Seqrite Endpoint Security 8.2

Release Notes

27 July 2023

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

Revision History

The information in this document is provided for the sole use of Quick Heal Research and Development, and Support Team. It is strictly forbidden to publish or distribute any part of this document to any other party.

Doc Version	Date	Comment
1.0	27 July 2023	Seqrite Endpoint Security 8.2 Released

Features and Enhancements

With this release, the following features are added to EPS 8.2.

- **High Availability (HA)**

  High Availability (HA) refers to the design and implementation of systems and architectures that ensure continuous and uninterrupted access to services, applications, and data, even in the case of hardware failures, software glitches, or other disruptions.

  This feature:

  - Provides high availability for the Seqrite EPS 8.2 solution.
  - Automates deployment of complete clustering components through Ansible.
  - Supports directory synchronization for log backups.
  - Deploys cluster maintenance and alert scripts using Ansible.

- **Custom Server Certificate**

  EPS 8.2 by default supports self-sign certificates. Now, there is a provision to replace the public key certificate if a customer has it. This enhancement lets you replace the custom certificate. It can be done more than once.

- **OVA**

  You can now deploy OVA on the VirtualBox and set up Seqrite Endpoint Security server.

- **Application Control – Block All**

  In addition to the Allow All settings, now Block All is added. With these settings, all applications are blocked by default except for the applications present in the Allowlist.

- **EDR**

  - **MISP Integration**
    - MISP Threat Sharing, an open-source threat intelligence platform is now included in the EDR setup.
    - High threat level malicious data is pulled from the open source MISP server in endpoint threat hunting and the automated ETH scan is performed on clients. This activity is run daily or weekly so that the actions can be performed on real-time hashes present on client.
  - **OS Query – Endpoint Interactivity for Information Gathering**

    Live Query is a new EPS feature from which a query can be run on endpoints in real-time and identify areas of improving security.

- **Blocking IOCs Based on Hash Values**

Apart from the existing on demand/scheduled ETH scan, real-time searching and blocking of hashes is added as a new feature.

- **Web Security**
    - YouTube Access Controller
        - YouTube videos can now be allowed/blocked based on categories.
        - Selected publishers and channels on YouTube can now be blocked/allowed by using the block or allow list.
        - Google Chrome (version 92 and above) or Microsoft Edge (version 110 and above) are the only supported browsers.
    - Google Access Controller
        - With the Seqrite's new extension 'Web Access Controller', administrator can ensure that the users within the organization can only sign into the Corporate Google Accounts on the endpoints. (For specific domains that are configured by the Administrator).
        - Google Chrome (version 92 and above) or Microsoft Edge (version 110 and above) are the only supported browsers.
- **Dashboard**
    - ETH Widgets - UI
        - ETH related data can be availed from UI. There is a separate tab for ETH widgets that is EDR tab.
- **Admin Settings**
    - Email notifications are now part of Admin settings
        - Email Configuration is now tenant level setting instead of policy level setting.
        - Instead of Groups, now it will be applicable to all the registered endpoints.
- **Installer**
    - EPS 8.2 Installation via FQDN
        - Now we support FQDN based EPS server installation along with IP Address based installation. The Server Console URL can now have a fully qualified domain name.
- **Configure Update Agent by IP Address**
    - Now you can assign Update Agent role to the selected endpoint by IP address as well as domain name.
- **Linux**
    - **Self-Protection Support**

        - The Self-protection feature is to provide a common framework to protect Seqrite installation files and folders from unauthorized modification.
    - **Roaming Support**
        - Added roaming support for Linux agents.
- **Https Communication**
    - Added capabilities for MAC and Linux.
        - Communication over Https protocol.
        - AV updates on Https only for MAC whereas Linux continues taking updates using Http protocol.
        - URL Categorisation.
- **Heartbeat Interval**
    - Default heartbeat: 3 minutes. It can be configured from 1 minute to 5 minutes from the Admin settings.
- **Device Control**
    - **Temporary USB Access Control Duration to 30 Days**
        - Now we support USB device access for a maximum of 30 days.
        - Supports Windows.
    - **USB Tethering**
        - Administrators can now block internet sharing through mobile phones/dongles.
- **Logging Support for MAC**
    - This feature allows you to enable Web Security logs under the product installation directory.
    - If any issue occurs on the Mac client related to Web Security, then you can enable debug log.
    - This feature is applicable to only MAC clients.
- **[Mac, Linux] Web Protection Unknown Category Support**
    - [Mac, Linux] Web Protection 'Unknown' and 'Cyber Security Awareness and Training Simulation Site' category Support.
- **Client Install/Uninstall Notification**
    - Client Agent now sends Installation Notification to the server. This notification is sent to the server after successful AV Installation as well successful activation of AV.
    - Client Agent also sends an uninstallation notification to the server once AV uninstallation is successful on specific endpoint.
- **Export Excluded Devices List**

- Export list of excluded devices in excel format which are used under policy.
- CSV export functionality is available for device control configuration.
- Navigation: Reports > Advance device control > tabular.
- A new default query should be added to view exception list.
- After clicking View, tabular data is shown, without any filter (same as host integrity).
- Following column details are displayed in Device Exceptions Report:
  - Device Name, Device Type, Model Name, Serial Number, Policy Name, Policy type, Encryption Status, Authorized, Vendor ID, Product ID.

