of days when the reports should be deleted automatically. It is recommended to keep older reports for no longer than 90 days. Not removing older reports can impact the performance. The number of days is set in the Installation wizard.
- In Automatically email reports for past... days to following recipients, set the number of past days for which the reports are required.
- In the Email Address text box, type the email addresses.
If you type multiple email IDs, separate them by a comma.

4. Under Email Frequency, set frequency and time when the reports should be sent.
5. Under Select Reports to email, set the types of reports that you want to email.
6. To save your settings, click **Save**.

Note: If any module contains more than 1000 records, then only latest 1000 records will be emailed.

Export

This feature helps you export the reports in PDF in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Reports > Manage > Export**.
3. Under Select Criteria, select what reports you want to export from the following:
 - To export all the reports, select **All Reports**.
 - In As per below criteria, set the criteria such as start date and end date, select a group name, and then type an endpoint name.
4. Under Select Reports, select the modules for which you want to export the reports.
The modules of the flavor of Seqrite Endpoint Security that you might have purchased are displayed.
5. After setting all the criteria, click **Export** to export the reports in PDF.

Delete Reports

This feature helps you delete the reports manually in the following way:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Reports > Manage > Delete Reports**.
3. Under Manually delete reports, select one of the following options:
 - **Delete reports older than ... days:** Select the number of days to remove the reports older than the selected days.

You can select either 30 days, 60 days, or 90 days. It is recommended to keep older reports for no longer than 90 days. Not removing older reports can impact the performance.

- **Delete all reports:** Select this option if you want to remove all the reports generated till date.

4. Under Select Reports, select the report types that you want to remove from the following:

- Clients Reports
- Server Reports

5. Click **Delete** to remove the reports.

Admin Settings

The Admin Settings section includes the following topics:

Server

This feature allows you to configure various settings related to server. This includes settings on how to send notifications and for what reasons, SMTP settings, and adding devices to allow access, redirecting server in case of need, and managing users.

Change Password

To prevent unauthorized users from modifying your settings or removing the Seqrite client from endpoints it is advisable that you password-protect Seqrite Endpoint Security. Seqrite Endpoint Security requires you to specify a console password; however, you can modify your password from the Seqrite Endpoint Security.

To change the console password, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Change Password**.
3. In the Old Password text box, type current Super Administrator Password.
4. In the New Password text box, type the new password, and then retype the new password in the Confirm Password text box.
5. Click **Apply**.

Change Email Address

Here you can see your registered Email address. If required, you can change the Email address.

To change the Email address, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Change Email Address**.
3. In the Email Address text box, edit the Email address
4. Click **Apply**.

Notification

This feature helps you set rules for sending notifications for various events such as when virus is detected, virus is active in memory, virus outbreak or ransomware detected on endpoints. Notifications are sent against intrusion detection, if an unauthorized device or application is accessed or virus definitions get outdated. This also includes alerts for failure of synchronization with Active Directory, or any license related information etc. Notifications keep you informed about the incidents occurring across the network so that appropriate action can be taken to avoid any mishap.

Notification includes the following:

- Email & SMS Notification for various incidents.
- Configure Email & SMS for Event Notification for creating a list of Email IDs and Mobile Numbers for sending SMS.
- You need to configure the mobile numbers without country code.

Email & SMS Notification

To configure Email & SMS Notification, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Notification**.
3. To activate notifications to be sent, select the **Select Event** for which notification should be sent option under Email & SMS Notification.

All other options under Notifications to be sent are activated.

4. Under Virus Infection and Virus Outbreak, select the mediums through which you want to get the notification for the following incidents:
 - Virus detected on endpoint
 - Virus active on endpoint
 - Virus outbreak in network
 - Ransomware detected on endpoints

You can get notifications either through Email or SMS or both. However, for Virus detected on endpoints, you can get the notification only through email.

If you select the option Virus outbreak in network, you can further customize the settings on when you want the notifications. This alerts you on virus outbreaks.

To customize Virus outbreak in network, follow these steps:

- Next to Virus outbreak in network, click **Customize**.
- The Virus Outbreak details screen appears.
- Under Total number of virus incidents exceeds, set number of incidents and the number of systems on which the virus outbreak happens.

- Under And in the time span of, set time about how often the notification will be triggered.
 - To save your setting, click **Save**.
5. Under IDS/IPS, select the events for which you want to get notifications:
 - Intrusion detected on endpoint
 - Port Scanning incident detected on endpoint
 - DDOS Attack detected on endpoint

Note: The notification for Intrusion Prevention can be sent through emails only.
 6. Under Advanced Device Control, select the events for which you want to get notifications:
 - Attempt to breach the Device Control policy

Note: The notification for Device Control event can be sent through email only.
 7. Under Application Control, select the events for which you want to get notifications:
 - Attempt to access unauthorized application

Note: The notification for Application Control event can be sent through email only.
 8. Under Update, select the medium through which you want to get the notification for the following incidents:
 - Service pack is available
 - Endpoints are not updated with the latest virus definitions
 - Virus definitions of Update Manager are outdated
 - Virus definitions of Update Manager are updated

Note: The notification for Endpoints are not updated event can be sent through email only.
 9. Under Install through Active Directory, select the medium through which you want to get the notification for the following incidents:
 - Synchronization with Active Directory failed
 10. Under Disconnected Endpoints, select the events for which you want to get notification:
 - Endpoint disconnected from the network due to infection
 - Endpoint disconnected from the network due to DDOS Attack
 - Endpoint disconnected from the network due to Port Scan

Note: The notification for all incidents can be sent through email only.
 11. Under License related, select the medium through which you want to get notification for any of the following incidents:
 - License expired
 - License is about to expire

- License limit exceeds
12. Under Data Loss Prevention, enable notification for event:
 - Attempt to breach Data Loss Prevention policy
 13. Under Asset Management, enable notification for event
 - Hardware changes made in the Endpoint
 14. Under Client Deployment, enable notification for event
 - Endpoint installation successful
 - Endpoint uninstallation successful
 - Unprotected Endpoints
 15. To save your setting, click **Apply**.

Configuring Email & SMS for Event Notification

To configure Email & SMS Event Notification, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Notification**.
3. In Configure Email & SMS for Event Notification, click **Configure**.
The Email & SMS Notification prompt appears.
4. In the List of Email IDs, type an email address and then click **Add**.
You can enter multiple email addresses.
5. In the List of Mobile Numbers, type a mobile number and then click **Add**.
6. To save the email addresses and mobile numbers, click **Apply**.
7. To save your setting, click **Apply**.

Note: For receiving email notifications, you will need to configure SMTP settings first.



- Currently notification through SMS facility is available only for the users based in India and UAE.
- For some events, SMS Notification may not be applicable.
- Mobile numbers listed in the National Do Not Call Registry (DND) list may or may not be able to receive notification depending on the Indian government's current telephone regulatory policies.

Buy Now

This feature helps you buy Seqrite Endpoint Security SMS bundle for sending notification.

The Number of SMS left section displays the number of SMS notifications that can be sent. As you send the notifications, this limit is consumed. To continue sending notification, you need to have SMS limit that you can increase by buying the SMS bundle.

You can buy the SMS bundle in any of the following ways:

- By clicking the Buy Now link: This link will redirect you to the portal of Seqrite Endpoint Security SMS bundle for notification where you can buy SMS bundle.
- By visiting the online portal directly: You can also visit the online portal directly to buy the SMS bundle. The URL for SMS bundle is <http://www.seqrite.com/psms>.

On the shopping portal, follow the instructions about how to buy the SMS bundle.

As soon as you buy the SMS bundle, the limit in the Number of SMS left option gets updated with due limit. If you find that the limit has not been reflected, you can update it by clicking the Update License Information button.

You can refresh the SMS bundle limit by updating the license information in the following way:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Home > View License** link.
3. On the License Manager, click the **Status** button.
4. On the License Status screen, click the **Update License Information** button.

Your license is refreshed to display the updated balance.

SMTP Settings

This feature helps you set the SMTP Host Details. All emails from Seqrite Endpoint Security such as Notification mails and Report mails will be sent to the SMTP Server for further routing.

To configure the SMTP Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > SMTP Settings**.
3. In the SMTP Server text box, type the IP Address or domain name of SMTP server.
4. In the Port text box, type the port number.
5. In the Notify from Email Address text box, type the email address.

This email address will appear as From Address in all the emails sent from EPS server.

6. For user authentication, type the user name in the User name text box.

The User name field depends on your SMTP server. It may ask you to provide either user name or email ID.

7. In the Password text box, type the password.
8. In User Authentication Method, select one of the following:
 - None: Select this option to send email notification through HTTP protocol.
 - SSL: Select this option to send email notification through SSL (Secure Sockets Layer) protocol.

- TLS: Select this option to send email notification through TLS (Transport Layer Security) protocol.
9. Seqrite recommends that to ensure the SMTP host details are correct, test the SMTP settings. To test the SMTP settings, click **Apply**, and then click **Test SMTP Settings**.
 10. In the Test Mail dialog, in the **To** text box, enter the email ID of the user.
 11. Click **Send Mail**.



