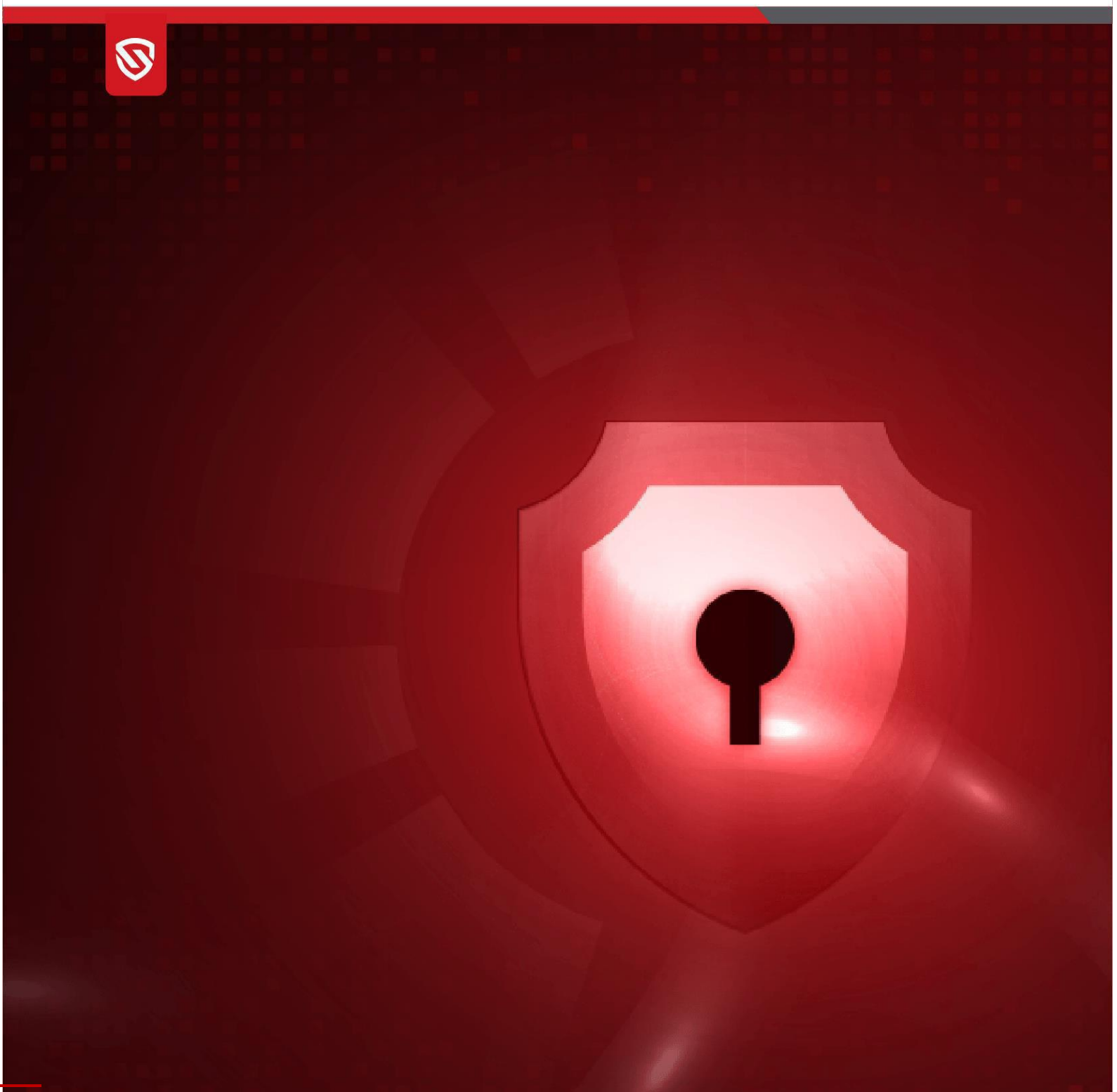
Seqrite

Endpoint Protection



Release Notes

EPP 8.5

31 Mar 2026

www.seqrite.com

Copyright Information

Trademarks

License Terms

Contents

Revision History

Doc Version	Date	Comment
1.0	31 March 2026	Seqrite Endpoint Protection 8.5 Released

Overview

Seqrite Endpoint Protection Platform (EPP) version 8.5 introduces enhancements focused on deployment flexibility, usability, reporting, and centralized endpoint management. This release strengthens security operations across Windows, macOS, and Linux environments.

