Seqrite Endpoint Security 8.1

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

Seqrite Endpoint Security is an integrated solution that allows the management and regulation of multiple Endpoint Security products deployed at different geographical locations. IT administrators from any location can easily connect to view the latest security status, configure product policies, receive notifications, and rectify critical network events from one single dashboard. Seqrite Endpoint Security also facilitates policy configuration, backup and more for Seqrite products.

Features and Enhancements

- File Sandbox
  - A new add-on feature which helps you submit a suspicious file for analysis to determine if the file is malicious or safe.
  - Sandbox detonation means Sandbox security testing detects malware by running suspicious code in a safe and isolated environment and monitoring the behavior and outputs of the code. This is known as “detonation”.
- File Activity Monitor (FAM)
  - FAM monitors file activities on the local drive and removable drive and generates reports as per event.
  - The copy, delete and extension change file activities are monitored. (Copy activity is monitored only in the removable drive)
  - FAM feature is available in clients with Windows and Mac operating systems.
  - FAM is supported on macOS Catalina 10.15 and above.
- Multi-factor Authentication (MFA) support is provided for signing in the Seqrite account.
  - Multifactor Authentication (MFA) provides two-step verification which provides stronger security for your account by requiring a second verification step when you sign in. Here, after providing credentials, you need to provide OTP for authentication via registered Email.
- SIEM Integration helps to push all the events logs from EPS Server to the configured SIEM server.
- IDS / IPS policy
  - Customized support to exclude port and IP address added for Port Scanning attacks and DDOS attacks.
- Firewall
  - Support to add the following in the Firewall exception.
    - Multiple Remote IP addresses
    - Domain name
    - Application Path
    - Inbound/Outbound Connections
- In Advanced Device Control, support is added for ‘Add USB by Serial Number’.

- While installing the EPS client, if another antivirus software is already present on your endpoint, client installation does not proceed further until you uninstall the other installed antivirus software to avoid conflicts.

  Now, you can set the automatic uninstallation of other antivirus software.
- Policy Migration from EPS 7.6 to EPS 8.1. For the current EPS 7.6 customers, SEQRITE is providing a tool to migrate the data of clients, groups, and policies from EPS 7.6 to EPS 8.1.
- Drilldown capabilities on Dashboard widgets

  On the Dashboard page, the count on the widget is drilled down to the status page or respective report page with an applied filter.
- Patch Management
  - You can add multiple Patch servers.

    User can assign different Patch Server for different policies.
  - Provision to Synchronize with the Local Seqrite Patch Server.
  - You can Schedule Patch Synchronization or you can start Synchronization instantly.
- Complete backup / Restore for EPS Console (Mongo only)
- Mac
  - Roaming support for Mac Client
  - Mac client compatibility with macOS Ventura 13
- New web categories ‘Unknown' and 'Cyber Security Awareness and Training Simulation Sites' are added in the Web Security list.
- Application control – Latest application versions are included.
- Update Agent and Standalone Update Manager to download the updates
- Support to remote connect to EPS Server using TeamViewer

For more detail on the Features and working, please refer the help/Manual.

System Requirements

- Single Node: Server that supports up to 5000 endpoints
  - CentOS: 7.5
  - Disk Space: 40 GB or above
  - RAM: 8 GB or above
  - Processor: 4 Core(x86-64),2.60GHz or above

- Single Node: Server that supports up to 25000 endpoints
  - CentOS: 7.5
  - Disk Space: 100 GB or above
  - RAM: 32 GB or above
  - Processor: 16 Core(x86-64),2.60GHz or above

  Note:

  For distributed installation, two machines are required with the same configuration as mentioned above.

- OVA support, Server that supports up to 3000 endpoints (Single Node)
  - OVA File name: EPS8.1_CentOS7.9.ova
  - Oracle Virtual box version: 6.1.38
  - RAM: 8 GB

  For more details refer to Features and Enhancements.

Known Issues

Server Side

- Hostname is not supported during Server Installation.
- After DB is restored, duplicate entries of the default client appear on the Status page, one with online status and the other with offline status.

