Seqrite Endpoint Security Cloud 2.0

Release Notes

26 August 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	26 August 2023	Seqrite Endpoint Security Cloud 2.0 Released

Features and Enhancements

With this release, the following features are added to EPS Cloud 2.0.

- **AV Status**

  With this new enhancement, you can now view the anti-virus status of the endpoint on the **Endpoint Security** > **Status** screen of HawkkEye.

  These are the AV status options:

  - **In Progress:** Is displayed if only Client Agent is installed, and if it is a fresh installation.
  - **Success:** Is displayed once the installation is successfully completed.
  - **Failed:** Is displayed if the installation is interrupted and if an error code comes.
  - **Reboot Required:** Is displayed when the antivirus is already installed on an endpoint however, the reboot is required for its proper functioning. Usually, it happens when the upgrades are received for the endpoints.
  - **NA:** Is displayed for the Linux or Mac clients. Is also displayed for the already existing endpoints before implementing this UI change on the server side.

- **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.

- **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.

- **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.
- **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.
- **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.
- **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 2.0**
  - Added capabilities to move endpoints by the group.

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

System Requirements

System Requirements for EPS Clients

For Installing SEQRITE Endpoint Security client through client install utility, the System requirements are as follows:

Any one of the following operating systems:

Windows OS

- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (64-bit)
- Windows 10 November 2019 Update
- Microsoft Windows Server 2022 Standard / Datacenter / Essentials

MAC

Processor

- Intel core or Apple's M1, M2 chip compatible

Mac OS

- MacOS X 10.12, 10.13, 10.14, 10.15, 11, 12, and 13

Linux 32-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier

Supported Distributions for EPS Client

- Debian 9, 10
- Ubuntu 14.04,16.04
- Boss 6.0
- Linux Mint 19.3

Linux 64-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier

Supported Distributions for EPS Client:

- Fedora 30, 32
- Linux Mint 19.3, 20
- Ubuntu 16.04, 18.04, 20.4, 22.04
- Debian 9, 10
- CentOS 7.8, 8.2
- RHEL 7.5, 7.8, 8.2, 8.6 Enterprise
- SUSE Linux 12. SP4 / Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0
- Oracle Linux 7.1, 7.9 and 8.1

General Requirements

Windows

Processor

- Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) processor
- Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) processor

RAM

- Minimum: 1 GB
- Recommended: 2 GB free RAM

Hard disk space

- 3200 MB free space

Web Browser

- Internet Explorer 7 or later

Network protocol

- TLS 1.2

MAC

Processor

- Intel core or Apple’s M1, M2 chip compatible

RAM

- Minimum: 512 MB
- Recommended: 2 GB free RAM

Hard disk space

- 1200 MB free space

Linux

Processor

- Intel or compatible

RAM

- Minimum: 512 MB
- Recommended: 1 GB free RAM

Hard disk space

- 1200 MB free space

Known Issues

- On selecting migration option for a group with one Linux and another Windows client machines, the warning message **Linux client migration is not supported** is not displayed.
- Before migration, if the Admin user knowingly adds the same USB by serial no. on both EPS consoles (7.6 and 2.0), then migration fails.

  Work Around:

  1. Log on to the SEQRITE Endpoint Security 2.0.
  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 2.0 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 folders are also getting added even if Parent folder is already whitelisted.
- Application Control: An alert is not displayed on the server if Golden image is not downloaded on Client after maximum number of attempts.
- 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 2.0 client.
2. To install EPS 2.0 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.