Seqrite

# Endpoint Protection Cloud

# Release Notes

Cloud 5.0 | 31 Aug 2024

www.seqrite.com

# Copyright Information

## Trademarks

## License Terms

# 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 | 31 Aug2024 | Seqrite Endpoint Protection Cloud 5.0 Released |

# What’s New

With this release, the following features are added to EPP Cloud 5.0.

## Server-Side: Feature Highlights

### Collecting Logs from Endpoints via Console

Administrators can now collect logs directly from the Seqrite EPP Web Console from Windows, macOS, and Linux clients required for key diagnostic information for troubleshooting. Logs are available for download via Dashboard > Status > Endpoint Status.

### Introducing Windows Server Container Policy and Group for Windows Sever Operating Systems

A new Windows Server Group and Windows Server Container Policy has been introduced, for Seqrite EPP clients running on Windows Server Operating Systems. This update includes a new configuration setting located under **Console > Configurations > Client Installation** for assigning clients to this Group-Policy.

- For new customers, the group-policy will be automatically applied by default.
- For existing customers, additional steps are required to configure the new setting.

### Automatic DLP License Assignment

Introducing the DLP license assignment mode that allows administrators to select between manual and automatic license allocation for endpoints. This update includes a new configuration setting located under **Console > Configurations > Data Loss Prevention.**

- **Automatic Assignment**:
  - Licenses are assigned automatically when available.
  - If no licenses are available, notifications will be displayed.
  - For new customer onboardings, if the DLP License Count matches the Total License Count, Automatic mode is used. Otherwise, Manual mode is applied.
- **Manual Assignment**: will remain as is.
  - When switching to Automatic mode, if no licenses are available notifications will appear in the EPP Console. These notifications will continue to display for all new registrations until you revert to Manual mode.

## Server Receipt Time for Endpoint Events

**Enhanced Event Tracking**: Added server receipt time for events from endpoint to accurately map the flow from endpoints to the server. This enhancement includes the addition of the Server Date & Time column in both the server console report and CSV exports.

## Third-Party Antivirus Detection

We've added a new setting under **Console > Configurations > Client Installation > Detect other Antivirus applications**. This feature helps identify and manage third-party antivirus software during Seqrite EPP client installation. Ensure this option is selected to detect existing antivirus programs and prevent conflicts. Deselect this option only if you are certain no other antivirus applications are installed.

Note: This setting will only apply to new client packagers or Client Agents deployed after the change in the Seqrite EPP Web Console. It will not affect clients or packagers deployed before the change.

## Windows Defender Detection

Windows Defender on server operating systems and Quick Heal Retail AV products will continue to be detected regardless of the 'Detect other Antivirus applications' setting. However, these products will not be uninstalled automatically.

## Enhanced Third-Party Antivirus Reporting

The client installation process now includes a feature that sends the name of any third-party antivirus software causing installation conflicts directly to the Seqrite EPP Web Console. The name of the third-party antivirus will be displayed on the Seqrite EPP Web Console **Dashboard > Notifications**.

## Seqrite EPP 10.12 Client Agent: Quick Heal Anti-Fraud Detection

Added Quick Heal Anti-Fraud detection.

## Complete Hostname Display Enhanced

**Increased Hostname Length**: The maximum allowable length for hostnames has been increased from 15 characters to 25 characters. This ensures that the complete hostname is now fully visible wherever hostnames are displayed in the Seqrite EPP Web Console.

## User Role Management Enhancement

You can now modify user roles directly from the Seqrite EPP Web Console. Additionally, the "Role Name" is now displayed on the User Page for reference.

## Patch Management Configuration Using Public FQDN

Patch management installation now supports the use of public Fully Qualified Domain Names (FQDNs).

## New Search Functionality

- Application Control
    - Added search functionality in *Configuration > Application Control > Allow All Applications***,** allowing searches by application name or process name**.**
- Policies
    - Enabled search by endpoint name in Policies > View Details > Pending Endpoint**.**
    - Enabled search by application name in Edit Policies > Application Control > Allow All Applications**.**

## Data Loss Prevention (DLP)

- Custom Action addition

  This option gives us more freedom to report or block (for example, now only PDF can be blocked and other file formats like word, excel can work freely and vice versa.
- Custom Apps
    - Custom Applications: This feature lets you add the applications that you need to monitor or exclude from the DLP.
    - User can now customize the block report action on multiple data types.
    - Users can Block and report multiple data types and can customize the block all and report only files respectively.
- Custom Classifiers

  A custom list of classifiers is meant for monitoring data transfer through a channel. It is a tailored set of rules or criteria used to identify and categorize specific types of data as they move through communication channels within a network.

## Boot Scan Protection

Added password protection for skipping boot scans, enhancing security measures.

## Miscellaneous Feature Highlights

- Added a Cancel button on the Policy Page alongside the existing Save button**.**
- Addressed vulnerabilities related to password management on the client side.
- Added a "Manufacturer Name" column to the advanced device control features for improved device identification.

- Added "MAC Address" and "IP Address" columns to reports for more detailed network information.
- Third-party Antivirus Detection: Added support for
    - HP Wolf Security 11.x.
    - Sophos Endpoint Agent 2023.2.x.
    - Added support for ESET Endpoint Security 11.x.

