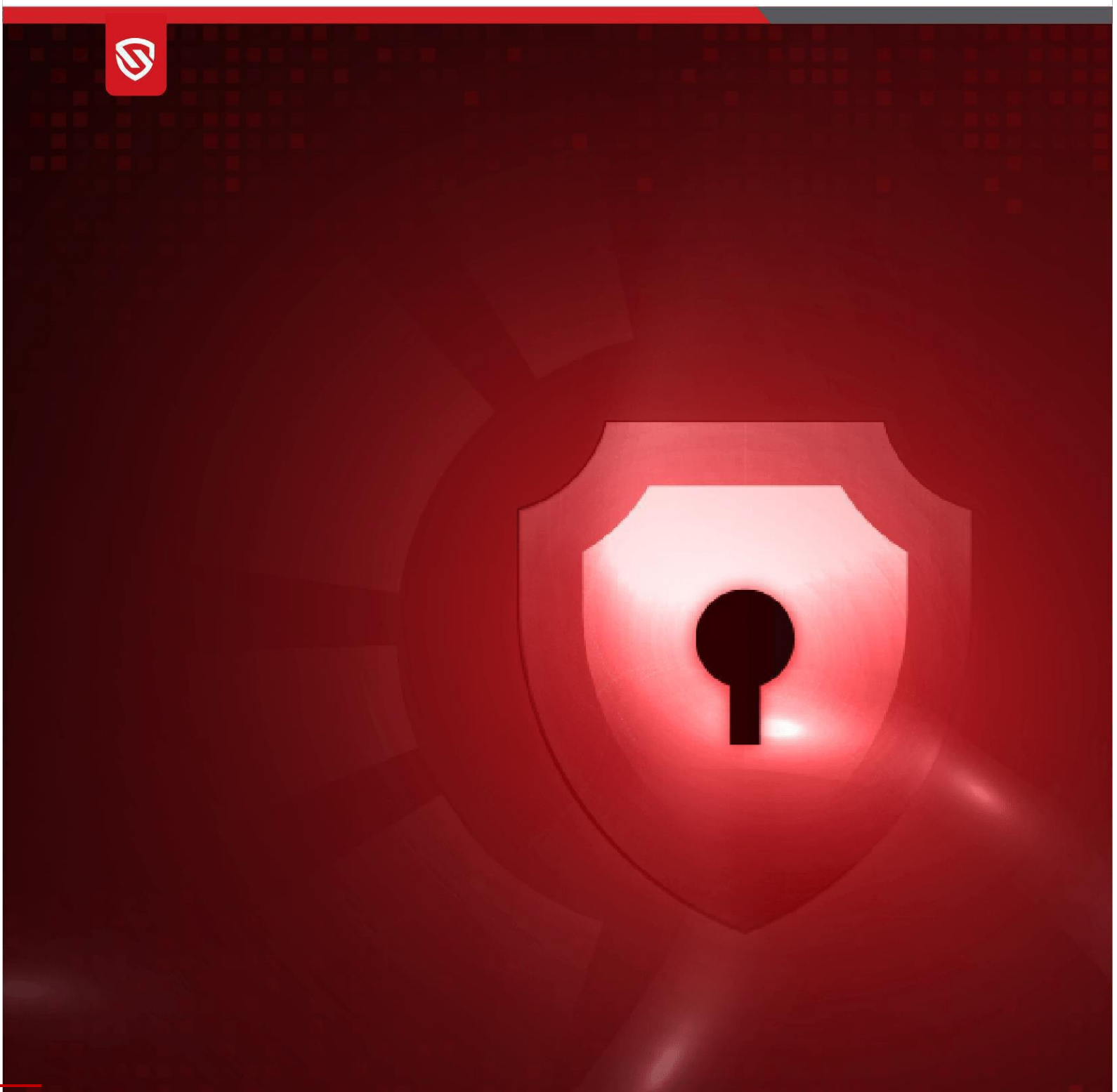
Seqrite

Endpoint Protection



Release Notes

EPP 8.4

19 Sep 2025

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

Doc Version	Date	Comment
1.0	19 September 2025	Seqrite Endpoint Protection 8.4 Released

Features and Enhancements

Data Loss Prevention (DLP) Enhancements

1. Watermarking via Right-Click [Windows]
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 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. Monitoring and Watermarking for CD/DVD Burning [Windows]
DLP now monitors and watermarks files burned using Windows native CD/DVD burning. The solution tracks file operations in the burn staging folder using FAM. This feature requires FAM to be enabled and supports Windows 10 and above (desktop) and Windows Server 2016 and above.

5. 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. DLP incidents will not be generated for non-confidential files, but such activities can be tracked via FAM reports.

