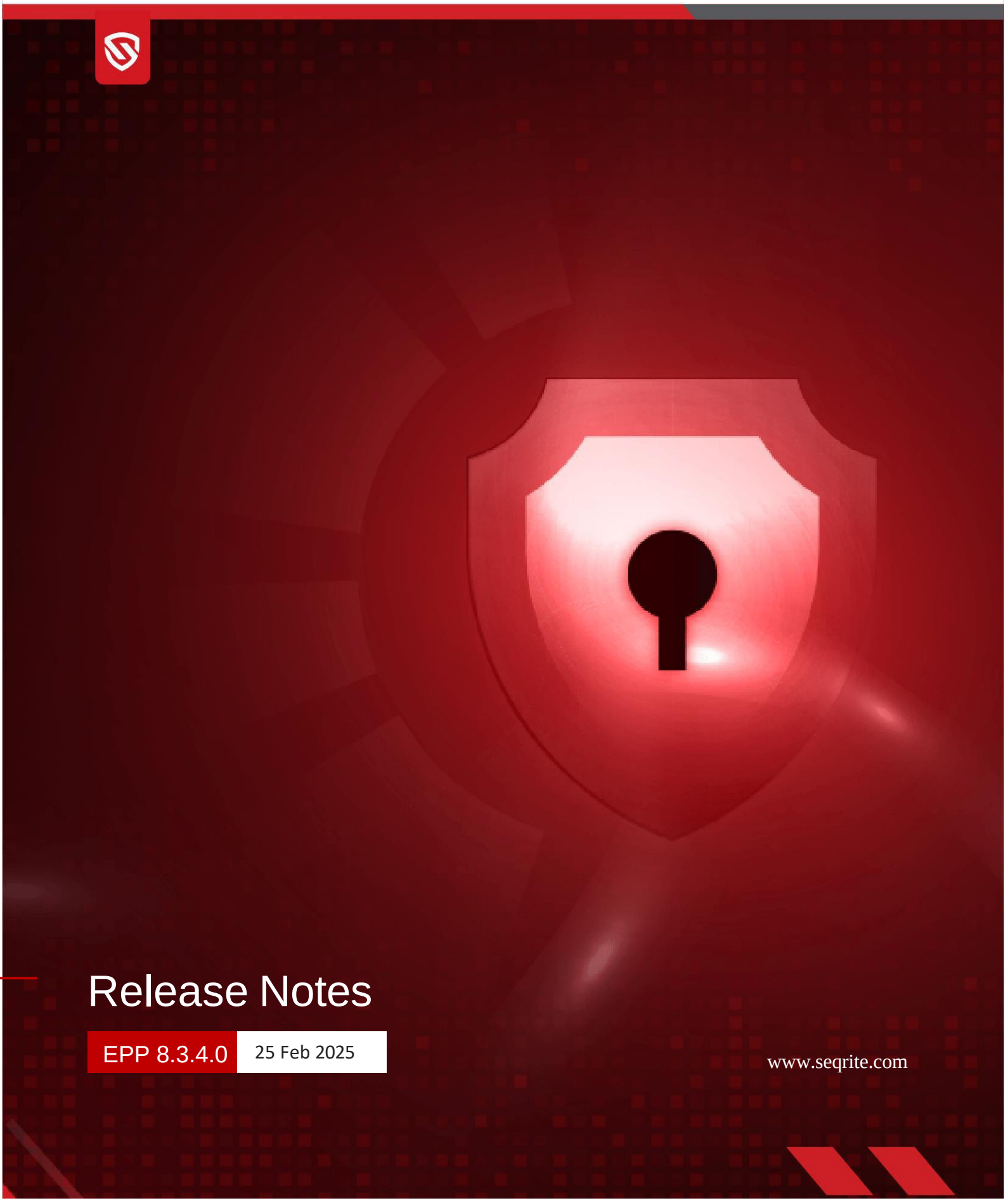
Seqrite

Endpoint Protection

SEQRITE



Release Notes

EPP 8.3.4.0 | 25 Feb 2025

www.seqrite.com

Copyright Information

Trademarks

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

Feature and Enhancements 2

Bug Fixes 2

System Requirements for Endpoint Protection Server 4

- EPP Standalone Setup 4
- EPP Distributed Setup 5
- EPP Multisite Setup 5

System requirements for Seqrite Endpoint Protection clients 6

- Windows 6
- Mac 6
- Linux 32-bit 6
- Linux 64-bit 7
- General Requirements 8

System requirements for Patch Management server 9

Known Issues 10

Usage Information 12

Revision History

Doc Version	Date	Comment
1.0	25 February 2025	Seqrite Endpoint Protection 8.3.4.0 Released

Feature and Enhancements

This Service Pack (SP) is a cumulative update that incorporates previously released service packs and enhancements. It includes the following key improvements:

- Migration Changes from 8.3.x to Cloud:
- Data Loss Prevention (DLP) Watermark capability.
- The Service Pack addresses various customer-reported issues, and improve reliability and ensure a smoother user experience.

