Seqrite
Endpoint Protection Cloud

External Release

Cloud 6.3 | Nov 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 the 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

1. What's New 3
    - Full System Asset Scan 3
    - Daily Asset Scan 3
    - Data Loss Prevention (DLP) 3
    - Data-At-Rest (DAR) Scanner integration with Data Loss Prevention (DLP) Policy 4
    - Schedule Daily Reports 4
    - Group Actions from the Status Tab 5
    - Export option for Notifications 5
    - Virtual Patch 5
    - Upgrade Control Settings 5
    - Display Endpoint Action Log on Endpoint Details page 5
    - Centralized Quarantine Management 6
    - QUIC Support for Safari Browser 6
    - Linux Support for USB Serial Number 6
    - Third-Party AV Detection Insight 6
    - Updated list for Third-Party Antivirus Detection 6
2. System Requirements 7
3. Usage Information 9

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	15 Nov 2025	Seqrite Endpoint Protection Cloud 6.3 Released

What’s New

With this release, the following features are added to EPP Cloud 6.3:

Full System Asset Scan

Added new client action to initiate a full system asset scan for selected managed endpoints. This will help the admins get the complete endpoint/asset details on demand.

Daily Asset Scan

Admin can set the Asset scan frequency as daily, too. To keep the Asset inventory up to date

Data Loss Prevention (DLP)

1. Watermarking via Right-Click

Users can now manually apply watermarks to files using the “Seqrite Watermark” option available in the Windows Explorer right-click menu. This provides flexibility to print files with watermarking as needed.

2. Channel-Level Control for DLP Actions

DLP actions can now be configured at the channel level (USB, Network Share, Print). If the channel action is set to "Block", it overrides data-level settings. Watermarking can be applied based on configuration: disabled, all supported documents, or confidential documents only. For print, only activity reporting and watermarking are supported.

3. Watermarking on Printed Documents

DLP now supports watermarking of documents during printing. If a document is already watermarked by the Seqrite Watermark feature from another system, printing will be blocked unless it is re-watermarked via the right-click print option. A toggle is available under the watermark column to enable or disable this feature.

4. Watermarking on File Transfers to USB and Network Share

Office and PDF files copied to USB, removable media, or network shares can now be watermarked even if they are not marked as confidential. Watermarking behavior is configurable.

5. Extended Domain Exception Limit

The limit for domain exceptions in DLP policies has been increased, allowing administrators to configure more trusted domains.

6. Extended Support on PDF Document Scan

Support for PDF document scan has been added with the existing Word, Excel, and PowerPoint formats.

7. DLP Control based on data occurrence

Admin can now set DLP control for blocking based on data occurrence, configured under **"Threshold Breach Count"**. For report-only cases, it will scan for all the occurrences present in the file based on configured classifiers and UDD.

8. The support for the following new applications is added in the Data Transfer Channels > Application list.

- Browser- Tor Browser, Brave
- Email - Photon Mail, Mail Spring
- Instant Messaging- Telegram, Discord, SignalZoom Webex
- File Sharing / Cloud Services- Sync.com, Mega.nz, Egnyte, Resilio Sync
- Social Media / Others- Trello

Note: All the new DLP features are applicable for Windows, except the Extended Domain Exception Limit.

Data-At-Rest (DAR) Scanner integration with Data Loss Prevention (DLP) Policy

Data-At-Rest helps the admins to discover all the data from the endpoints associated with a set Data types, Classifiers, and User Defined Dictionary (UDD).

- **Policy alignment**: The Data-At-Rest (DAR) scanner (on-demand and scheduled) now uses the same Data Loss Prevention (DLP) policy settings that are already configured.
- **Confidential data and User Defined Dictionary (UDD) discovery**: Data-At-Rest (DAR) scans apply the Confidential Data rules defined in the Data Loss Prevention (DLP) policy. User-defined dictionaries from the DLP policy are also applied during DAR scans.

Note: This feature will be applicable for client above 10.13.1.0

Schedule Daily Reports

Admins can schedule daily reports on specified email IDs to get the previous day's security.

Group Actions from the Status Tab

Administrators can now perform actions on selected groups that will be applicable to all the associated endpoints, streamlining management tasks that previously required individual client actions.
From the Group Action dropdown, you can initiate:

- **Scan** – Scan on all selected endpoints.
- **Update** – Apply updates across all endpoints.
- **Upgrade Client** – Upgrade the client software on all endpoints.

Export option for Notifications

Users can now view and download client antivirus (AV) status notifications directly in CSV format from the cloud portal.

