Seqrite Endpoint Security 7.2

Release Notes

Copyright Information

Trademarks

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.

Contents

1. Introducing Seqrite Endpoint Security 2
2. New Features and Enhancements..... 4
3. Resolved Issues..... 7
4. Technical Support 8

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 designed to provide complete security solutions to small and enterprise-level networks against various kinds of malicious threats such as; viruses, Trojans, worms, backdoors, spyware, riskware, adult content, and hackers.

SEPS is a Web-based management solution that integrates 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.

Available flavors

Seqrite Endpoint Security is available in the following flavors:

- SME (Small and Medium Enterprises Edition)
- Business

- Total
- Enterprise Suite

More Information

For information on the installation and system requirements of Seqrite Endpoint Security, refer to the Administration Guide.

For more information about the product and Data sheet, visit

https://www.seqrite.com/seqrite-endpoint-security

New Features and Enhancements

- Provision to schedule Internet Access - In Web Security, provision to 'Schedule Internet Access' is provided. At endpoint level, internet access can be blocked/allowed as per the policy settings.
- DLP enhancements for new detections - Pin Code, Aadhar Number and Vehicle Registration Number fields are added in the report.
- Email protection supports scanning of encrypted messages sent over POP3 secure socket connection (SSL) protocol.
- Windows 2016 server support added for the EPS client.
- Provision to control Attachment Control Settings – you can block certain type of attachments, emails crafted to exploit vulnerabilities and block attachments with multiple extensions.
- More number of Email IDs/Mobile Numbers in Notification settings. Now you can add 50 email ids and 50 mobile numbers in the notification settings.
- Mail scanning over SSL for DLP detection support for mail body and mail subject for other mail clients.
- In the exported client status report (Clients>Client Status), **Last Connected On** column is added. Now the Administrator can know when the client was last time connected to the EPS Console.
- In the Manages Devices section, **Encryption Status** column is added in the list of devices. This helps to identify encrypted devices. If the devices is encrypted, you can know the encryption type of devices (Not encrypted/Partial/Full). This is applicable for devices added using USB Device method.
- Patch Management supports the following applications along with Microsoft applications,
  - VideoLAN Player
  - Adobe Acrobat
  - Adobe Flash Player
  - Adobe Reader
  - puTTY
  - Notepad++
  - Java
  - 7-zip compression Tool
  - Mozilla Thunderbird
  - Mozilla Firefox
- You can create an offline Patch Repository. With the Seqrite offline Patch synchronizer wizard, you can create an offline patch repository from the Seqrite Patch Server and synchronize the Seqrite patch server from the Offline Patch Repository.

- Now the Patch Management - client-wise report page displays the following patch details:
  - Scanned Patches - Displays the details of scanned patches.
  - Patch Downloaded - Displays the details of downloaded patches.
  - Installed Patches - Displays the details of installed patches.
  - Installation Failed - Displays the details of failed installation of patches.
- In this release, Patch Server Control Panel is incorporated. 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 or of older version and patch server does not need this data in future.
- Provision to enable/disable Backup feature. This feature 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 Reports section, you can generate user wise reports of all the incidents happening on the endpoints.
- The 'User Name' field is added for the following modules in the client reports section:
  - Virus Scan
  - Web Security
  - IPS
  - Application Control (On Access)
  - Advance device control
  - Data Loss Prevention (On access & On Demand)
  - File Activity Monitor
  - Vulnerability Scan
  - Asset Management

  This feature is available in the clients with Windows and Mac operating systems. For Linux clients, there is no change in the reports.
- Admin will receive reports and notification for ransomware incidents occurred at the endpoints. Ransomware detected on endpoints can be configured from Admin Settings > Email and SMS Notification.
- The **User Name** field is added in the Email notification of the following modules:
  - Virus Scan
  - Application control on access
  - Device Control
  - Data Leak Prevention

- Asset Management
- Intrusion Prevention

- In Email notifications Endpoint Name, Domain Name, IP Address, date and time are displayed wherever applicable.
- Default application list in Application Control is updated.
- Mirroring Logic is introduced in the Update Manager feature. This download applicable definition files from the update server if these files are missing or corrupt in the Update directory.

  Mirroring Logic have resolved 'Unable to complete the download process Error (1001)' reported for EPS Client.
- Linux client
  - New OS support for Linux-
    - Fedora – 25 (32-bit)
    - openSUSE -13.2, 42.2 (32-bit)
    - Linux Mint – 18 (32-bit)
    - Ubuntu - 16.10 (32-bit)
    - Linux Mint – 18 (64-bit)
    - Ubuntu - 16.10 (64-bit)
    - RHEL - 7.3 (64-bit)
    - SUSE Linux - 12.2 (64-bit)
    - CENTOS – 7.0 (64-bit)
  - Remote Support module helps us easily connect to your computer system remotely and assist you in resolving technical issues. The Remote Support feature is now available in the clients with Linux. Till now the feature was available in the clients with Microsoft Windows and Mac operating systems.

Resolved Issues

The following bugs are fixed:

- Unable to revert Windows Update Settings back to default after disabling PM Server from Policy.
- Getting Error "Some internal error occurred, please try later" while scheduling Patch synchronization.
- CD/DVD contents does not show if unknown category is blocked under ADC- EPS 6.4
- Browsing/Internet Activity stops suddenly on random time post installing Linux Client
- System hang issue due to high disk consumption by Seqrite Scanner process EPS 7.0.
- When the EPS server is installed in multi-server mode and then uninstall lower EPS version, the clients of higher EPS version are not displayed in the console.

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.seqrite.com/contact_support

Other sources of support

To get other sources of support, please visit:

http://www.seqrite.com/seqrite-support-center

If the Product Key is Lost

Product Key serves as your identity to your Seqrite Endpoint Security product. If you lose the Product Key, please contact Seqrite 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.seqrite.com.

Email: support@seqrite.com