EPS cannot send emails if the SMTP settings are configured using public mail server (Example: Gmail) and if Allow less secure apps setting is disabled in the public mail servers.

Manage Devices

This feature helps you to authorize all USB Devices and system internal devices (Example: Bluetooth, Webcam). Authorized devices can be allowed or blocked at EPS client system when configured through policy. This authorization must be done for every USB storage device to manage the devices in the EPS environment.

Cleaning USB device

Before adding a device to the Device Control tool (dcconfig tool), clean the disk.

To clean the disk, follow these steps:

1. Connect the device.
2. On the command prompt, type the following commands one by one:

```
diskpart
list disk
Select disk <#>
clean
convert mbr
```

3. After clean up, create partition on the disk.

Now the disk is ready to be added.

Viewing details of devices

To view details of devices, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Devices**.

A list appears which contains devices which can be added to the device exceptions in Device Control settings.

The list displays the following details of the devices:

Fields	Description
Device Name	Displays the device name.
Device Type	Displays the device type of the device.
Endpoint Name	Displays the name of the endpoint.
Serial Number	Displays the serial number of the device.
Model Name	Displays the model name of the device.
Encryption Status	Displays one of the following encryption type of the devices, <ul style="list-style-type: none"> • Not encrypted • Partially encrypted • Fully encrypted
Authorized	Displays status of the encryption, whether Yes / No

Adding device where EPS client is installed/ not installed

To add the device where EPS client is installed/ not installed, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Connect the clean device.
3. Go to **Admin Settings > Server > Manage Devices**.
4. Select **Add Devices > USB Devices**. Add Device dialog appears.
5. Click the link **click here** to download Device Control package.
6. Extract the zip file DEVCTRL.7Z.
7. From the devctrl folder, double click the `dcconfig.exe` file.
8. The device details appears in the Device control dialog. In the **Device name** box, enter device name.
9. To authorize the device, do one of the following:
 - If you are using the system where the EPS client is installed, the available encryption options are:
 - No encryption
 - Partial encryption
 - Full encryption
 - If you are using the system where the EPS client is not installed, encryption is not available.
 - To apply the encryption, refer the following table:

Encryption	Action
No	<ul style="list-style-type: none"> • Clear the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Partial	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Full	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Select the Encrypt this device check box. • When you apply the full encryption, Format window appears. Format the device.

10. Click **Save to File**. A file `dcinfo.dat` is created.
11. Save `dcinfo.dat` file in the `devctrl` folder.
12. Go to **Admin Settings > Server > Manage Devices**.
13. Select **Add Devices > USB Devices**. Add Device dialog appears.
14. Click **Browse** and upload file `dcinfo.dat`.
15. Click **Apply**.

The device is added to the device exceptions and appears in the list.

Adding device in the dcconfig tool through Admin folder

To add device in the dcconfig tool through Admin folder

1. Connect the clean device.
2. On the Seqrite Endpoint Security server, browse to the folder "<installation directory>\Seqrite\Endpoint Security 7.60\Admin"
3. Double click `dcconfig.exe` file. Device Control dialog appears.
4. Click **Retrieve** button to view the details of the device attached.
5. The device details appears in the Device control dialog. In the **Device name** box, enter device name.
6. To authorize the device, the available encryption options are:
 - No encryption
 - Partial encryption
 - Full encryption

To apply the encryption, refer the following table:

Encryption	Action
No	<ul style="list-style-type: none"> • Clear the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Partial	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Full	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Select the Encrypt this device check box. • When you apply the full encryption, Format window appears. Format the device.

7. Click **Add**.



Partial encryption supports only NTFS. No encryption and full encryption support all the file systems.

Adding exceptions to the device control policy

You can add exceptions for removable devices that are used by authorized persons so that the devices are excluded from the policy.

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Devices**.
3. Select the device category from the **Add Devices** drop down list. The following device categories are displayed:
 - **Network Device:** A list of devices connected to the network is automatically displayed. Select the devices that you want to manage. Click **OK**.
 - **USB Devices:** Use this option if you want to add a USB device that is not in the Network Device list and not connected. For more information, see [EPS server is installed](#) or [Adding device where EPS client is installed/ not installed](#).
 - **USB by Model:** Use this option. If your organization has a large number of USB storage devices of the same make and model. You can add these USBs by model name. The Add device by Model Name dialog box appears. Enter the **Device Name**. Select a mode from the **Add Model Name** list box. The following modes are displayed:
 - **Automatically:** The device model name is automatically displayed if a USB mass storage device is attached to the Windows operating system.

Automatically fetching of model name is not supported on Mac operating system.
 - **From the list:** A list of pre-specified device model names appears. Select a model name from the list.

- **Manually:** Enter **Model Name**. Follow the procedure mentioned on the dialog box.



If same USB storage device is authorized as USB Device and USB by Model, the priority will be given to the Model name.

- **USB by Serial Number:** Use this option to add the USB by serial number without connecting the USB. The Add device by Serial Number dialog box appears. Enter the **Device Name**. Enter the **Serial Number**. Click **OK**.
 - **Other devices:** Use this option if you want to add a device that is not connected, and not in the list. Select the device type and enter the corresponding details for that device.
4. Select the devices that you want to manage from the displayed list and click **OK**.
After the device appears in the list, toggle the button under **Authorized** to Yes or No as required. You can also use the Edit icon that appears to change the device name as it appears or use the Trash box icon to delete the device from the list.
Note: If you set the device authorized permission to 'No', then that device cannot be added to the exceptions list.
 5. To add the device to the exceptions list, go to Settings > Client Settings > Advanced Device Control.
 6. Click **Exceptions**.
 7. Click **Add**. The Managed Devices dialog box displays the list of authorized devices.
 8. Toggle the **Add to Exceptions** button for that device.
 9. Click **OK**.
 10. Click **Yes** on the Managed Devices confirmation dialog box. The device is now added in the list of exceptions.
To delete a device, select the device, and then click the Trash icon that appears.
 11. Set the access permissions as required.
 12. Click **Save Policy**.



- In case you are accessing Web console on Windows Vista, turn off the 'Protected Mode' option in Internet Explorer.
- If you are unable to add devices through the Web console, you can also use the Device Control Tool to add USB Storage devices. This tool is available at the following location on the EPS Server: <Installation folder>\Admin\dcconfig.exe
- Add device functionality will not work with Edge browser on Windows 10 operating system and on Google Chrome 44 and later versions.

Data Loss Prevention

For Data Loss Prevention, you can do the global settings for the following features:

- User Defined Dictionary
- Domain Exceptions
- Custom Extensions
- Applications
- Network share Exceptions

User Defined Dictionary

You can add certain key words, or phrases that might contain, or refer to confidential information in the User Defined Dictionary. If any of the documents on your endpoints contains the text or phrase that you have added to the User Defined Dictionary, the [Data-At-Rest Scan](#) or [Data Loss Prevention](#) feature displays the path or location of these documents.

In this section, User Defined Dictionaries can be created or managed which will be monitored through Data Loss Prevention Settings.

Adding Dictionary

To add dictionary, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > User Defined Dictionary**.
3. Click **Add Dictionary**.
4. Enter the details such as name, description and the word that you want to add.
5. Click **Add**.

You can add multiple words to the dictionary.

You can delete a word from the list by selecting a particular word and clicking **Delete**.

6. Click **OK**.

Importing Dictionary

You can also import a dictionary that you prefer to use.

To import the dictionary, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > User Defined Dictionary**.
3. Click **Import**.
4. In the Import Dictionary dialog, click **Browse**.

The File Upload dialog appears.

5. Select the valid exported dictionary database file (Example: `expdict.db`).
6. Click **Open**.

The database file is imported.

Exporting Dictionary

You can export a dictionary that you have created.

To export the dictionary, follow these steps,

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > User Defined Dictionary**.
3. On the User Defined Dictionary page, select the dictionary that you want to export.
4. From the Actions column, click **Export** icon.

The database file is downloaded. The default name of the database file is `expdict.db`.
If required, you can change the filename.

Actions on Dictionary

You can edit, delete or export the added dictionary by selecting the dictionary from the provided list and performing the required action from the Actions column.

Domain Exceptions

In this section, you can add the domain names that you want to exclude from Data Loss Prevention.



- Domain Exceptions support the Windows platform only.
- Domain Exceptions support Microsoft Outlook and Thunderbird email clients only.
- If sender and receiver are from different domains, add both domain names in Domain Exception.

Adding domain name

To add a domain name to exclude from Data Loss Prevention, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. Enter the domain name in the text box.
4. Click **Add**.

Deleting domain name

- To delete an individual domain name, click the **Delete** icon available next to the domain name.
- To delete multiple domain names, select the check boxes of the domain names that you want to delete, and then click **Delete**.

Importing domain name

You can import a domain name that you prefer to use.

To import the domain name, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. On the Domain Exceptions page, Click **Import**.