Virtual Patch

The EPP Console provides proactive protection by shielding endpoints from known and emerging vulnerabilities without requiring immediate OS or application updates. It provides Detailed **CVE information** (CVE-ID, name/title, description) for each signature. Also, granular control allows administrators to enable or disable individual signatures directly from the console based on CVE IDs.

Upgrade Control Settings

The users can now enable automatic upgrades to keep endpoints current without manual intervention. Unsupported (EOL) agent versions will be upgraded during regular cycles, which may require a system restart. In addition, the users can opt in to automatic features and minor upgrades so endpoints always receive the latest enhancements and service packs.

For EOL details, you can refer- https://www.seqrite.com/end-of-product-life-announcements-information/

Display Endpoint Action Log on Endpoint Details page

A new **Action Logs** tab has been added to the Endpoint detail view. This tab displays the action logs of the selected endpoint in a table format, providing clear visibility into activity history.

- **Export support**: Users can export action log records for reporting or analysis.
- **Filtering options**: Action logs can be filtered by **Initiated By**, **Action Type**, **Action Status**,

This enhancement improves traceability and makes it easier for admins to review and manage endpoint actions.

Centralized Quarantine Management

Administrators can now manage quarantined files centrally through the **EPP Console**, improving visibility and control across all connected endpoints. The supported admin actions are: Pull from Agent, Send to Seqrite Lab, Send to Sandbox, Restore, and Delete

QUIC Support for Safari Browser

On macOS, only the Safari browser supports web security features for websites using the QUIC protocol.

Linux Support for USB Serial Number

Device Control now supports 120-character USB Serial Numbers on Linux systems.

Third-Party AV Detection Insight

Third-party AV name is now visible even after its removal in Notification, and can be exported too.

Updated list for Third-Party Antivirus Detection

The following new third-party antivirus detections are added while installing Windows Client AV.

- Sunrise Total Security 7.x
- Secura Web Total Security 3.x
- ESET Endpoint Security 12.x
- KV Antivirus 13.x
- Actipace Total Security 1.x
- Comodo Internet Security Premium 11.x
- Comodo Internet Security Premium 12.x
- SiyanoAV Total Security 1.x
- SiyanoAV Internet Security 1.x
- SiyanoAV Antivirus 1.x
- CrowdStrike Falcon 7.
- McAfee Security Scan Plus 3.x, 4.x
- AhnLab V3 Internet Security 8.x
- VMware Carbon Black EDR Sensor 7.x
- HP Wolf Security 11.x
- Sophos Endpoint Agent 2023.2.x
- ESET Endpoint Security 11.
- Trellix Agent 5.x
- Trellix Endpoint Security 10.x

- Microsoft Defender ATP 10
- Avast! Free Antivirus 25

System Requirements

System Requirements for EPP Clients

For installing the Seqrite Endpoint Protection client through the client install utility, the System requirements are as follows:

Any one of the following operating systems:

Windows OS

- Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Pro / Enterprise (32-bit/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 2008 Server R2 Web / Standard / Enterprise / Datacentre (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 R2 Standard / Datacentre (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacentre (64-bit)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2022 Standard / Datacentre / Essentials
- Microsoft Windows Server 2025 Standard / Datacentre / Essential

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, 15, and 26

Linux

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

Note: Supported only till Linux agent version 10.9.

Linux 64-bit

- GNU C Library 2.5 and later
- SAMBA version 4.22 and earlier

Supported Distributions for EPP client:

- Fedora 30,32,35,37, 38, 39,40, 41, 42
- 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, 9.3,9.4 and 9.5
- SUSE Linux 12. SP4 / Enterprise Desktop 15
- Rocky Linux 8.4, 9.3, 9.4, 9.5
- Boss 6.0, 8.0, 9.0 (Desktop), 8.0 (Server)
- Oracle Linux 7.1, 7.9, and 8.1

Note: The Linux agent version 10.11 and onwards, only 64-bit Linux systems are supported.

Usage Information

1. For Windows 2016, Windows 2019 Server, Windows 2022 Server, and Windows 2025 Server, uninstall Windows Defender before installing the EPP client.
2. To install the EPP 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 a Windows 7 32-bit client, you must upgrade to Internet Explorer version 11.
4. If the administrator initiates a tune-up notification for the endpoint and if the endpoint is not logged in, then the tune-up 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, the 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. The Watermark feature is only compatible with Microsoft Office versions 2016, 2019, and 2022, and is not supported by WPS Office, LibreOffice, Office 365, or OpenOffice.
10. Linux
    - The Remote Support tool cannot be executed with the ‘sudo’ command. The tool can be executed with the superuser (su) command.
    - On selecting the migration option for a group with one Linux and another Windows client machine, a warning message **Linux client migration is not supported** is displayed.