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

7. Support for PDF Document Scan
Support for PDF document scan has been added with the existing Word, Excel, and PPTx formats.

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

- 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

HA Configuration Support for Air-Gapped Networks

High Availability (HA) configuration is now supported in air-gapped environments, enabling resilient deployments without internet access.

Group-wise Client Actions from Status Tab

Client actions Scan and Update are now added along with the existing actions, such as Export, Patch Install, and Migration, on selected endpoint groups directly from the Status tab, maintaining the same action sequence.

Server Installer Support with Third-Party Separation

The server installer now supports deployment with third-party component separation, improving modularity and compliance. This is available for Site Server/Standalone (SSR) and Control Center.

Installer Support on Ubuntu 24.04.3

Site Server/Standalone (SSR) and Control Center installation is now supported on Ubuntu 24.04.3 with third-party separation, expanding compatibility with the latest Linux distributions.

Server Backup and Restore Qualification on Ubuntu 24.04.3

Backup and restore operations are now qualified on Ubuntu 24.04.3, ensuring data protection and recovery support on the latest OS version.

EPP Endpoint Color Theme and Icon Redesign

The color theme for the entire Seqrite Endpoint Protection (EPP) interface has been updated from green to blue.
Additionally, the **Seqrite system tray icon** has been redesigned. It now appears in **red**, accompanied by a **status dot** that can be green, orange, or red, indicating the current protection status:

- **Green**: Seqrite Endpoint Protection is configured with optimal settings, and your system is fully protected.
- **Orange**: One or more features require your attention. While not urgent, it is recommended to address them at the earliest.
- **Red**: Critical issues detected. Seqrite Endpoint Protection is not optimally configured, and immediate action is required to ensure your system remains protected.

The Seqrite EPP System tray icon is available under the Seqrite Universal Agent (SUA)

The EPP product, along with the quick access options, is available under the system tray icon when both Seqrite Endpoint Protection and Seqrite Universal Agent (SUA) version 1.3.9 or above are installed on the endpoint.

Action log notifications for allow/revoke 'Temporary Device Access' on EPP web console

Action log notifications will be generated on the EPP Web Console for Temporary Device access in the following events

- When OTP is generated
- When access is granted
- When access is revoked

Note: These notifications are displayed for Windows and Mac OS.

Enhanced Application List for Application Control Support

Application Control Support feature within Endpoint Protection Platform (EPP) now includes a refreshed list of supported applications.

Consent Based Upgrade and Reboot for Windows

Prerequisite: For client v10.11 to v10.13- For Consent based upgrade The VDB Date should be on or after 16th September 2025. If the date is older than this, then the upgrade will happen without consent.

Admins can now manage upgrade settings directly from the **Server Console** by navigating to **Admin Settings → Upgrade Control**. This feature lets you set how many days (choose from 0, 1, 3, 5, or 7) users can delay a system reboot during client upgrades.

- **If set to 0 days**, the upgrade will happen automatically without asking for user consent.

On the **client side**, a new **upgrade consent window** has been introduced. Users will see two options:

- **Upgrade Now**: Start the upgrade immediately.
- **Snooze**: Delay the upgrade until the maximum number of days set by the admin.

This gives users time to save their work and prepare for the restart, helping ensure a smooth and disruption-free experience.

Updated list for Third-Party Antivirus Detection

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

- Trend Micro Apex One Security Agent 14.0.12685 and later
- Trend Micro Apex One 14.x
- Trend Micro Deep Security Agent 8.x, 12.x
- Sentinel Agent 24.x
- McAfee 1.x
- McAfee WebAdvisor 4.x
- Sophos Endpoint Agent 2024.x
- Avast Business Security 24.x
- WithSecure Client Security 16.x
- WithSecure Client Security Premium 16.x
- WithSecure Server Security 16.x
- WithSecure Server Security Premium 16.x
- Kaspersky Embedded Systems Security 3.x
- Trellix Endpoint 23.x
- eScan Corporate Edition 14.x
- 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

Consolidated Policy Status Page

An enhancement has been introduced to improve the visibility and accessibility of policy details. When users click **'View Details'** for a policy, they are now redirected to the **Status** page, where all relevant information is presented on a single screen—eliminating the need for horizontal scrolling. Additionally, administrators can now **Export the status** directly from this page. Clicking on an **Endpoint name** within the status page also reveals the associated **Feature Policy status**.
This enhancement streamlines policy management and significantly improves the user experience for administrators.