The File Upload dialog appears.

4. Select the valid exported domain database file (Example: `exdomain.db`).
5. Click **Open**.

The database file is imported.

Exporting domain name

You can export a domain name that you created.

To export the domain name, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. On the Domain Exceptions page, select the domain name that you want to export.
4. Click **Export**.

The database file is downloaded. The default name of the database file is `exdomain.db`. If required, you can change the filename.

Actions on domain name

You can also edit or delete the added domain name by selecting the domain name from the provided list and performing the required action from the Actions column.

Custom Extensions

In addition to the default extensions of the files, you can monitor other extensions as per your requirement. These additional extensions are called Custom Extensions.

In this section, you can add the Custom Extensions to monitor from Data Loss Prevention.



Custom Extensions support the Windows platform only.

Adding Custom Extensions

To add Custom Extensions, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.

3. Enter Custom Extensions.
4. Click **Add**.

Deleting Custom Extensions

- To delete an individual Custom Extensions, click the **Delete** icon available next to the Custom Extensions.
- To delete multiple Custom Extensions, select the check boxes of the Custom Extensions that you want to delete, and then click **Delete**.

Importing Custom Extensions

You can import a Custom Extension file that you prefer to use.

To import a Custom Extension file, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.
3. On the Custom Extensions page, Click Import.

The File Upload dialog appears.

4. Select a valid Custom Extension database file (Example: `expfiles.db`).
5. Click **Open**.

The database file is imported.

Exporting Custom Extensions

You can export a Custom Extensions that you have created.

To export a Custom Extension file, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.
3. On the Custom Extensions page, select the Custom Extension that you want to export.
4. Click **Export**.

The database file is downloaded. The default name of the database file is `expfiles.db`. If required, you can change the filename.

Actions on Custom Extensions

You can also edit or delete the added Custom Extensions by selecting the Custom Extension files from the provided list and performing the required action from the Actions column.

Applications

In this section, you can add custom application to monitor; also, you can add application to exclude from Data Loss Prevention.



Applications supports the Windows platform only.

Adding Applications

To add an Application, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Applications.**
3. To add an application, click **Browse** and provide complete path to the exe file of the application.

If the application contains multiple exe files, add all exe files.

If the application exe file is being used for multiple applications, and you add here to monitor/exclude, all the applications will be affected.

If there is a DLP occurrence in the monitored/excluded application, the application behaviour may change. Depending upon the application behaviour, DLP may or may not be able to monitor.

4. Enter the application name.
5. Click **Add**.

Applications added from the standard category will appear as per category in the list and custom application will appear in the **Custom** list on the DLP policy page.



If you are adding an application from **system32** folder on X64 bit OS, copy that application from **system32** folder to any other location. Then add the application from that location.

Deleting Applications

- To delete an individual Application, click the **Delete** icon available next to the Application.
- To delete multiple Applications, select the check boxes of the Applications that you want to delete, and then click **Delete**.
- If you delete any application, make sure you save respective policy on the Policy page.

Importing Applications

You can import an Application that you prefer to use.

To import the Application, follow these steps,

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Applications.**
3. On the Applications page, Click **Import**.

The File Upload dialog appears.

4. Select a valid exported application database file (Example: `expapps.db`).
5. Click **Open**.

The database file is imported.

Exporting Applications

You can export an Application that you created.

To export the Application, follow these steps:

1. On the Application page, select the application that you want to export.
2. Click **Export**.

The database file is downloaded. The default name of the database file is `expapps.db`. If required, you can change the filename.

Actions on Applications

You can also edit or delete the added Applications by selecting the Applications from the provided list and performing the required action from the Actions column.

Network share Exception

In this section, you can add a network share path in UNC format to exclude from Data Loss Prevention.

Adding Network share Exception

To add Network share Exception, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to Admin Settings > Server > Data Loss Prevention > **Network share Exception**.
3. Enter the Network share Exception.
4. Click **Add**.

Deleting Network share Exception

- To delete an individual Network share Exception, click the **Delete** icon available next to the Network share Exception.
- To delete multiple Network share Exception, select the check boxes of the Network share Exception that you want to delete, and then click **Delete**.

Importing Network share Exception

You can import a Network share Exception that you prefer to use.

To import the Network share Exception, follow these steps,

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Network share Exception**.

3. On the Network share Exception page, Click **Import**.

The File Upload dialog appears.

4. Select a valid exported network share database file (Example: `expnetsh.db`).
5. Click **Open**.

The database file is imported.

Exporting Network share Exception

You can export a Network share Exception that you created.

To export the Network share Exception, follow these steps:

1. On the Network share Exception page, select the application that you want to export.
2. Click **Export**.

The database file is downloaded. The default name of the database file is `expnetsh.db`. If required, you can change the filename.

Actions on Network share Exception

You can also edit or delete the added Network share Exception by selecting the Network share Exception from the provided list and performing the required action from the Actions column.



Network share Exception supports the Windows platform only.

Redirection

This feature helps you change the EPS Server for upgrading your EPS to new version. This helps in redirecting the existing clients to new EPS Server and thereby using the new EPS Server for communication. You can select the clients or configure all the clients to be redirected to the new server. This feature is particularly useful in cases of large networks where the clients are connected through low bandwidth lines. You can use this feature to move the clients in groups selectively to the new server so that redirection is gradual and at your convenience.

In case of software version upgrade, the previous version EPS Client will get uninstalled and new version of EPS Client will get installed.

Redirection is applicable from Master to Master server or from Secondary to Secondary Server with same or higher EPS Version.

If EPS version earlier than 7.6 is installed on the Mac client with OS earlier than 10.9, redirection is not applicable. To redirect, upgrade the Mac OS. The redirection feature is applicable only for the clients with Mac OS X 10.9 and above.

The following table explains the supported redirection cases,

EPS Server of earlier version	EPS Server of higher version
Installed on local/private IP	Installed on local/private IP
Installed on local/private IP	Installed on local/private Domain

Installed on local IP (natted with public)	Installed on local IP (natted with public)
Installed on public IP	Installed on public IP
Installed on public IP	Installed on FQDN (Fully qualified Domain Name)



- When the redirection process is in progress, the previously installed EPS should not be uninstalled. If you uninstall the previous EPS before the redirection process command is delivered to all the clients, then the clients who fail to receive the command will neither communicate with previous EPS nor with the new EPS.
- Redirection is not applicable for the clients installed on Linux operating system.
- Group Revival: To maintain the earlier client group-policy structure after client redirection, administrator can export the older client group-policy structure from Manage Groups and import it in new EPS server. After redirection old client will be placed in the same group as earlier on new EPS server.
If group with same name is present on redirected server then newly imported group is renamed with suffix “_1”.
- Group revival is applicable for MAC and Windows clients only.

To configure Redirection, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Redirection**.
3. In the Server Name/IP text box, type the sever name or IP address of new EPS server.
4. In the Port text box, type the Port number.
5. Do the following:
 - i. Select the **Select this check box to add a public IP address/Hostname** check box.
 - ii. Only In case of remote clients, in the **Server Name/IP** text box, type the sever name or public/natted IP address of new EPS server.
If EPS is installed through public mode, then the above two fields do not appear.
6. Select one option from **Redirection Type** list:
 - Redirect all clients: To select all the clients which are to be redirected.
 - Redirect and Auto-Reboot all clients: To redirect all the clients and auto-reboot them during upgrade process. Enabling this option would prompt user with 15 minutes countdown reboot prompt, and a forceful reboot will occur after 15 minutes. After the client reboot, the new version of Client will be installed (silently) and complete the redirection process.
 - Redirect selected clients: If you select this option, you can select specific clients for redirection process. On selecting this option, the Select Clients link is displayed. Click

Select clients. In the Select Clients dialog box, select the clients that you want to redirect and click **OK**. Use the Endpoint name\IP search box on the upper-right corner to search for endpoints by name or IP address.

7. To apply your settings, click **Apply**.



Client system will not reboot automatically if the redirection process is carried out for same EPS version even if the Redirect and Auto-Reboot all clients option has been configured.

Manage Users

This feature helps you create, edit, disable, and delete a list of users of Administrator level, Report Viewer level and Group Administrator level. The following are different types of users:

Super Administrator

A Super Administrator user has access to all the features of Seqrite Endpoint Security. A Super Administrator can create and modify Administrator users. Only Super Administrator has the privilege to uninstall Seqrite Endpoint Security.

There can be only one user with Super Administrator privilege. The default user name for Super Administrator is 'administrator'.

Administrator

User with Administrator privileges has all the privileges of a Super Administrator, with two exceptions:

1. Such a user cannot create another user with Administrator privileges.
2. Such a user cannot uninstall Seqrite Endpoint Security.

Report Viewer

A user with the Report Viewer privileges can only view reports and status of features. This user has no other privileges. However, this type of users can change their own password.

Group Administrator

The Group Administrator has given access to specific policy settings as per requirement. When Group Administrator logs on, only selected settings will be enabled in the policies assigned to the groups and subgroups of the Group Administrator.

