Seqrite
Endpoint Protection Cloud

Release Notes

Cloud 5.2 | 4 Jan 2025

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Protection 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	4 January 2025	Seqrite Endpoint Protection Cloud 5.2 Released

What's New

With this release, the following features are added to EPP Cloud 5.2.

Server-Side: Feature Highlights

New DLP-Watermarking Feature for Enhanced Document Security

A new DLP watermarking feature has been introduced to enhance document security under DLP policies. This feature can be accessed through Policies > Edit > Policy Settings > Data Loss Prevention.

Supported File Types: .docx, .xlsx, and .pptx
Supported Operating Systems: Windows 10, Windows 11, Windows Server 2016, 2019, and 2022.

Pre-Requirements for Watermarking Feature:

- The DLP-Watermarking feature needs to be enabled through Support, as it is an add-on feature.
- To enable and utilize the new Watermarking feature under DLP policies, clients must have the latest VDB update following the 5.2 release.

Monthly Report Configuration Changes

The default monthly reports will no longer be sent automatically. Users can now enable and configure monthly reports from the **Scheduled Report Settings** tab, located under **Admin > Settings**. Additionally, users can add up to 5 valid email addresses to receive a consolidated monthly report.

Policy Change Details in Activity Log

This feature offers greater visibility and traceability of user actions, ensuring comprehensive auditability for all policy-related changes.
The **Admin > Activity Logs** now provide detailed tracking of all policy changes made by users. Key information captured includes the Timestamp, Username, Policy Name, the Before & After state of policy settings, and the Action Type (Add, Delete, Modify).

Endpoint Inactivity Management

A new **90 days** option has been added to the "Remove a client if inactive" dropdown under Admin > Settings. With this setting, endpoints inactive for 90 days will be automatically removed from the system. The previously available options were 15, 30, 60 days, and Never.

Policy Status Enhancements with New Failed at Endpoint Filter

A new Status filter, labeled **Failed at Endpoint**, has been added under the Policy Status on Endpoints. When the admin selects this filter, four sub-filters appear under the search field: Applied, Pending, AV not installed, and Failed at Endpoint.

Client-Side: Feature Highlights

Linux

- #### Linux Build Refresh

  The Linux build has been refreshed to ensure up-to-date performance and stability.

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 release:

Server	
1	The issue where the policy status for a newly registered client was incorrectly set to "Pending" instead of "AV Not Present" has been fixed. Now, the policy status is correctly marked as "AV Not Present" when a new client is registered at the server end.

Known Issues

The following are known issues identified in the EPP Cloud 5.2 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.