Seqrite Endpoint Security 8.2.1

Release Notes

22 February 2024

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	22 February 2024	Seqrite Endpoint Security 8.2.1 Released

Features and Enhancements

With this release, the following features are added to EPS 8.2.1.

- **Encryption Policy**

  Seqrite encryption policy lets you encrypt sensitive data and protect it from unauthorized access.

  This feature enables you to encrypt or decrypt:

  - Windows operating system Volumes.
  - fixed data volumes.
- Option to configure custom update download path from the EPS console.
- Allow Group Admin to move endpoints within its own group/subgroup.

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

System Requirements

System Requirements for Configuring the Encryption Policy:

Server Pre-requisites:

Service Pack 1.0 applied on Linux EPS Server.

Note: Refer the Steps_To_Apply_SP guide for more details on applying the SP.

Client Pre-requisites:

1. Hardware**:**
   - TPM 2.0
   - BIOS with UEFI mode
2. OS**:**
   - Windows 10 64-bit
   - Windows 11
3. AV update – VDB 21st Feb 2024 or later

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.
- Have 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, 13, and 14

  Note: No support for Mac OS 10.11 and below.

- **Linux**

  Supportability matrix remains the same as 8.1.

Bug Fixes

The following table consists of the bug fixes from previous releases.

Sr. No.	Summary
1	Enhanced application security.
2	Enhanced endpoint details in CSV exported from status page.
3	Group Admin Role User can perform patch install on endpoint.
4	Issue in sorting groups is fixed.
5	Password fields on Client Package creation are made interactive.
6	Policy UI field under Device Control, MAC-Address is now called as **BSSID**.
7	Enhanced Health monitoring Services integrated.
8	Custom added Update Agent name is now getting saved and is now visible when we press the default button in the policy.

Known Issues

- The encryption events in the 'Activity Report' might not be in sequential order.
- For checking the completion status of encryption/decryption, refer to the endpoint status from the server console > Status.
    - Completion status for encryption/decryption will not be available in the activity report.

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.