Features and Enhancements

Windows Installer

Seqrite Endpoint Protection Platform (EPP) introduces a new installer for Windows OS

Deployment and Installation

- Active Directory-based deployment using MSI packages for Windows endpoints.
- Proxy configuration support for Remote Installer and AD deployments.

Web and Network Security

Support for QUIC and TLS 1.3 protocols in Chrome and Edge browsers on macOS and Linux.

Data Loss Prevention Enhancements

- Enhanced source path detection for improved policy accuracy.
- Files larger than 30 MB excluded from report-only actions to improve performance.

Usability Enhancements

- Increased endpoint visibility with support for viewing 100 endpoints per page.
- Antivirus status notifications can be exported in CSV format.
- New Action Logs tab provides detailed endpoint action history with filtering and export options.
- Group-level actions for Scan, Update, and Client Upgrade directly from the status view.

Reporting and Maintenance

- Client module reports are downloadable locally in PDF and CSV formats without SMTP dependency.
- Scheduled daily security reports delivered via email.
- Group-wise Service Pack upgrades enable phased and controlled rollout.

Centralized Endpoint Management

- Centralized Quarantine Management with actions including restore, delete, and cloud analysis.
- On-demand full system asset scans for selected endpoints.

System Requirements for Endpoint Protection Server

EPP Standalone Setup

A server that supports up to 1 to 2000 endpoints

Operating System	Versions / Editions
Windows 11	Enterprise
Windows Server 2022	Standard / Essentials

- Available Disk Space: Minimum 150 GB or above
- Available RAM: Minimum 12 GBs or above
- Processer: Minimum 4 Cores (x86-64), 2.1GHz or above

More Information: For the latest and detailed system requirements, supported platforms, and configuration guidelines, refer to the **official Seqrite documentation** available at: https://docs.seqrite.com/docs/seqrite-endpoint-protection-8-5/system-requirements/server-requirements/

System requirements for Seqrite Endpoint Protection clients

Windows

- Windows 7 (32-bit / 64-bit)
- Windows 8.1 (32-bit / 64-bit)
- Windows 10 (32-bit / 64-bit, all editions)
- Windows 11 (all editions)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 / 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note: Windows Defender must be uninstalled on supported Windows Server operating systems before installing the EPP client.

Mac

- macOS versions 10.12 and later
- Supported on Intel- and Apple Silicon–based systems (M1 / M2 / M3 / newer)

Linux

- Fedora 30, 32, 35, 37, 38, 39, 40, 41, 42
- Linux Mint 19.3, 20, 21.3
- Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04
- Debian 9, 10
- CentOS 7.8, 8.2, 9
- RHEL 7.5, 7.8, 8.2, 8.6, 8.8 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, 8.8, 8.10, 9.6

Linux agent version 10.11 and above supports **64-bit systems only.**
More Information: For the latest and detailed system requirements, supported platforms, and configuration guidelines, refer to the **official Seqrite documentation** available at: https://docs.seqrite.com/docs/seqrite-endpoint-protection-8-5/system-requirements/client-requirements/

Important Usage Notes

- The **Watermark** feature is supported only on Microsoft Office 2016, 2019, and 2022. It is not supported on Office 365, WPS Office, LibreOffice, or OpenOffice.
- Legacy Windows systems (Windows 7 and Windows Server 2008 R2) require **SHA-2 compatibility updates** and a system restart before client installation.
- If a **tune-up notification** is triggered while the endpoint user is not logged in, the notification will fail.
- In **Advanced Device Control**, formatted authorized and encrypted devices are treated as unauthorized and must be re-added.
- To use **Browser Sandbox**, **Secure Boot must be disabled** in BIOS.
- **Spam Protection** is disabled by default and may show a warning indicator until enabled.
- On Linux endpoints: Remote Support must be executed using the su command; sudo is not supported.
- **Linux client migration is not supported** and will display a warning if attempted in mixed OS groups.