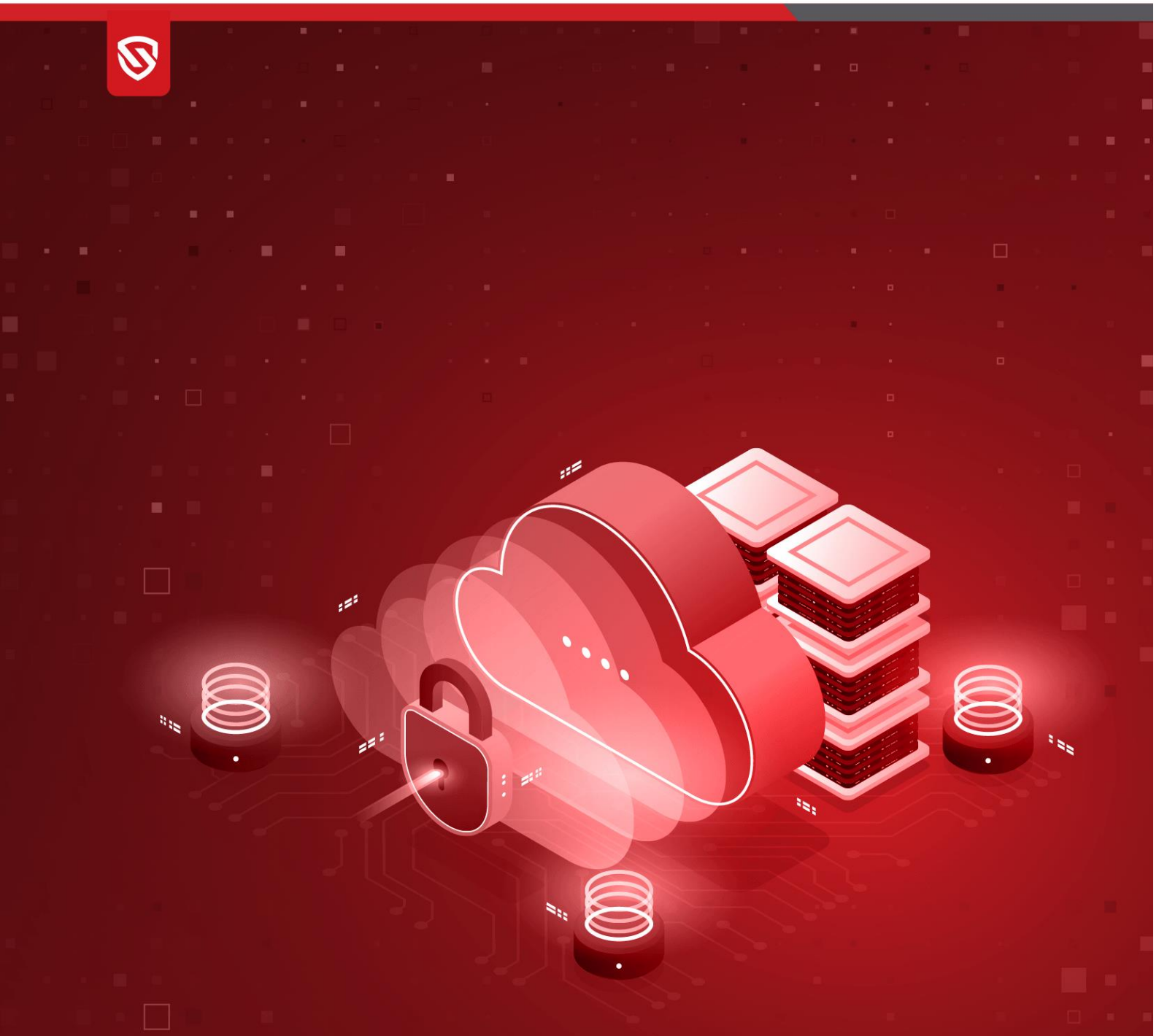
Seqrite
Endpoint Protection Cloud

SEQRITE



Release Notes

Cloud 6.5 | Jun 2026

www.seqrite.com

Copyright Information

Trademarks

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

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	26 Jun 2026	Seqrite Endpoint Protection Cloud 6.5 Released

What's New in EPP 6.5

With this release, EPP Cloud 6.5 introduces the following enhancements:

Unified Deployment Support for Seqrite EPP

Seqrite EPP is now integrated into the SUA deployment Setup, allowing administrators to deploy EPP alongside ZTNA, Data Privacy, and XDR using a single installer. This enhancement simplifies deployment by consolidating installation workflows into a unified experience across Seqrite security products.

Key Benefits

- Deploy multiple Seqrite security solutions through a single installation package.
- Eliminate the need to manage separate installers and deployment processes.
- Minimize the risk of configuration mismatches across products.
- Streamline setup and accelerate deployment across environments.
- Establish a scalable foundation for integrating additional products into the unified deployment framework.

Changes to Deployment Management

- As part of this enhancement, deployment management has been centralized within the CSM Console:
- Deployment methods are no longer available in the EPP Console.
- All deployment-related activities can now be accessed from the **Deployment** tab in the **CSM Console**.
- In the EPP Console, only the **Online Installer** tab remains available in **read-only mode**.
- Administrators can continue to create installers from the EPP Console; however, the generated installers must be downloaded from the CSM Console.