Centralized Quarantine Management

Administrators can now centrally manage the quarantine process on endpoints through the EPS Console with enhanced control and visibility. Key features include:

Action Controls from Console:

Restore / Delete / Send to Seqrite Lab / Pull from Agent

- **Upload (On-Prem only)** with license-based feature flag; not applicable for Cloud deployments.
- **Quarantine Data Visibility:**
  Full details, including file hash, endpoint info, and quarantine metadata now visible on the server console, matching agent-side data.
- **Action Status Tracking:**
  Statuses include: Quarantined, Deleted, Restored, In Progress (Delete/Restore/Send to Lab), Sent to Lab, Upload in Progress, Downloaded.
- **File Upload & Download:**
  Roaming endpoints upload to cloud (3-day retention); EPP Server handles uploads via POST method.
  Admins can download password-protected files post successful upload.
- **Synchronization:**
  Actions performed via Agent UI are reflected on the Server Console and vice versa.
- **Selection Support:**
  Single Selection: Pull from Agent
  Multi-Selection: Restore, Delete, Send to Lab (skips records with Restored/Deleted/Sent status)
- **Retention & Reporting:**
  CQM report retention: 60 days for Restored/Deleted, 90 days for others.
- **Export options:** CSV/PDF; Scheduled reports via Admin Settings.
  Hash code copy & filter support.
- **Client Upgrade Handling:**
  Agent backs up and restores Quarantine DB during major upgrades.

QUIC Support for Safari Browser

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

Viewing SIEM Encryption Reports

The encryption key is sent in encrypted format; however, the users can view it in a well-structured format in the Reports section.

Collecting Logs from Endpoints via Console

This client action allows administrators to initiate a log collection process from the EPP Server Console. When this action is triggered, the client receives a request to gather all relevant logs. Once the logs are collected, they are sent back to the EPP Server Console for review and troubleshooting.

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

- **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.

- **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.

Update Agent Protection

The Update Agent is now tamper-proof, enhancing security and preventing unauthorized modifications.

Linux Support for USB Serial Number

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

EPP Status Page Enhancement

A new column has been added to display device serial numbers in the EPP status page.

Client-Side Visibility

Clients can now view Server details, Group, and Policy assignments directly on their systems.

Hostname Visibility on Mac & Linux

EPS Console now displays complete hostnames for Mac and Linux endpoints.

EPP Cloud Web Console Enhancements

BIOS Serial Number is now visible from client systems. Active MAC ID is now captured and displayed.

AV Build Version on Mac & Linux

The EPS Console now displays the AV build version for Mac and Linux endpoints.

Third-Party AV Detection Insight

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

Admin Control Over AV Uninstallation

Admins can now choose to skip the removal of detected third-party AVs via the Server UI.

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

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

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.

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.

Added 90 days for inactive endpoints removal and email notification

Remove endpoint if inactive for 90 days. Email notification for automatic remove of inactive client.

Enhanced Application Control Search

The Application Control Search feature now supports Hexadecimal input, enhancing precision and flexibility.

DLP License Assignment Mode

You can choose how DLP licenses are assigned to endpoints and manage automatic or manual allocation.
Manual: Manually assign DLP licenses to endpoints via client actions. Licenses are assigned through client actions. If you switch to Automatic mode and no licenses are available notifications will be displayed in the EPP Console for all new subsequent registrations until you revert to Manual mode.

Automatic: Licenses are assigned automatically when available. If no licenses are left, notifications will be shown. For new customer onboardings, if the DLP License Count matches the Total License Count, the Automatic mode is used. Otherwise, the Manual mode is applied.

System Requirements for Endpoint Protection Server

Prerequisites

It is recommended that all unattended update processes are in a completed state on the Ubuntu system before proceeding with the server installation process.

EPP Standalone Setup

A server that supports up to 1 to 2000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14(supported on server as well as desktop image)
- Available Disk Space: 150 GBs or above
- Available RAM: 8 GBs or above
- Processer: 4 Core (x86-64), 2.60GHz or above

A Server that supports up to 10000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 250 GB or above
- Available RAM: 16 GBs or above
- Processer: 8 Core (x86-64), 2.60GHz or above

A Server that supports up to 10001 to 15000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 350 GB or above
- Available RAM: 24 GB or above
- Processer: 12 Core(x86-64), 2.60GHz or above

A Server that supports up to 15001 to 20000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 450 GB or above
- Available RAM: 32 GB or above
- Processer: 16 Core(x86-64),2.60GHz or above

A Server that supports up to 20001 to 25000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 500 GB or above
- Available RAM: 48 GB or above
- Processer: 24 Core(x86-64),2.60GHz or above

EPP Distributed Setup

Distributed Server Architecture with 2 Node, each server with the following configuration:

A Server that supports up to 10000 to 15000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 250 GBs or above
- Available RAM: 16 GBs or above
- Processer: 8 Core (x86-64), 2.60GHz or above

A Server that supports up to 15001 to 20000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 350 GBs or above
- Available RAM: 16 GBs or above
- Processer: 12 Core(x86-64), 2.60GHz or above

A Server that supports up to 20001 to 25000 endpoints

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 350 GB or above
- Available RAM: 24 GB or above
- Processer: 12 Core(x86-64),2.60GHz or above

EPP Multisite Setup

Controller Server that supports up to 50 Site Server (SSR)

- Ubuntu 24.04.3 with signed Kernel Version 6.14 (supported on server as well as desktop image)
- Available Disk Space: 250 GB or above
- Available RAM: 16 GBs or above
- Processer: 8 Core (x86-64), 2.60GHz or above
  Note: Site Server Configuration will be similar to the Standalone recommendation.