- **Port - IP Whitelisting for (IDS level only)**
- **Group wise Endpoint Migration from EPS 7.6 SP5 to EPS 8.2**
  - Added capabilities to move endpoints by the group.
- **Alert Enhancement for Email**
  - If the SMTP server is down for some reason, an alert message appears on the screen as **Failed to send Email as SMTP server is not reachable.**

  It appears once in 24 hours.

For more detail on the Features and functionalities, refer the respective guide/help.

System Requirements

System Requirements for EPS Server

Server that supports up to 0 to 5000 endpoints

- Ubuntu 22.04
- Available Disk Space: 60 GBs or above
- Available RAM: 8 GBs or above
- Processer: 4 Core(x86-64), 2.60GHz or above

Server that supports up to 5001 to 15000 endpoints

- Ubuntu 22.04
- Available Disk Space: 100 GBs or above
- Available RAM: 16 GBs or above
- Processer: 8 Core(x86-64), 2.60GHz or above

Server that supports up to 15001 to 25000 endpoints

- Ubuntu 22.04
- Available Disk Space: 150 GBs or above
- Available RAM: 32 GBs or above
- Processer: 16 Core(x86-64),2.60GHz or above

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

System Requirements for OVA Server

- Physical Windows Machine with RAM >= 16 GB
- Windows 10 and above OR Windows server 2019 and above
- Disk space: 60 GB and above.
- CPU: 4 Core (x86-64) or above.
- The VT-x must be enabled in the physical machine's BIOS.
- Oracle Virtual Box 7.0.8
- EPS_8.2_UBUNTU22.ova build file.
- Keep the following details ready and handy.
    - Product Key

- Static IP Address
- Gateway
- Subnetmask
- DNS

Note: For seamless working of OVA over virtual box, it is recommended to have only one hypervisor installed on the system. Other than the Oracle Virtual Box, ensure that no other hypervisor is installed on the system.

System Requirements for EPS Client

- **Windows**

  Supportability matrix remains the same as 8.1.

- **Mac**
  - **Processor**: Intel core or Apple's M1, M2 chip compatible
  - **OS**: X 10.12, 10.13, 10.14, 10.15, 11, 12, and 13

  Note: No support for Mac OS 10.11 and below.

- **Linux**

  Supportability matrix remains the same as 8.1.

Known Issues

- **High Availability**
    - Installation of HA setup on an EPS server configured with IP is supported. If it is configured with a Domain Name, then it is not supported.
    - After a failover, the Pending Policy and Client Action of the failed node might not get processed on another node intermittently. As a workaround, you can reapply Policy and Client Action on the affected endpoints.

  Recommendations and limitations for virtualized deployments:

    - Ideally, place all three nodes on separate Hypervisors to mitigate the risk of physical node failure.
    - Consider placing the disks of the two data-bearing nodes on different data stores.
    - The architecture cannot guarantee stable behavior or prevent a split-brain situation if an older snapshot is incorrectly restored that does not merge the state with stateful services on either node.
    - HA requires a minimum of 2 nodes out of 3 to be operational for cluster formation and application launch.
- On selecting migration option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is not displayed.
- Duplicate entry is getting reflected for default client after DB backup restoration.
- Before Migration, if the Admin user knowingly adds the same USB by serial no. on both EPS consoles (7.6 & 8.2) then migration fails.

  Work Around:

  1. Log on to the SEQRITE Endpoint Security 8.2.
  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 8.2 console > Deployment > EPS 7.6 Migration page.

     Again, Import the Export.zip file.

     Migration will be successful.
- Failed detonations do not show the Completion Time in the File Sandbox report.
- If malware is found at the long path (more than 260 characters), the complete file path is displayed in Virus Protection and Scanner Reports on a client in Scanner > Reports

section. But the same path is displayed in the truncated format in the Virus Scan Reports on EPS Console.

- For Mac: 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.
- 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".
- Application Control: Child Folder are also getting added even if Parent folder is already whitelisted.
- Application Control: An alert is not displayed on Server if Golden image is not downloaded on Client after maximum attempt.
- Application Control: Applications are blocked when executed from network mapped drive even when their publishers are in allowed list.
- Application Control: Allowed and Opened exe is not getting terminated after changing its policy (status) to block.
- 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.
- EPS Clients are not compatible if Smart App Control is Turned-On on Windows 11.
- Application Control: On the Allow All Applications settings screen, when you click the Checkbox, all the custom checkboxes are selected
- For 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.
- Linux Tray icons and notifications are not supported on systems using the Wayland display protocol.
- Linux: 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 8.2 client.
2. To install EPS 8.2 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 distribution stream.
   - Remote Support tool cannot be executed with ‘sudo’ command. The tool can be executed with super user (su) command.
   - On selecting migration option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is displayed.

