Seqrite Endpoint Security 7.3

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 4
2. New Features and Enhancements..... 6
3. Resolved Issues..... 9
4. Technical Support 10

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

- Support for Medium Size Networks of up to 5000 endpoints
- Master-Slave architecture to support larger network
- Improved Performance in terms of disk and memory utilization
- Group Administrator for groups

  Provision to create a Group Administrator user to be assigned to any group. The Group Administrator can manage certain groups and locations.
- Device Control

  Connection to Authorized Wi-Fi Access Point only
- Improved Application Control feature

  Provision to block an application by its name.
- Self Protection for Seqrite EPS Server components (files, folders, processes, services, and registries)
- Support to IMAP and MAPI protocols for Email and Spam Protection
- Improved Firewall with ability to block/allow application.
- Port configuration in Email Settings

  Provision to configure different ports in the Email client settings so that email protection can be availed on another port when the Email Client runs on the port other than the default ports.

  Port configuration can be done for POP3, IMAP, SSL Port.
- Trusted email client configuration on endpoints

  Provision to configure trusted email client settings to control which Email clients are allowed to send the Emails on the endpoints.
- Desktop Shortcut creation at client side

  You can configure the desktop icons which are automatically created during EPS Client Installation.
- System Tray Icon should turn to red after specified days.

  Provision to configure number of days for not up to date client. The system tray icon at the client turns red when the client is not being updated for specified number of days.
- Dashboard Enhancements
  - Statistics of Not up-to-date clients for more than 1, 3, 7, 15, and 30 days
  - Report of those endpoints where updates are not successful/failed along with error information.

- Centralized Rollback Option

Provision to rollback updates for selected endpoints so that you can revert to previous updates if required in case of faulty updates.

- Reports
    - Under Virus scan reports, provision to view scan status of endpoints that are not scanned from 1, 3, 7, 15 or more than 30 days.
    - User will need to fetch the reports of Vulnerability Scan using Endpoint Name only
- Automatic installation of Service Pack on EPS Server

  Provision to apply the EPS Service Pack automatically or manually on the EPS Server.
- Enhancements in Notifications

  Provision to receive E-mail notifications in the following scenarios,
    - unprotected systems in the network
    - when any EPS client gets installed/uninstalled from remote endpoints
    - when new updates are downloaded by the Update Manager
- Context sensitive Help
- EPS Server Platform Compatibility

  New OS support for EPS Server-
    - Microsoft Windows 10 Fall Creators Update
    - Microsoft Windows 10 Creators Update
    - Microsoft Windows Server 2016
- Client Platform Compatibility
    - Linux client

      New OS support for Linux-
        - RHEL – 6.9, 7.0, 7.1, 7.2, 7.3
        - Fedora – 22, 23, 24, 25
        - Ubuntu – 17.04
        - CentOS – 6.6, 6.7, 6.8, 6.9, 7.0
        - OpenSUSE – 42.3
        - SAMBA version 3.5.x to 4.5.x (32-bit & 64-bit)
    - Mac Client
        - Mac OS support - 10.13 High Sierra
- EPS clients are not supported on Windows 2000 operating system.

- The following antivirus products can be detected in addition to the existing antivirus products,
    - Symantec Endpoint Security 14.0 RU1 MP1
    - Panda Global Protection 2016
    - Kaspersky Endpoint Security 10.3.0.6294 for Windows
    - Eset Endpoint Security 6.6.2068.
    - eScan Corporate for Windows Client 14.0.1400.2029
    - Avast Endpoint Protection Client 8.0.1609
    - Trend Micro OfficeScan Client 12.0.1222
- Patch Management
    - Server
        - Throttling support for Patch Install and Patch Scan
        - DB Compression
        - One Click Patch Scan
        - Support for Windows Server 2016, Windows RS2 and RS3
        - Updated error message for Patch installation failure
        - Support for Putty's MSI installer
    - Client
        - PMCLSRV.EXE will be installed at the client; if Patch Server is enabled under Policy
- If Email id is modified/changed on Activation Server the change will be automatically reflected on Roaming Platform.

Resolved Issues

The following bugs are fixed:

- Partial Uninstall causing system crash / Unable to Boot Win 10 - 1709 Build - EPS 7.0
- Correct status is not shown when patch installation fails
- Windows 8.1 updates stored in control panel but are not installed on the system
- Browsing & browser functionality gets hamper due to Web Security Protection on MAC systems
- Unable to Send Email due to Core Mail Protection Service - EPS 7.2
- Server Drive Backup getting Failed due to Real Time Virus Protection - EPS 7.2

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