System requirements for Seqrite Endpoint Protection clients

Windows

- 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
- Microsoft Windows Server 2025 Standard / Datacenter / Essentials

Note:

- EPP client cannot be installed on Windows 7 and Microsoft Windows Server 2008 R2 if these updates are not installed:
  - KB4474419
  - KB4490628
- Install them by clicking on the link OR
  Install Internet Explorer 11 to get the updates automatically. After installing the KB articles, you need to restart the system.
- For Windows 2016, Windows Server 2019, Windows Server 2022, and Windows Server 2025 you need to uninstall Windows Defender. Post the uninstallation, make sure that you restart the system.

Mac

- Processor: Intel core or Apple's M1, M2, M3, M4 chip compatible
- macOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13, 14, 15, and 26

Linux 32-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier
- Supported Distributions for the Seqrite Endpoint Protection 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 4.22 and earlier
- Supported Distributions for Seqrite Endpoint Protection 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
  - Debian 9, 10
  - CentOS 7.8, 8.2
  - RHEL 7.5, 7.8, 8.2 & 8.6 Enterprise, 9.0,9.1, 9.2, 9.3, 9.4, 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

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, M4 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

System Requirements for the Patch Management server

Operating System:

- Microsoft Windows 10 (64-bit) and above
- Microsoft Windows Server 2012 (64-bit) and above

Disk Space:

- Minimum: 40 GB
- Recommended: 1 TB

RAM:

- 8 GB or above

Processer:

- 4 Core(x86-64), 2.60GHz or above

Note:

- For more than 25 clients, Seqrite recommends installing Patch Management server on the Windows Server operating system.

Known Issues

- Watermarking feature is not working as expected on Microsoft Office Offline Installer, Microsoft Access, Microsoft Publisher, Polaris Office Suite, Chromium-based browsers. When a user tries to open and print Microsoft Publisher with a '**Save as PDF**' option, the saved PDF does not display the watermark.
- The print watermark may exceed the printable area.
- Watermark doesn't get applied for some of the specific printer layout options such as **Mirrored, 2Pages, or 16PerPrint.**
- File classification dropdown does not appear in the right-click menu when DLP is enabled for the first time via policy.
  Workaround: 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**.
- The right-click watermark feature does not function for files larger than 10 MB.
- **'Data Transfer Channels'** settings don't take precedence over **'data-settings'** for native CD/DVDs in the **'removable devices'** channel

  For example:
  If users select the '**With CD/DVD Player'** option in the **'Removable Devices'** channel and set it to **'Block & Report'**, but in the '**Data Type'** settings set **'Driving License'** to **'Report Only'** and **'Email'** to **'Block & Report'**, then the 'Data Type' settings will override the general device setting.
  This means:
  - **'Driving License'** data will only be reported (not blocked).
  - **'Email'** data will be blocked and reported.

  In summary, the specific '**Data Type'** settings take priority over the general device settings.
- **'Temporary Device Access'** may stop working after a system restart.
  Workaround: Reapply the policy from the console.
- Bluetooth blocking functionality does not work on macOS Tahoe 26, even though the " Device Control Blocked prompt appears.
- **Asset Management**: Sometimes Software Details may be incomplete when more than 100 applications are installed on the endpoint.

Usage Information

1. 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.
2. For Windows 2016, Windows 2019 Server, and Windows 2022 Server, uninstall Windows Defender before installing the EPP 8.4 client.
3. To install EPP 8.4 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: KB-4474419 and KB-4490628
4. To install patches on a Windows 7 32-bit client, you must upgrade to Internet Explorer version 11.
5. 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.
6. 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. To use Browser Sandbox, turn off the Secure Boot feature of the system from BIOS Configuration.
7. By default, Spam Protection is disabled. So, a red exclamation mark appears on the client Dashboard.
8. Linux
   - The Remote Support tool cannot be executed with the 'sudo' command. The tool can be executed with the super user (su) command.
   - On selecting the migration option for a group with one Linux and another Windows client machine, warning message **Linux client migration is not supported** is displayed.