Seqrite Endpoint Security 7.6

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

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.

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

- Master and multi-level secondary server architecture - As per your geographical locations, multiple and multi-level secondary servers are possible as per your requirement.
- 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

  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.
- When Master admin logs on Secondary server via auto login, then Master admin activity logs will be generated in Secondary sever event logs.
- Asset Management feature displays the 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.
- Provision to lock license with respect to country. The EPS License should be functional only in the specified countries.
- 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.
- As a part of branding, added logo for GoDeep.AI on EPS console footer.

- Provision to add Multiple IP addresses and DNS names (URL) in exception of Seqrite Firewall.
- 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.
- 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 is 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

    When a new Microsoft Office file is generated, DLP asks to classify the file as Confidential or Public. You can classify existing files also.
- Included latest 'Remote Support Tool - Team Viewer version (14.1.18533 QSC)' in Windows client AV builds.
- EPS server compatibility with Windows 10 RS5 - 32 bit/64 bit.
- EPS server supports MySQL 5.6.42 version.
- On 64-bit Linux operating system - Linux Client AV GUI is now supported.

Technical Support

Seqrite provides extensive technical support for its users. In case you face any technical issue, you can contact our Technical Support center using the options available at the following URL:

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