# Client-Side: Feature Highlights

## Group and Policy Visibility Enhancement

A new feature has been added for Windows, macOS, and Linux clients, allowing users to view associated group and policies. Access this information through the client console under **Help > About Page** by clicking the **Server Details** button. This section displays:

- **Server:** IP address or domain name of the Seqrite Endpoint Protection server.
- **Group:** Seqrite Endpoint Protection group assigned to the client.
- **Policy:** Seqrite Endpoint Protection policy applied to the client.
- **Connection Status:** Indicates if the connection between client and server is active or inactive.
- **Last Connected Time:** Shows the most recent successful connection time.
- **Error Message:** Provides details on connection issues, or states 'No Error' if none are present.

# Windows

## Update Agent Compatibility and Support

The latest Update Agent supports downloading updates for clients from Client Agent version 10.8 onward, across Windows, macOS, and Linux platforms.

# macOS

## Advanced Device Control Support for macOS ARM64 Systems

The latest update introduces support for Advanced Device Control on macOS ARM64-based systems, improving device management capabilities for ARM64 architecture environments.

# Linux

## Client Support for Mint 21.3 and RHEL 9.x

The Seqrite EPP Cloud 5.0 client is now supported on Linux Mint 21.3, RHEL 9.0, 9.1, 9.2, 9.3.

*For more details on the features and functionalities, please refer to the online help or manuals.*

# System Requirements

**System Requirements for EPP Clients**

For Installing Seqrite Endpoint Protection 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, M3 chip compatible

macOS

- macOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13 and 14

**Linux 32-bit**

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

**Supported Distributions for EPP 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 EPP client:**

- Fedora 30, 32, 35
- Linux Mint 19.3, 20, 21.3
- 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, 8.8 Enterprise, 9.0, 9.1, 9.2, 9.3
- SUSE Linux 12. SP4 / Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0 (Desktop), 8.0 (Server)
- Oracle Linux 7.1, 7.9 and 8.1

**Note**: Linux Client Agent (v10.11) and above supports deployments only on Linux 64-bit OSs. The existing deployed agents on Linux 32-bit (v10.9) will continue to function as expected.

**System requirements for configuring Encryption policy**

**Client Pre-requisites:**

- Client version: 10.11 and above.
- License Edition: Premium

**Hardware**:

- TPM 2.0
- BIOS with UEFI mode

**OS:**

- Windows 10 64-bit
- Windows 11

**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, M3 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

## Bug Fixes

The following is a list of bugs that are fixed in the EPP Cloud 5.0 release:

| **Server** | |
|---|---|
| 1 | Updated device control configuration to ensure that "Vendor ID" and "Product ID" fields correctly accept hexadecimal values. |
| 2 | Resolved issue causing delays in the reflection of patch scan reports on the EPS Cloud. |
| 3 | Resolved error occurring during the export of the client status page. |
| 4 | Corrected export details in the SIEM server to display event descriptions instead of event identifier. |
| 5 | Resolved issue in where the virus report graph displayed as blank despite reports being generated. |
| 6 | Fixed issue where the client status export report was showing "No records found”. |
| **Client** | |
| **Windows/Mac/Linux** | |
| 1 | Fixed issue preventing website browsing and the appearance of an exclamation mark on the network icon for Linux systems caused by the qhwebsec service - EPS Cloud. |
| 2 | Addressed BSOD issue on Windows 11 machines related to catflt.sys when using IntelliJ software - EPS Cloud 4.0. |
| 3 | Corrected Seqrite folder space consumption issue caused by tmp files created by DLP - EPS 7.60 |
| 4 | Fixed the issue where Application Control Scan would exit without performing the scan |
| 5 | Resolved problem with the schedule scan time not displaying correctly on the dashboard portal |
| 6 | Fixed the issue with asset details not displaying for recently installed Linux clients - UEM 10.8 |
| 7 | Corrected the patch installation failure issue on client systems - EPS 8.2 |
| 8 | Fixed the problem with the "Seqrite Endpoint Security Helper service WSC" being in a stopped state due to the scanopt.dll binary - EPS NG 8.2 |
| 9 | Resolved the problem of last schedule scan time status not reflecting correctly on the EPS NG console page under the status tab - EPS NG 8.2 |

| | |
|---|---|
| 10 | Corrected issue where tuneup reports were not appearing on the console under the Reports section due to pcuner failing to write files in the configuration - EPS 8.2 |
| 11 | Fixed problem with DLP blocking Excel, CSV, and PDF attachments in Outlook mail as confidential data, even when the extensions are not enabled |
| 12 | Addressed patch download failure on the Patch server with error [INTERNAL FAILURE] - EPS 7.60 |
| 13 | Fixed issue with Seqrite Encryption service terminating after applying encryption policy - EPS NG 8.2.1 |
| 14 | Addressed problem with drive encryption failing and generating "system not supported" reports - EPS NG 8.2.1 |
| 15 | Resolved issue with the last schedule client scan date not updating on the UEM 4.0 dashboard |
| 16 | Fixed the issue of clients not appearing under the Clients-> Assets tab - EPS 7.60 |
| 17 | Solved a problem where internet access would stop functioning when Browsing & Phishing protection was enabled. |
| 18 | Fixed an issue preventing users from opening the macOS Client Dashboard on macOS Ventura with ARM64 architecture. |
| 19 | The Sonoma Performance Issue when using certain applications on macOS Sonoma has been resolved. |

# Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPP 4.0 client.
2. To install EPP 4.0 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: KB4474419 and KB4490628
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. The Antimalware scan report contains an old brand name 'Endpoint Security'.
9. 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.