The Group Administrator can view the group hierarchy of its own group only.

The Group Administrator can view and export reports of clients of its own group and its subgroups. On the Reports page, only Client tab is visible for the Group Administrator.

Only Super Administrator user can create/edit/delete the Group Administrator user and assign/unassign the Group Administrator to any group.

Creating New Users

To create a new user, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Users**.
3. On the Manage Users page, click **Add User**.
An Add/Edit User dialog appears.
4. In the **User Name** text box, type the user name.
5. In the **New Password** text box, type the new password.
6. In the **Confirm New Password** text box, retype the new password.
7. In the **Email ID** text box, type the email Id of the user.
8. From the Type list, select the user type.

The user type includes: Administrator, Report Viewer and Group Administrator.

When you select Group Administrator option, the configure link is enabled.

- i. Click the **configure** link.
 - ii. Configure access rights by selecting the settings.
 - iii. Click **Apply**.
9. Select to enable or disable the user from the User Status list.
 10. To save your settings, click **Save**.

Modifying Existing Users

To modify the settings of an existing user, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Users**.
A list of all users appears.
3. Click the **Edit** button next to the user that you want to edit.
4. You can modify the setting according to the right privileges assigned to you.
The Add/Edit User dialog appears.
5. In the New Password text box, type the new password.
6. In the Confirm New Password text box, retype the new password.
7. From the Type list, select the new type if you want.
8. Select to enable or disable the user from the User Status dropdown.
9. To save you settings, click **Save**.

Deleting Users

To delete an existing user, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Manage Users**.

A list of all users appears.

3. Click **Delete** next to the user that you want to delete.

You can delete a user if you have the right privileges to do so.

A confirmation message appears.

4. To delete the users, click **Yes**.

Internet Settings

This feature gives the administrators to use proxy settings for server modules that need an Internet connection to work. You can configure the Internet settings for server modules like Cloud connectivity, License Synchronization, View License History, Sending Email & SMS notifications and Messenger. This is very helpful in allowing the server modules to function in a secure work environment where default Internet connection is not allowed.

To provide Internet Settings, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Internet Settings**.
3. To set the proxy setting for Internet, select **Enable Proxy Setting**.

The proxy settings details are activated.

4. In Proxy Server, type the server name.
5. In Port, type the port number.

You can also set authentication rule if you use Firewall or proxy server. For this, type the User name and Password under Authentication.

6. To apply your settings, click **Apply**.



The Internet Settings provided in Admin Settings will reflect in Update Manager Connection Settings.

Patch Management

Patch Management enables the centralized management for checking and installing the missing patches for the applications installed in your network. With this too, you can also automate checking and installation of the missing patches.



The Patch Management feature is applicable only for the clients with Microsoft Windows OS; does not support Mac, and Linux operating systems.

Installing Patch Server

To install the patch server, follow these steps:

1. For 32-bit Windows OS, download the setup from one of the following links:
<http://dlupdate.quickheal.com/builds/seqrite/760/en/pmsetup32.msi>
<http://download.quickheal.com/builds/seqrite/760/en/pmsetup32.msi>
For 64-Bit Windows OS, download the setup from one of the following links:
<http://dlupdate.quickheal.com/builds/seqrite/760/en/pmsetup64.msi>
<http://download.quickheal.com/builds/seqrite/760/en/pmsetup64.msi>
2. Launch the setup on the system in the network where you want to install the Seqrite patch server.
3. After the installation is complete, add Seqrite patch server through EPS console and then it becomes available to use.

Adding New Patch Server

To add new patch server, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Add New Patch Server** tab.
4. In the Add New Patch Server section, enter Server Name.
5. If the Patch server is deployed in the network of local client, follow these steps:
 - i. In the **Server IP/Hostname** text box, type private IP address or host name of the Patch Server.
 - ii. In **Port**, type the port number. Default Port HTTP is 3698 SSL:6201.
 - iii. Ensure that the **Use SSL (Ensure Patch server supports SSL, if SSL is checked)** check box is selected. This check box is selected by default.
 - iv. In the EPS Details section, in the **EPS IP/Hostname** text box, provide private or public IP/Hostname of the EPS server. Seqrite recommends provide the Private IP/Hostname.

If the Patch server is deployed in the network of remote client, follow these steps:

- i. In the **Server IP/Hostname** text box, type public IP address or host name of the Patch Server.
- ii. In **Port**, type the port number. Default Port HTTP is 3698 SSL:6201.
- iii. Ensure that the **Use SSL (Ensure Patch server supports SSL, if SSL is checked)** check box is selected. This check box is selected by default.

- iv. In the EPS Details section, in the **EPS IP/Hostname** text box, provide public IP/Hostname of the EPS server.

6. Click **Add**.



Windows XP 64 and Windows Server 2003 does not support SSL communication of client with the Patch Server.

Removing Patch Server

To remove the patch server, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Add New Patch Server** tab.

Existing Patch Server Status appears. The status options are as follows:

Status	Description
Online	The patch server is online.
Offline	The patch server is offline.
Uninstalled	The patch server is being uninstalled.
Invalid	The patch server is added on EPS console. Then the same patch server is added on another EPS console. In this case, the status of the patch server in the first EPS will be shown as invalid.

4. You cannot remove a patch server, if it is applied to a policy. Select the Patch server that you want to remove and click the link **Remove** next to it.

A confirmation message appears.

5. Click **Yes** to remove the patch server.

Configuring Patch Server

Configure the port for Seqrite patch server to which EPS server and endpoints will communicate.

To configure the patch server, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Configure Patch Server** tab.
4. Select the patch server from the list. Configuration section appears.
5. Select the **Configuration** tab and do the following:
 - i. The port number of the patch server appears. You can edit the port number.

- ii. Select the check box **Use SSL (Select the check box if the patch server is configured with SSL).**
- iii. In the Automatic Download section, select the **Automatic download the detected missing patches if severity equal to or greater than:** check box.
- iv. Select the severity level from the list. The severity options are:

Severity	Description
Critical	Vulnerability may allow code execution without user interaction.
Important	Vulnerability may result in compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	Vulnerability may result in random malfunctions.

6. Select the **Internet Settings** tab and do the following:

The details of the proxy server appears. By default, the **Enable Proxy Settings** check box is selected. You can clear the check box to disable the proxy settings.

- i. In the **Proxy Server** text box, the IP address of the proxy server appears. Edit the IP address if required.
- ii. In **Port** text box, the port number of the proxy server appears. Edit Port number if required.
- iii. Select the check box **Enable Authentication (if any)** to enable authentication.
- iv. In the **User name** and **Password** fields, type in your server credentials.

7. Select the **Patch Synchronization** tab and do the following:

- i. Previous patch synchronization status and last successful patch synchronization dates appear.
- ii. In the Configure Upstream Patch Server section, select the upstream patch server from the following options:

Upstream Patch Server	Description
Microsoft Patch server	The upstream patch server used is Microsoft patch server. This option is selected by default.

Organization Patch server (WSUS)	The upstream patch server used is Organization Patch server (WSUS - Windows Server Update Service). If you select this option, type in WSUS server URL.
Seqrite Patch server	The upstream patch server used is configured Seqrite Patch server. If you select this option, select the patch server from the list.

- iii. In the Configure Patch Synchronization section, select the **Enable Schedule Patch Synchronization** check box.
 - iv. Select **Frequency** of patch synchronization, either Weekly or Monthly.
 - v. Select **Weekday** from the list to run patch synchronization.
 - vi. Select time to run patch synchronization by selecting hours and minutes in the **Start At** list.
 - vii. Click **Filters..** to specify filters for patch synchronization. Windows Patch Synchronization Settings dialog appears.
 - a. In the **Products** tab, select the products for which you want to receive the patches. Select the folder to expand and then select.
 - b. Select the **Categories** tab. Select the type of patches to be synchronized.
 - c. Select the **Languages** tab. Select the languages for the patches by selection one of the following options:
 - Download patches in all languages
 - Download patches in below selected languages
 - d. Click **Apply** to apply the filters for patch synchronization. To restore the default settings, click the **Default**.
 - viii. Click **Start** to run patch synchronization instantly.
 - ix. Click **Stop** to stop patch synchronization if it is running. A notification is sent to the patch management server.
8. Click **Apply** to apply the configuration settings.



Patch Management supports the following applications along with Microsoft applications,

- VideoLAN Player
- Adobe Acrobat
- Adobe Flash Player
- Adobe Reader
- puTTY
- puTTY with MSI installer
- Notepad++

- Oracle Corp.
- Java
- 7-zip compression Tool
- Mozilla Thunderbird
- Firefox

Upgrading Windows 10 to latest version through Seqrite Patch Management

You can configure Seqrite Patch Server to get upgrade patches for Windows 10 operating system using newly added 'Upgrades' category through Seqrite Endpoint Security 7.6 Service Pack 5.

This will help the Administrator to upgrade Windows 10 Operating System to the latest released version.

