Seqrite

Endpoint Protection Cloud

SEQRITE

Release Notes

Cloud 5.2.1 February 1, 2025

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	February 1, 2025	Seqrite Endpoint Protection Cloud 5.2.1 Released

What’s New

With this release, the following features are added to EPP Cloud 5.2.1.

Server-Side: Feature Highlights

New Feature: Endpoint Action Log Page

The **Endpoint Action Log** page has been added under Admin Settings, allowing users to view action logs for all endpoints. Previously, logs could only be viewed for a single endpoint at a time, but now users can view logs for multiple endpoints. The page includes search and filter options, allowing administrators to filter by **Endpoint Name**, **Initiated By**, **Action Type**, **Action Status**, and **Time Range** (Last 7 Days, Last 15 Days, Custom Range). Additionally, users can **export** the logs to CSV for further analysis.

Introducing the Reapply Policy Client Action

A new client action, **Reapply Policy** has been introduced. It can be accessed from the **status page > client action** dropdown. This action allows you to reapply a policy to selected endpoints with a Pending or Failed policy state. It does not affect endpoints where the policy is already applied.

New Column: Serial Number on Status Page

A new **Serial Number** column has been added to the Status page. This column displays the serial number associated with and retrieved from each endpoint. The serial number can be used in both search and export functions. This Serial Number will start appearing as soon as the planned Service Pack (planned in a phased manner*)* is applied to the client machine

New Column: Policy Saved Time

A new column, **Policy Saved Time**, has been added on the Policies page, showing the date and time when the policy was saved by the user.

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

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, 14, and 15

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, 24.04 LTS
- 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 5.2.1 release:

Server	
1	Fixed an issue where moving an endpoint with a custom policy applied caused the custom policy to be erroneously applied to all endpoints within the target group, affecting web category-based access rules. The issue has been resolved, and policies are now correctly applied to individual endpoints without impacting the target group.
2	Resolved an issue preventing users from viewing DLP reports for dates prior to December 31, 2024, in the Reports section.
3	Resolved an issue where clients running version 10.12 could not be sorted on the status page.

Known Issues

The following are known issues identified in the EPP Cloud 5.2.1 release:

- When making changes under all subcategories within the Web Security policy and saving them, the Policy Diff activity logs show an incorrect path for all sub features.
- When modifying the "Exception", "Detect Port Scanning Attack", or "Detect DDoS Attack" configurations within the IDS/IPS policy, the specific field names for the modified values do not appear in the Policy Diff activity logs.
- When IDS is disabled, Port Scan and DDOS may remain enabled on the client, potentially causing the client to go offline due to these attacks.

  Workaround: Enable IDS, disable Port Scan and DDOS, then disable IDS again and save the policy.

Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPP 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.

   Note: Browser sandbox functionality is not supported on Microsoft Edge.
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 [7.6/7.4/7.2 to cloud] option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is displayed.