  Workaround:

  To remove the offline client, follow these steps:

  1. On the Status page, select the offline endpoint.
  2. The client action bar is enabled above the table. In the Client Actions dropdown, select **Remove Selected Endpoint(s).**
  3. Click **Submit**. A confirmation message appears.
  4. Click **OK**. The endpoint is removed.
- While adding USB by serial number, editing the existing device name sometimes throws an Error “40065 if the name already exists in the list.
- Before Migration, if the Admin user knowingly adds the same USB by serial no. on both EPS consoles (7.6 & 8.1) then migration fails.

  Work Around:

  1. Log on to the SEQRITE Endpoint Security 8.1.
  2. Go to configuration > Device Control.

     The list of devices which are already been added appears.
  3. Select that duplicate USB Serial Number Entry and delete the entry.
  4. Go to EPS 8.1 console > Deployment > EPS 7.6 Migration page.

     Again, Import the Export.zip file.

     Migration will be successful.
- File marked as Confidential in the DLP feature cannot be submitted for detonation in the File Sandbox.
- Failed detonations do not show the Completion Time in the File Sandbox report.
- Mac client - Sometimes Software change reports for Asset Management are not generated.
- In the reports of IDS/IPS port scan and DDOS scan, the "Target IP" column does not contain any data.

- CNTRL+C command is not recommended during EPS Server installation process. If CNTRL+C is pressed on the terminal at the time of installation (GUI mode) then rollback may fail to initiate and installation need to be initiated again.
- Help portal
  - "Home" link on the help documentation page redirects to the global online help portal.
  - You cannot print the Help page with help of the **Print** icon on the help page. You can download and print PDF from the **Download PDF** link in the left pane.
- The health monitoring emails do not support YOPmail and Gmail.
- AD Sync Failure Notification is not sent to the configured Email address.
- Email containing the report will not be sent if PDF reports contains non-ASCII characters.
- HTTP Port is not supported for communication with Patch Management (PM) Server.
- In roaming's reactivation OTP mail, instead of "Roaming Service", the words used are "Roaming Clients".

Client Side

- Web Security - web categorization and block specified feature currently not supported on RHEL 8.6.
- Roaming Status is displayed as 'Not Connected' on endpoint AV application > About Seqrite Endpoint Security> Server Details even though the client is in the Roaming state.
- File Activity Monitor (FAM)
  - Copy events are not captured when the file is copied from Removable Drive to Local Drive.
- EPS Clients are not compatible if Smart App Control is Turned-On on Windows 11.

Mac

- Data Loss Prevention (DLP)
  - DLP block functionality will not work on macOS Catalina 10.15 and above if the attachment is sent through any mail application through the Safari browser.
  - File downloading is getting blocked through the browser if DLP is enabled.
- File Activity Monitor
  - The 'Delete' event is created with some temporary file name while 'creating' or performing the 'Save/Save As' file on the Local Drive or Removable Drive.
  - The Extension changed event is captured if we copy file using TeamViewer from other Mac system on the Local Drive and Removable Drive.

- If we compress files using any compressing tool, then a Delete event is captured for all the compressed files.
- The events are not captured if we drag and drop or move the file using the terminal command mv on the same Removable and Local drive.

Linux

- Tray icons and notifications are not supported on systems using the Wayland display protocol.
    - Desktop shortcuts for Seqrite needs a user's Trust Approval to display product's icon shortcut. Double click the shortcut and click "Trust & launch".

Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPS 8.1 client.
2. To install EPS 8.1 client on windows 7 and windows 2008 R2, you need to install these windows Patches for SHA2 compatibility:
   - For Windows 7: KB4474419 and KB4490628.
   - For Windows 2008 R2: KB-4474419 and KB-4490628
3. To install patches on Windows 7 32-Bit client, you must upgrade to Internet Explorer version 11.
4. If the administrator initiates tuneup notification for the endpoint and if the endpoint is not logged in, then the tuneup notification will fail.
5. Advanced Device Control: If an authorized and encrypted device is formatted, the device will be treated as an unauthorized device. In this case, Administrator will need to add the device again in Device Control and configure the policies accordingly.
6. To use Browser Sandbox, turn off the Secure Boot feature of the system from BIOS Configuration.
7. By default, Spam Protection is disabled. So, a red exclamation mark appears on the client Dashboard.
8. Linux
   - It is recommended to disable SELinux for RHEL-based distro stream.
   - Remote Support tool cannot be executed with ‘sudo’ command. The tool can be executed with super user (su) command.

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