Applicable OS: Windows 10 RS1 (1607) and above

With Seqrite EPS 7.6 Service Pack 5, Upgrade support is added for Windows 10 Operating system through Seqrite Patch management. Administrator can configure Seqrite Patch Management to synchronize Upgrade patches for Windows 10 operating system.

Prerequisites:

1. Seqrite Endpoint Security (EPS) must be installed and activated.
2. Seqrite Patch Management must be installed and configured with Seqrite EPS server.
3. Service Pack 5 must be applied on Seqrite EPS 7.6 server.
4. Perform patch synchronization to get the newly added 'Upgrades' category.

To configure Seqrite Patch Server, follow these steps.

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Configure Patch Server** tab.
4. Select the patch server from the list. Configuration section appears.
5. Click **Filters** to specify filters for patch synchronization. Windows Patch Synchronization Settings dialog appears.
6. In the **Products** tab, under Microsoft > Windows, select "**Windows 10**" and "**Windows 10, version 1903 and later**" check boxes.
7. In the Categories tab, select the **Upgrades** check box.
8. Click **Apply** to apply the configuration settings.
9. Click **Start** to run Patch Synchronization

After successful Patch Synchronization, perform Patch Scan for Endpoints with Windows 10 OS.

10. Go to **Clients > Client Action > Patch Install**. Patch Install page appears.

The list of upgrades available for existing version of Windows 10 OS appears.

11. Select the upgrade patches and Click **Start Install**.

Note: Seqrite recommends upgrading to the latest version of Windows 10.

For more information, refer to the KB article, [Upgrading Windows 10 to latest version through Seqrite Patch Management](#).

General

This feature helps you configure the settings about when the running session should time out. The session is timed out if the current session is inactive for the specific time. You can also configure TLS version.

To configure General, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > General**.
3. Select the **Automatic installation of the Service Pack** check box to install the Seqrite Endpoint Security Service Pack automatically on the EPS Server. If you do not enable, you will have to install the Service Pack manually.
4. From the **Session time out period** list, select the time period.
You can select either 20 minutes, 30 minutes, or 60 minutes.
5. In the **Configure TLS Version for Server Client Communication** section, select **TLS Version**.

Note

If you select TLS 1.3, endpoints that are not updated to SP5 may stop communicating with EPS server.

6. Click **Apply**.

Multiserver Migration Period

Multiserver Migration Period feature allows you to install a higher version of EPS without uninstalling the previous one for a certain time, with this you can easily migrate the existing clients to a higher version. You can select the time period according to your schedule ranging from 30 to 90 days. Follow the given steps to use the feature:

1. Log on to Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Server > General**.
3. In the Multiserver Duration list, select the number of days.
4. Click **Apply**.



- This option will only be available on the higher version installed in case of Multi-server installation.
- By default, 60 days option is selected.

Clients

This section includes the following.

Client Installation

This feature helps you specify the path to the location where you want to get the client installed. By default, a path is configured that you can change if required.

To change Seqrite client installation path, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients > Client Installation**.

The Client Installation page appears.

3. To configure the client installation path, type the installation path in the **Please specify client installation path** text box.
4. To limit the download bandwidth, select the **Specify maximum speed for downloading Antivirus build and Service Packs on the endpoints** check box.
5. Enter the speed in the **Download Speed** text box. Enter the speed value between 64 to 10,000 kbps. By default, the speed value is 1024 kbps.
6. From the Scan and Report section you can select following options to start the scan when SEPS gets installed:
 - **Vulnerabilities:** To configure the vulnerability scan of the client endpoint and send the report to SEPS server after successful installation of SEPS, you can select this check box.
 - **All installed applications:** To configure the scan of all the installed applications on a client endpoint after successful installation of SEPS, you can select this check box. The scan report is sent to the SEPS server. This option is selected by default.
7. To apply the setting, click **Apply**.



- These features are not available in the clients with Mac and Linux operating systems.

Inactive Client Settings

When you uninstall the Seqrite client from an endpoint, the program automatically notifies the server. When the server receives this information, it removes the client icon in the computer tree subsequently.

However, if the client is removed using other methods, such as you reformat the computer hard drive or delete the client files manually, Seqrite Endpoint Security will display the client as inactive. If a user unloads or disables the client for an extended period, the server also displays the client as inactive.

To protect the display of active clients, you can configure Seqrite Endpoint Security to remove inactive clients from the computer protection list.



The Inactive Client Settings feature is available in the clients with Microsoft Windows, Mac, and Linux operating systems.

To remove inactive clients, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients**.
The Client Installation page appears.
3. Under Inactive Client Settings, select the **Enable automatic removal of inactive clients** check box.
4. In the Remove a client if inactive for list, select number of days after which Seqrite Endpoint Security considers a Client is inactive.
5. To apply the setting, click **Apply**.

Asset Management

This feature helps in enabling collection of various information about endpoints such as, system information, hardware information, software installed, and updates installed.

You can enable the Asset Management reporting by the following procedure.

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients**.
3. Select the **Enable Asset Management** check box.
4. Select the **Display Windows Product key** check box to view the complete product key at [Clients > Assets > View Details](#). If you don't select this check box, only partial product key will be displayed.
5. Click **Apply**.

Roaming Clients

Roaming service allows interacting with the EPS Server via Seqrite Cloud when the clients are outside the organizational network (mobile endpoints).

Roaming service allows the administrator to apply policies, initialize Tune-up, and scans like application control scan, vulnerability scan, and virus scan remotely from the EPS Server.

The clients can update their status (This will be displayed as Roaming on the Client status tab and Dashboard by default as the client goes roaming), download the latest configuration, and send client reports.

EPS will communicate with the Cloud-based roaming service using the Proxy settings configured using the Internet Settings tab. In case these settings are not available, EPS will use a direct connection.

You can enable the roaming service by the following procedure:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients > Roaming Clients**.
3. Click **Connect to cloud platform**.

The Connection Process Complete page is displayed.

4. Click **OK**.
5. Select the **Enable Roaming Service** check box.
6. Select the Roaming mode for the clients:
 - Automatic
In this mode, every EPS client can connect to Roaming Service automatically as it is out of the organizational network.
 - Manual
In this mode, only selected clients can connect to Roaming Service. Selecting this mode enables you to select the specific clients, as follows:
 - a. Click the **Select clients**.
 - b. To use this service, select the clients in your network and enable them.
 - c. Click **OK**
7. Click **Apply**.

Reinstallation

In case of Reinstallation with the same product key, you need to activate the Roaming Clients as mentioned below:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients > Roaming Clients**.
3. Click **Connect to cloud platform**.
Connection Process Complete page is displayed.
4. Click **OK**.
5. Select the email address where you want to receive the OTP.

6. Click **Next**.
7. Check the given email address and click **Confirm** to receive the OTP.
8. Enter the OTP as received in the email.
9. If you have not received any email, click **Regenerate OTP** to generate it again.

The connection process is complete.

10. Click **OK** to proceed.
11. Select **Enable Roaming Service** and **Roaming mode**.



- Roaming Clients feature is only supported for Windows and Mac operating systems.
- An Internet connection is required for using this service.

Data Loss Prevention (DLP)

In this section, you can see the count of DLP licenses purchased and DLP licenses utilized. You can enable or disable the DLP Pack for any endpoints.

The page displays the following information,

- Total number of DLP licenses entitled (purchased)
- Number of DLP licenses utilized

Enabling DLP feature

To enable the DLP feature, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. Go to **Admin Settings > Clients > Data Loss Prevention**.

A list is displayed with all the endpoints for which the DLP feature is enabled.

3. Click **Add**.

A window displaying all the groups appears. Each group includes the names of the endpoints belonging to that group.

4. Under EPS Console, select a group.

In the right pane, all the endpoints of a relevant group are displayed.

5. Select an endpoint and then click **OK**.

The DLP feature is enabled for the selected endpoints.

You can also remove the endpoint, if you prefer.

Fields	Description
Search	Helps you search the endpoint by name.
CSV	Helps you save the list in csv format.

Add	Helps you add the endpoint to enable DLP for that endpoint.
Remove	Helps you remove the endpoint.



If the EPS client is removed from the client list, it will be removed from the DLP availed list also.

Update Manager

Update Manager is a tool integrated with Seqrite Endpoint Security. It is used to download and manage the updates for Seqrite Endpoint Security. It provides you the flexibility to download the updates on a single machine. All the Seqrite Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Seqrite Endpoint Security for enhancements or bug fixes. Update Manager integrated with Seqrite Endpoint Security includes all the features that are available in the Update Manager application. Any change in settings made here will reflect in the Update Manager application.

Viewing Update Manager Status

Use this feature to view information of all types of updates downloaded by Update Manager. The console displays the Version, Service Pack, and the date of the associated Virus Database.