Browser Security Controls

Introduced Browser Controls section in Web Security Policy to centrally configure and manage browser security settings from the EPP console.

- Added controls to enable or disable browser extension installation, Incognito/Private Browsing mode, and Developer Tools.
- Ensured backward compatibility by disabling newly introduced browser control settings by default in existing policies.
- Enabled newly introduced browser control settings by default in newly created policies.

- Enhanced Activity Logs to record browser security policy changes, including the administrator who made the change, modified settings, and the corresponding timestamp for audit and compliance purposes.

Group-Based Notifications

Introduced group-based endpoint event notifications for Group Administrators and HODs.

- Enabled notifications to be sent only for events associated with users in the administrator's assigned groups.
- Added support for notifying multiple administrators assigned to the same group.
- Enhanced operational visibility and compliance monitoring through targeted event notifications.

Client Support for Linux 32 Deprecated

Starting with Endpoint Protection version 6.5, the Linux 32-bit Client build has been deprecated and is no longer available

Enhanced Web Security capabilities across Windows, Mac and Linux

This release expands Web Security with new access control capabilities and support for modern web protocols across supported platforms.

- **Microsoft Access Controller (Windows):** Introduced Microsoft Access Controller (MAC) for Windows endpoints, allowing administrators to restrict access to Microsoft services by configuring approved organizational login URLs and allowed domains. The feature can be enabled or disabled through policy, ensuring users access organizational resources only through authorized accounts. It also includes event logging for monitoring and auditing access activities.
- **QUIC and TLS 1.3 support (Mac & Linux):** Added support for the QUIC and TLS 1.3 protocols in Google Chrome and Microsoft Edge browsers, improving compatibility with modern web applications.
- **Google and YouTube Access Controller (Mac & Linux):** Added support for Google Access Controller and YouTube Access Controller in Google Chrome and Microsoft Edge, enabling administrators to enforce organizational access policies for Google services and YouTube.

Expanded Linux OS support

Seqrite Linux Client now supports the following additional operating system versions:

- Debian: Versions 12 and 13
- Rocky Linux: Versions 8.10, 9.6, and 10

Enforced Secure Communication (HTTPS Only) across all Seqrite EPP Components

All communication between Seqrite Endpoint Protection Platform (EPP) components and Seqrite/Quick Heal cloud infrastructure and content delivery network (CDN) now uses secure HTTPS/TLS protocols, ensuring encrypted and secure data transmission across all supported operating systems.

Data Loss Prevention (DLP) Enhancements

Improved DLP event logging:
DLP events now capture and display the original source file path when files are copied or moved from:

- A local system to a network location
- A local system to supported removable storage devices, including:
    - USB pen drives
    - USB hard drives
    - USB DVD/flash drives

Performance improvement for DLP scanning:
To improve scanning performance, DLP will now scan only files up to **30 MB by default**. Files larger than 30 MB will be excluded from DLP scanning. Users can configure the scan limit up to 60MB.

No DLP scanning for incoming files:
Files received from external sources (such as network locations or removable devices) will no longer be scanned by DLP when they are copied to the local system. This reduces unnecessary scanning and improves overall system performance.

Enhanced Endpoint Logging in Patch Management

To make troubleshooting and root cause analysis easier, Patch Management now includes improved endpoint logging.

- Added new Patch Management logs to the log collection process.
- Implemented log size limits to prevent excessive log growth.
- Enhanced logging to provide more comprehensive information while making logs easier to collect for diagnostics.

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 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, 12, 13
- 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, 8.10, 9.3, 9.4, 9.5, 9.6, 10
- 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.

Known Issues

- When users right-click a PDF file on an endpoint, the alert **“File is being watermarked”** is displayed, even if PDF file types are not selected for watermarking in the DLP policy.
- Files are still traced by DLP when copied to network share locations that are configured as exceptions.
- The DLP **Match Count** feature does not detect confidential data located in document headers or footers.
- Watermarking features are not supported on Microsoft Publisher or MS Access.
- When a user tries to open and print Microsoft Publisher with a ‘Save as PDF’ option, the saved PDF does not display the watermark.
- Watermark doesn’t get applied for some of the specific printer layout options such as Mirrored, 2Pages or 16PerPage print.
- File classification dropdown does not appear in the right-click menu when DLP is enabled for the first time via policy. If re-save and reapply the same DLP policy. The file classification option then appears in the right-click menu.
- Watermark is not applied when a confidential file is embedded into a non-confidential parent Office document (e.g., Word) using Insert → Object → Create from File, even though the DLP policy is set to “Report only” for confidential files and watermarking is enabled.
- Watermarks are not applied when documents are printed using Command Prompt or PowerShell.
- Printed documents show watermarks in a diagonal orientation, even when set to Horizontal under DLP > Watermark > Orientation
- During Asset scheduled scans on Windows, the size of installed applications is not captured.
- Bluetooth blocking functionality does not work on macOS Tahoe 26, even though the " Device Control Blocked prompt appears.
- The USB device added to the exception list by serial number using ‘USB Devices’ by dcconfig tool will not work on macOS. As an alternative, users can add the USB device using 'USB by Serial Number' under the Device Control Configuration settings to make the exception work on macOS.

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.