Seqrite
Endpoint Protection Cloud

External Release Notes

Cloud 6.0 | May 2025

www.seqrite.com

Copyright Information

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

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	09 May 2025	Seqrite Endpoint Protection Cloud 6.0 Released

What's New

With this release, the following features are added to EPP Cloud 6.0:

Server-Side: Feature Highlights

Endpoint Status Fields Updated

Enhanced the Endpoint Status screen to display detailed policy information, including:
- Group Container Policy (Single)
- Group Feature Policy (Multiple)
- Endpoint Feature Policy (Multiple)
- Last Policy Published Time
- Last Policy Applied Time

Users can view these details by navigating to **Dashboard > Status > Click the Endpoint Name > Endpoint Status**.

New UX Loader integration in EPP Cloud

Integrated the new UX-designed loader across all Seqrite products, providing a more consistent and visually enhanced user experience during loading states.

One tab for all actions

Consolidated all endpoint action logs under a single tab titled *Endpoint Action Logs* for improved accessibility, streamlined navigation, and better log management.

For N-1 versions, Minor Upgrade should be triggered from Console if Upgrade Client action is triggered

New Functionality:

- **Client Version Check for Upgrades:** When the upgrade client action is triggered from the front end, the client version will be considered before deciding on a Major or Minor upgrade.
- **Minor Upgrade Trigger:** If the client version is N-1 (where N is the latest version), a minor upgrade will be triggered.
- Added UI-level validation for the *Upgrade Client* action to restrict selection to a single major version at a time (e.g., 10.12.x.x or 10.11.x.x).

- **Error Handling for Multiple Major Versions:** If multiple major versions (e.g., 10.12.x.x, 10.11.x.x) are selected for the Upgrade Client Action, an error will pop up in the UI, instructing users to select only same version with same platform (Win/Mac/Linux) at a time for Upgrade Client actions. This validation will occur on the front end, not the back end.

Addition of Policy Status Column on Status page and Export of Policy Status

- **Default Column View:** The policy status column will be disabled by default, similar to the serial number column.
- **Search Functionality:** Users will be able to search using the policy status in the client status page.
- **Export Inclusion:** Policy status will be included in exports.
- **Policy Insight Page:** No changes; it will remain as it was in the February release.
- **Column Sorting:** Policy status column sorting will be available in this release.
- **Column Position:** The policy status column will be positioned after the policy column.
- **Policy Type Display:** Only container policy statuses will be displayed, not custom policies.
- **Applicability:** This feature applies to the client status report, not the comprehensive report.

UI Update for "SOHO Total" Edition in EPP Cloud

Introduced the new *SOHO Total* edition for EPP On-Prem (v7.60) and EPP Cloud. The product UI has been updated to correctly display the *SOHO Total* edition name for new customer purchases, ensuring clear visibility and accurate selection during setup and management.

Virtual Patching feature in Seqrite EPP

Added *Virtual Patching* feature in Seqrite EPP to provide timely protection against emerging threats without requiring immediate patch deployment. This enhances security and operational efficiency, and also helps meet compliance requirements often specified in tenders.

[Linux] Asset Management - Optimizing the Asset Discovery

Improved asset scan reporting for Linux clients by ensuring only third-party applications are sent to the EPP Server, significantly reducing inflated software counts. Also resolved an issue causing duplicate asset entries in EPP Cloud due to version mismatch logic, and fixed a problem where upgrading Linux clients resulted in duplicate asset records

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, M4 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 6.0 release:

Server	
Sr. No.	**Summary**
1	This issue is fixed where the users were not able to sort the endpoint names alphabetical and the IP Addresses in numerical order.
2	A bug fix is performed where the users were unable to delete exported child groups (from on-prem) to cloud when parent group is same as in exported.zip. A workaround is provided.
3	This bug is fixed where the users were unable to export the comprehensive data of the Endpoints displayed.
4	When getting email notification about DLP, the value displays null instead of the keyword.

Known Issues

The following are known issues identified in the EPP Cloud 6-0 release:

- When making changes under all subcategories within the Web Security policy and saving them, the Policy Diff activity logs might 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 may 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.
- One Logger is not getting printed for the current version/latest, If minor is triggered on console.
- Detonation reports for files submitted to sandboxing are currently not being received.

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.

   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 option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is displayed.