Additionally, the console also provides the following details:

Fields	Description
Endpoint Name	Displays the name of the endpoint where Update Manager is installed.
IP Address	Displays the IP address of the endpoint where Update Manager is installed.
Status	Provides the information about Update Manager, whether it is online or offline.
Update Manager URL	Provides the Update Manager URL to download the updates. This URL can be used by the alternate Update Manager, client, and other EPS Update Manager.

The two buttons available under Update Manager Status are:

Buttons	Description
Update Now	Click this button to send a Notification from Seqrite Endpoint Security to the Update Manager to start downloading the updates. This process is in the background and will not be visible to the user. Click Back to go to the Status page.
Rollback	Click this button to take the Update Manager back to the previous update state.

	<p>Note: This feature will work only if Always take backup before downloading new update option is selected in the settings of the Update Manager. The steps for performing Rollback are as follows:</p> <ul style="list-style-type: none"> • Click the Rollback button. A pop-up window opens. The Seqrite product updates that will be affected by the rollback are displayed. • To begin the Rollback process, click Rollback.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Update Manager Settings

The following are the features available under Update Manager Settings:

Features	Description
Enable Automatic Updates	Select this box to enable automatic update of Seqrite Endpoint Security. However, this feature is enabled by default. It is recommended that you do not disable this feature.
Always take backup before downloading new update	Select this box to enable and take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. However, this feature is enabled by default.
Delete report after	Select this box to enable deletion of reports automatically after the time you specify. This feature is enabled by default and the default time is 10 days.
Download the Seqrite Endpoint Security Service Pack	To take the updates for Seqrite Endpoint Security service pack, select Download Endpoint Security Service Pack check box. This feature is enabled by default.
Select the updates you want to download.	A list of SEPS products appear. By default, all the products are selected. Verify which updates should be downloaded for your Endpoint security.
Restrict download speed (kbps)	<p>Select the Restrict download speed (kbps) check box if you want to restrict the update download speed. Enter the speed in the text box.</p> <p>You can enter speed limit in the range of 64 kbps to 8192 kbps.</p>

To save you settings, click the **Apply** button.

Update Manager Schedule

This feature helps you define the update schedules for the Update Manager at a certain frequency.

To configure Update Manager Schedule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.

2. On the Home page, click the **Update Manager** link available along with the product name and details.
3. On the Update Manager page, click the **Update Manager Settings** tab.
4. Click the **Settings** button available next to Enable automatic updates.

The Update Manager Scheduler dialog appears.

5. Select the **Custom** option and configure the following options:
 - i. In **Frequency**, select either the Daily or Weekly option.
If you select the **Weekly** option, select the weekday from the list.
 - ii. In **Start At**, set time in hours and minutes.
 - iii. If you want to repeat the update of the Update Manager, select the **Repeat Update** check box and set the frequency in days to repeat the update.
6. Click **Apply**.

Alternate Update Managers

In case of large network, you can deploy multiple Update Managers on different servers. This helps in load balancing and you can configure clients in Client Settings to take the updates from these locations. You can view the details, add, edit or delete the Alternate Update Managers.

Recommendation

- Seqrite recommends deploying a separate/dedicated Alternate Update manager for a group of up to 200 clients for proper load balancing.
- For remote clients, install the Alternate Update Manager in the network where the remote clients are deployed.

Adding New Alternate Update Manager

To add a new Alternate Update Manager in the EPS server, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. On the Home page, click the **Update Manager** link available along with the product name and details.
3. On the Update Manager page, click the **Alternate Update Managers** tab.
A list of all Update Managers appears.
4. Click **Add** to create new Alternate Update Manager.
5. A list of endpoints where the Alternate Update Manager is installed on EPS clients appears.
Select the endpoint from the list to create Alternate Update Manager on that endpoint.
6. In the **Update Manager Name** text box, type the name.

7. In the **Update Manager Site** text box, type the URL of the Alternate Update Manager.
8. To save your settings, click **Add**.

Viewing details of Alternate Update Mangers

To view details of Alternate Update Mangers installed on EPS clients, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. On the Home page, click the **Update Manager** link available along with the product name and details.
3. On the Update Manager page, click the **Alternate Update Manager** tab.
A list of all Update Managers appears.
4. Click the **Settings** link next to the Alternate Update Manager to view the status and settings of the Alternate Update Manager.
5. The Alternate Update Mangers Details screen appears. Click the **Status** tab to view the status with the following details:

Fields	Description
Update Manager Name	Displays the name of the Alternate Update Manager.
Endpoint Name	Displays the name of the endpoint where Alternate Update Manager is installed.
IP Address	Displays the IP address of the endpoint where Alternate Update Manager is installed.
Status	Provides the information about Alternate Update Manager, whether it is online or offline.
Update Manager URL	Provides the Update Manager URL to download the updates. This URL can be used by the EPS Update Manager, client, and other Alternate Update Manager.

Also, the list of the products installed with the details (Product Name, Version, Service pack and Virus Database Date) appears. The two buttons available under Update Manager Status are:

Buttons	Description
Update Now	Click this button to send a Notification from Seqrite Endpoint Security to the Alternate Update Manager to start downloading the updates. This process is in the background and will not be visible to the user. Click Back to go to the Status page.
Rollback	Click this button to take the Alternate Update Manager back to the previous update state.

	<p>Note: This feature will work only if Always take backup before downloading new update option is selected in the settings of the Alternate Update Manager. The steps for performing Rollback are as follows:</p> <ul style="list-style-type: none"> Click the Rollback button. A pop-up window opens. The Seqrite product updates that will be affected by the rollback are displayed. To begin the Rollback process, click Rollback.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6. Click the **Settings** tab to view the status with the following details:

The following are the features available under Alternate Update Manager Settings:

Features	Description
Enable Automatic Updates	Select this box to enable automatic update of Seqrite Endpoint Security. However, this feature is enabled by default. It is recommended that you do not disable this feature.
Always take backup before downloading new update	Select this check box to enable and take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. This feature is enabled by default.
Delete report after	Select this check box to enable deletion of reports automatically after the time you specify. This feature is enabled by default and the default time is 10 days.
Download Seqrite Endpoint Security Service Pack	To take the updates for Seqrite Endpoint Security service pack, select Download Endpoint Security Service Pack check box. This feature is enabled by default.
Select the updates you want to download	A list of SEPS products appear. By default, all the products are selected. Verify which updates should be downloaded for your Endpoint security.
Restrict download speed (kbps)	<p>Select the Restrict download speed (kbps) check box if you want to restrict the update download speed. Enter the speed in the text box.</p> <p>You can enter speed limit in the range of 64 kbps to 8192 kbps.</p>

7. To save your settings, click the **Apply** button.

Modifying Existing Alternate Update Manager details

To modify the details of an existing Alternate Update Manager, follow these steps:

- Log on to the Seqrite Endpoint Security Web console.
- On the Home page, click the **Update Manager** link available along with the product name and details.

3. On the Update Manager page, click the **Alternate Update Manager** tab.

A list of all Update Managers appears.

4. Click the **Edit** link next to the Alternate Update Manager that you want to edit.

The Edit Alternate Update Manager dialog appears.

5. Modify the **Update Manager Name** and/or **Update Manager Site**.

Update Manager site is not editable if Alternate Update Manager is installed on EPS clients.

6. To save your settings, click **Update**.

Alternate Update Manager Schedule

This feature helps you define the update schedules for the Alternate Update Manager at a certain frequency.

To configure Alternate Update Manager Schedule, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. On the Home page, click the **Update Manager** link available along with the product name and details.

3. On the Update Manager page, click the **Alternate Update Manager** tab.

A list of all the Update Managers appears.

4. Click the **Settings** link available next to the Alternate Update Manager to view the status and settings of the Alternate Update Manager.

The Alternate Update Managers Details screen appears.

5. Click the **Settings** tab.

6. Click the Settings button available next to Enable automatic updates.

The Update Manager Scheduler dialog appears.

7. Select the **Custom** option and configure the following options:

- i. In **Frequency**, select either the Daily or Weekly option.
If you select **Weekly** option, select the weekday from the list.
- ii. In **Start At**, set time in hours and minutes.
- iii. If you want to repeat update of the Update Manager, select the **Repeat Update** check box and set the frequency in days to repeat the scan.

8. Click **Apply**.

Deleting Alternate Update Manager

To delete an existing Alternate Update Manager, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.

2. On the Home page, click the **Update Manager** link available along with the product name and details.
3. On the Update Manager page, click the **Alternate Update Manager** tab.
A list of all Update Managers appears.
4. Select and then click **Delete** to delete the Alternate Update Manager.
A confirmation message appears. If you delete the update manager
5. To delete the Alternate Update Manager, click **Yes**.

License Manager

This feature allows you to manage Seqrite Endpoint Security licenses. You can check the status of your Seqrite Endpoint Security license and update license information. You can place an order to renew your license, add new licenses to your existing setup, or buy additional features packs.

Status

This feature helps you check the current status of your license information. To check the status of your license, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. On the Home page, click the **View License** link available along with the product name and details.
3. On the License Manager page, click the **Status** tab.

The license information includes the following details:

Title	Description
Company Name	Displays the name of the company to which Seqrite Endpoint Security is registered.
Product Name	Displays the product name. Example: Endpoint Security – Total.
Product Key	Displays the Product Key of Seqrite Endpoint Security.
Product Type	Displays the product type. Example: Regular.
Installation Number	Displays the installation number.
License valid till	Displays expiry date of the Seqrite Endpoint Security license.
Entitled	Displays total number of EPS and DLP licenses purchased.
Assigned to Secondary servers	Displays number of EPS and DLP licenses assigned to Secondary servers.
Unutilized by Secondary servers	Displays number of EPS and DLP licenses of unutilized by Secondary servers
Utilized by this server	Displays number of EPS and DLP licenses utilized by this server.

Remaining for this server	Displays number of EPS and DLP licenses remaining for this server.
---------------------------	--------------------------------------------------------------------

Update License Information

This feature is useful to synchronize your existing license information with Seqrite Activation Server. You can update your license information whenever required.

This is helpful in updating the following license information:

- License expiry date: If you have renewed the license, but the expiry date is not updated or displays the old expiry date.
- Number of SMS left: If you have purchased SMS bundle for notification, but the limit has not been refreshed.
- Email ID: If there is any change in email IDs provided at the time of activation but has not reflected in the account.
- Feature changes or edition changes are synchronized with activation server.



If you want to renew your existing license and you do not know how to renew it or are facing any problem during renewal, you can call the Seqrite Support team and provide your Product Key.

View license history

You can view the details of your license purchase history if you click the License History button. On the License History page, the product details are displayed. Also, the following information is displayed:

- Date & Time: The time and date when the transaction was carried out.
- Activity: The type of purchase, such as license activation, pack addition, license renewal, license addition, and reactivation of license.
- Details: Relevant details of the transaction, such as type, number of licenses added, type of feature pack added or removed, and validity of the license purchased.

License Order Form

This feature helps you create a license order form for an additional license, renewal of your existing license, or edition upgrade. This is an offline activity and helps to create the license order.

After generating an order form, take out its print, contact a vendor or dealer, and submit it. You can also send an email with the license order form to the Seqrite sales team. We will contact you for further process.

To create a license order form, follow these steps:

1. Log on to the Seqrite Endpoint Security Web console.
2. On the Home page, click the **View License** tab.

3. On the License Manager page, click the **License Order Form** tab.
4. To create a License Order form, select one of the following:
 - Renew my license: Helps you renew your current license.
 - Add license for new endpoints: Helps you buy additional licenses.
 - Edition Upgrade/Buy additional feature: Helps you upgrade the edition or buy additional features packs as per the following table:

EPS Edition	Upgrade Pack
SME	Business/Total
Business	Total

5. Click **Place an Order**.

An order is created, and an automated Email is sent to the Seqrite branch sales representative to process your order.

Renew my license

If you select the Renew My License option, you are redirected to the online portal of Seqrite where you can place an order for your license renewal. As you visit the portal, your license details are displayed.

On the Seqrite online portal, do the following:

1. In the **Product Details** section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the renewal order section, select **Duration** for renewal.
3. Select **Number of the endpoints** (licenses) to renew for the systems.
4. To add the DLP Pack, select the DLP Pack check box. If you have the DLP pack subscription, you can assign the number of the endpoints to the DLP pack.
5. Select the number of endpoints to assign the DLP pack.
6. Click **Next**.

A summary of the license renewal order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the **Back** button and make the required changes.

7. Type the email IDs to whom you want to send the order.
8. Click **Place a Request**.

Your license renewal request number is generated. Save this number as you will need to quote this number in all communications related to license renewal.

Add license for new endpoints

If you select the Add license for new endpoints option, you are redirected to the online portal of Seqrite where you can place an order for additional licenses for endpoints. As you visit the portal, your license details are displayed.

On the Seqrite online portal, do the following:

1. In the Product Details section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. Select the number of endpoints for which you want the additional licenses.
3. If you have the DLP pack subscription, you can assign the number of the endpoints to the DLP pack.
4. Click **Next**.

A summary of the additional license order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

5. Enter email IDs to whom you want to send the order.
6. Click **Place a Request**.

Your license addition request number is generated. Save this number as you will need to quote this number in all communications related to additional license order.

Buy additional feature

If you select the Buy additional feature option, you are redirected to the online portal of Seqrite where you can place an order for a license of additional features. As you visit the portal, your license details are displayed.

On the Seqrite online portal, do the following:

1. In the **Product Details** section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the **Select the upgrade pack from the following:** section, select one of the following:
 - Business
 - Total
3. Select the **DLP pack** (Includes Data Loss Prevention) check box.
4. Select the number of endpoints to assign the DLP pack.
5. Click **Next**.

A summary of the order for feature packs is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

6. Enter email IDs to whom you want to send the order.
7. Click **Place a Request**.

Your license request number for new feature packs is generated. Save this number as you will need to quote this number in all communications related to new feature packs.

Edition Upgrade

If you select the Upgrade License option, you are redirected to the online portal of Seqrite where you can place an order for edition upgrade. As you visit the portal, your license details are displayed.

On the Seqrite online portal, do the following:

1. In the Product Details section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the **Select the upgrade pack from the following:** section, select one of the following:
 - Business
 - Total
3. You can also select add-on feature pack. Select the **DLP Pack** check box.
4. Select the number of the endpoints to assign the DLP pack.
5. Click **Next**.

A summary of the order for upgrade packs is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

6. Verify email IDs to whom you want to send the order.
7. Click **Place a Request**.

Your license request number for new upgrade packs is generated. Save this number as you will need to quote this number in all communications related to new upgrade packs.

Upgradation to Higher Version

During valid license period, you are entitled for free upgradation to latest Seqrite Endpoint Security version.

Patch Management

Patch Management (PM) enables the centralized management for checking and installing the missing patches for the applications installed in your network. With this you can also automate checking and installation of the missing patches. Patch Management helps to identify endpoints integrity (host integrity) and reflects the status of the compliance in the reports.

Workflow of Patch Management

1. Install the Patch Management server
2. Add Patch Management server
3. Configure the Patch Management server
4. Scan for missing patches
5. Select the missing patches and install the patches
6. Generate report of the installed missing patches

The procedure of installation is given below. Other steps of Patch Management are described as per occurrence on the console.

System requirements for Patch Management server

System requirements for Patch Management server are same as system requirements for Seqrite Endpoint security server. For more information, see [System requirements for SEPS server](#).



- For more than 25 clients, Seqrite recommends to install Patch Management server on the Windows Server operating system.
- Installation of Patch Management server is not supported on Microsoft Windows XP (32-bit) system.
- The PM client is supported on Microsoft Windows XP (32-bit) system.

Recommendation

For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to public IP.

Installing Patch Management server

To begin installation of Patch Management server, follow these steps:

1. For 32-bit Windows OS, download the setup from one of the following links:

<http://dlupdate.quickheal.com/builds/seqrite/760/en/pmsetup32.msi>

<http://download.quickheal.com/builds/seqrite/760/en/pmsetup32.msi>

For 64-Bit Windows OS, download the setup from one of the following links:

<http://dlupdate.quickheal.com/builds/seqrite/760/en/pmsetup64.msi>

<http://download.quickheal.com/builds/seqrite/760/en/pmsetup64.msi>

2. Launch the setup on machine within the network where you want to install the Seqrite patch server.
3. On the Patch Management Server Setup Wizard, click **Next**.
The license agreement appears. Read the License Agreement carefully.
4. Select the **I Agree** check box to accept the license agreement and then click **Next**.
5. Click **Browse** if you want to install Patch Management server on a different location. To proceed with the installation default path, click **Next**.
6. The Patch Database Settings screen appears. The patch content storage folder path appears. Click **Browse** if you want to change the patch content storage path.
7. Select the **Import Patch Server Data** check box if you want to change the default location. Click **Browse** to locate the path.



If EPS 7.1 patch server database backup is already exported, you can import the database in the EPS 7.6 patch server.

8. Click **Next**.
9. To enable and configure proxy settings, do the following:
 - Select the **Enable Proxy Settings** check box.
 - In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
 - In **Port** text box, type the port number of the proxy server (For example: 80).
 - Select the **Enable Authentication (If any)** check box.
 - In the **User name** and **Password** fields, type in your server credentials.
 - Click **Next**.

10. The Pre-requisite – MySQL 5.6.42 screen appears.

You need to provide a path for MySQL 5.6.42 setup file. If you do not have MySQL 5.6.42 setup file, download from the given link and provide the path.

Click **Next**.

The file will be verified.

11. The MySQL Configuration Setting screen appears.

- i. Enter **Communication Port** number.
- ii. Enter password for MySQL 'Root' user. In the **Confirm password** text box, retype the password.
- iii. Click **Next**.

12. In the Upstream Patch Server screen, select one of the following:

- **Microsoft:** The upstream patch server used is Microsoft patch server. This option is selected by default.
- **Organization Patch server (WSUS):** The upstream patch server used is Organization Patch server (WSUS - Windows Server Update Service). If you select this option, type in WSUS server URL.

13. Click **Next**.

14. In the Website Configuration page, do the following:

- In the Server Configuration section, select one of the following:
 - **Full Computer Name:** Provide the computer name to configure the website
 - **IP address:** Provide the IP address of the target server. However, selecting IP address is not recommended if your network is configured using DHCP.
- In the **HTTP Port** text box, type a port number to use as the server listening port.
- **Enable Secure Socket Layer** check box is selected by default. Type the SSL port number. This port number will serve as a listening port for the server.
- Click **Next**.

15. On confirmation prompt, click **Yes**.

16. The installation summary screen appears. You can change your settings if required by clicking **Back**.

Click **Install**. The installation starts.

17. To complete the installation, click **Finish**.



If installation / uninstallation is failed, then only the **View installation log** check box is displayed. To view the log, select the **View installation log** check box.

18. After the installation is complete, add Seqrite patch server through EPS console and then it becomes available to use.



The Patch Management feature is applicable only for the clients with Microsoft Windows OS; does not support Mac, and Linux operating systems.

Recommendation for the remote clients

For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to public IP.

Back up the patch server data

You can back up the patch database and patch content of the patch server.

To back up the patch Server data, follow these steps:

1. Manually take backup of all the files and folders present in the <installation directory>/Seqrite patch management/patch server/content folder.
2. Select **Start > Programs > Seqrite Patch server Data Backup**. The Backup wizard starts.
3. Click **Browse** to specify the path where you want to back up patch database.
4. Click **Backup**.

The database file, `pmdb.exp` is generated. This file can be used to restore patch server data base.

Offline Patch Synchronizer

You can create an offline Patch Repository. Before repository creation, the Seqrite patch server must be synchronized for the patches of all required applications.

With the Seqrite offline Patch synchronizer wizard, you can do the following:

- 1) Creation of an offline patch repository from the Seqrite Patch Server.
- 2) Synchronization of the Seqrite patch server from the Offline Patch Repository.

This wizard creates an offline Patch Repository by importing patch server data from the Seqrite patch server.

An internet connection is required to download the patch contents if the patch contents are not available on the Seqrite Pat server.

To run the Seqrite offline Patch synchronizer wizard, follow these steps:

1. Select **Start > Programs > Seqrite offline Patch synchronizer**. The wizard starts.
2. Select one of the following,
 - Create offline Patch Repository
 - Synchronize from offline Patch Repository

3. If you select the option, **Create offline Patch Repository**, click **Browse** to specify the path where you want to create an offline Patch Repository.

If you select the option, **Synchronize from offline Patch Repository**, click **Browse** to specify the path which will be used to synchronize the Seqrite patch server.

4. Click **Finish**.

This wizard takes longer time for completion, when run for the first time, as per the patch server data size.



Use the same location next time to create the offline Patch Repository to add new patch server data. No need to create a new repository for the whole patch server data.

Patch Server Control Panel

You can view the status of patch management services with the help of Patch Server Control Panel. This view is used for troubleshooting purpose. To ensure that all the services are in running state for smooth functioning of the patch management server. You can also delete patch metadata and its content which are superseded or of older version.

To access the Patch Server Control Panel, follow these steps:

1. Select **Start > Programs > Patch Server Control panel**. The control panel opens.
2. In the Services section, you can see the current state of the Patch Management services.
3. Click **Start** to start the Patch Management services and all the dependent services. Click **Stop** when you want to stop the services.
4. Click **View Details** to view the status of the following patch management services,
 - AppPool - EPS Patch Scan 3.1
 - AppPool - EPS Patch Server 3.1
 - Website - EPS Patch Mgt 3.1
 - Service - MySQL – SQM31
 - Service – sqpmsvc
5. In the Cleanup section, Click **Start** to delete patch metadata and its content which are obsolete. Click **Stop** when you want to stop the cleanup.

Uninstalling patch server

If you need to uninstall the patch server, follow these steps:

1. Go to **Start > Programs > Uninstall patch server**.
The uninstall wizard starts.
2. Complete the wizard to uninstall the patch server.

SyslogAgent Tool – SIEM Integration

The SyslogAgent is an independent tool used to integrate Seqrite Endpoint Security (EPS) with SIEM (Security Information and Event Management) applications.

The SyslogAgent tool helps you to push all the events logs from EPS Server to the configured SIEM server.

The SyslogAgent tool works with many SIEM vendors that support CEF and LEEF formats. Few supporting vendors are mentioned below for your reference.

- IBM Security QRadar
- SolarWinds Papertrail
- ManageEngine
- Securonix

Operating System Requirement

- Microsoft Windows 8 and above

For windows 8.1

If the OS is Windows 8.1 (32-bit or 64-bit), you need to download and install a latest packager from the following link

<https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170>

Prerequisite

- SIEM Server is installed

Workflow of SyslogAgent tool

Download and execute the tool on the EPS server from which the data needs to be pushed.

After executing the tool, provide credentials of the SIEM Server. Then, set the schedule for pushing the data and select the events of which the data will be pushed to the SIEM server.

You can view the event logs on the configured SIEM server.

Installing SyslogAgent Tool

To install SyslogAgent tool, follow these steps.

1. Download SyslogAgent tool from the following link,
<https://dlupdate.quickheal.com/builds/seqrite/760/en/SyslogAgent/SQSYSAGINST.EXE>
2. Execute SQSYSAGINST.EXE file.
 The SyslogAgent tool is installed.

Using SyslogAgent tool

To push the events data to the SIEM server, follow these steps.

1. Execute SQSYSAGINST.EXE file. The SyslogAgent Configuration window appears. Set all the Syslog server configuration and event selection in the window.
2. Enter **Syslog Server IP\URL**.
3. Enter **Syslog Server Port** number.
4. Enter **Max Record Limit**. This number of records will be pushed to the SIEM server.
5. Select **Schedule Time** from the list. Records will be pushed as per selected schedule time.
6. Select **Protocol** either UDP or TCP.
7. Select **Start Date** with the calendar control.
8. Select **Data format** either LEEF or CEF.



The data formats supported are LEEF (Log Event Extended Format) and CEF (Common Event Format) only.

9. In the Event Selection section, select the events as required.
10. Click **Apply**. The configuration success message appears.
11. The SyslogAgent service will start automatically as per set schedule.

Updating Configuration

To update the configuration, follow these steps.

1. Run SyslogAgentUI.exe from the path, <installation directory>\Seqrite\Endpoint Security 7.60\Admin.
2. The SyslogAgent Configuration window appears.
3. Edit the information.
4. Click Apply.

Uninstalling SyslogAgent Tool

To uninstall the SyslogAgent tool manually, follow these steps.

1. You need to check status of Seqrite SyslogAgent service. Before uninstalling, the service must be stopped.

To check the status of the service, launch the SyslogAgentUI.exe file from <installation directory>\Seqrite\Endpoint Security 7.60\Admin.

2. If the status of service is Running, click **Stop** to stop the service.
3. Open the command line as an Administrator and run the following command

SC DELETE "Seqrite SyslogAgent" (Ensure you put double quotes here)

This command will uninstall the SyslogAgent service only. Installation files will not be deleted from EPS installation directory. These files will be deleted only when you uninstall the EPS Server.

4. If you want to reinstall the SyslogAgent tool, then first manually remove the previously installed SyslogAgent tool files mentioned below and then reinstall.

Keep Self Protection OFF while removing files.

- <Installation directory>\Seqrite\Endpoint Security 7.60\Admin
 - siem_win_service.exe, SyslogAgentUI.exe, sql_res.ini, syslogagent_sp.sql
- <Installation directory>\Seqrite\Endpoint Security 7.60\Admin\config
 - siem_log_config.ini, SiemConfig.json

Technical Support

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

The Support option includes FAQ (Frequently Asked Questions) 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.

To access the Support options, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. On the top right on Seqrite Endpoint Security Dashboard, click the **Support** button.

Support includes the following options:

Web Support: Includes **Visit FAQ** (Frequently Asked Questions) and **Visit Forums** – where you can submit your queries to get an appropriate answer.

Email Support: Includes **Submit Ticket** that redirects you to our Support webpage. 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.

Live Chat Support: Using this option, you can chat with our support executives.

Phone Support: Includes phone numbers. You can call our support team and get your issues resolved.

Remote Support: This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.



The Remote Support feature is available in the clients with Microsoft Windows, Mac, and Linux operating systems.

Remote support feature does not support the Linux clients connected through 'PuTTY' or using an OS without GUI.

Support by Phone

Contact number for phone support: 1800 212 7377

To know more phone numbers for support, please visit
http://www.segrite.com/contact_support

Other sources of support

To get other sources of support, please visit:
<http://www.segrite.com/segrite-support-center>

If the Product Key is Lost

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

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, Maharashtra, India.

Official Website: <http://www.segrite.com>.

Email: support@segrite.com