This cumulative Service Pack ensures that all previous service packs and critical improvements are included, providing users with the latest features and fixes in single installation.

Bug Fixes

The following table consists of the customer fixes provided in EPP 8.3.4.0 Release:

Sr. No.	Summary
1	The issue where the "^" symbol was incorrectly included in the CEF format has been resolved. **Note**: Due the delimiter being changed in the SIEM events LEEF and CEF(Tab & space respectively), the already configured SIEM users might need to reconfigure their SIEM actions if configured using delimiters
2	Corrected endpoint names in Status Page export reports (client.csv) post movement to a group.
3	Addressed vulnerabilities for HTTP Strict Transport Security (HSTS) on ports 443 and 8443 in EPP 8.3.
4	Fixed issue where allowed web categories were being blocked and blocked sites were accessible.
5	Clients migrating from EPS 7.6 to EPP will now retain their roaming status. This ensures that the client is correctly identified as roaming or local after migration.
6	Resolved issue preventing report exports from the client status page and reports from being sent via email.
7	Resolved issue causing license deactivation on server that has multiple MAC IDs.
8	Fixed issue where software details were not updating after asset scanning.
9	Added license check during client migration for 7.x migrated clients. Clients will no longer be imported if the license count is exhausted, ensuring proper license management.

Sr. No.	Summary
10	Resolved issue causing import of `export.zip` to fail on Cloud5, with a "decrypt: illegal state exception," during client migration.
11	Fixed issue with offline license sync not working on AGR SSR. SSR license distribution is now properly sent to the activation server when performing license sync on AGR using the support offline activation tool.
12	In offline activation, license details are now properly synced from AGR to the activation server. SSR license distribution is correctly sent to the activation server during license sync using the support offline activation tool.
13	Resolved issue where clients were not receiving renewal after offline setup. The tenant status is now correctly updated to "ACTIVE" when the offline server is activated with the renewed product key, ensuring proper client actions are restricted until the renewal is processed.
14	Addressed vulnerabilities related to SSL certificates using weak hash algorithms. The certificate has been updated to resolve these security issues.
15	Reordered columns in all reports, CSV, and PDF exports. The 'Mac Address' column is now placed next to the 'IP Address' column, and the 'IP Address' column is positioned next to the 'Endpoint Name' column.
16	Improved SMTP configuration check for Temporary Device Access. The check has been moved to a later step, occurring after generating the OTP, when the "Notify" button is clicked.
17	Resolved issue where user sync was not working from EPP to OPE when the EPP installation type was 0. Added a check for standalone EPP server type to ensure proper sync functionality.
18	Fixed SIEM integration issue. • The "Apply" button will now always be enabled. The "Test" button has been removed from the SIEM UI.
19	Resolved issue where the "Status" column was not visible in the DLP report CSV and PDF files.
20	Replaced the text "Custom" with "Removable Drives" under the section “Select location and events to monitor within the drives” on the Policy → Policy Settings → File Activity Monitor page.
21	Resolved issue where system and hardware details were showing as blank records in the Comprehensive Asset report exported from the web console.
22	Fixed issue where patch scan missing reports were sent in rpclient logs but not appearing on the EPP On Prem console.
23	Fixed issue where the Save button and Roaming Options remained disabled after toggling the RP option.
24	Fixed issue where column values were shifted to the right starting from the 'Virus Protection' column in the Status → Export → Comprehensive Asset Reports → SystemAndHardwareDetails. The column alignment is now correct.
25	Resolved issue causing random 500 internal server errors during login to the EPP console.
26	Addressed JQuery vulnerabilities in EPS 8.2 console. The issue was resolved by updating the JQuery version.
27	Fixed watermark issue by adding `wtmply.exe` to apply local DLP policy after endpoint restart. The executable is placed in the `.\\Seqrite\\` folder and registered to run on startup.
28	Resolved issue where null strings appeared for some columns and "N/A" was displayed in the "Action Taken" column.

System Requirements for Endpoint Protection Server

EPP Standalone Setup

Server that supports up to 1 to 2000 endpoints

- Ubuntu 22.04 (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

Server that supports up to 10000 endpoints

- Ubuntu 22.04 (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

Server that supports up to 10001 to 15000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 350 GBs or above
- Available RAM: 24 GBs or above
- Processer: 12 Core(x86-64), 2.60GHz or above

Server that supports up to 15001 to 20000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 450 GBs or above
- Available RAM: 32 GBs or above
- Processer: 16 Core(x86-64),2.60GHz or above

Server that supports up to 20001 to 25000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 500 GBs or above
- Available RAM: 48 GBs 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:

Server that supports up to 10000 to 15000 endpoints

- Ubuntu 22.04 (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

Server that supports up to 15001 to 20000 endpoints

- Ubuntu 22.04 (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

Server that supports up to 20001 to 25000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 350 GBs or above
- Available RAM: 24 GBs 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 22.04 (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
  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

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 and Server 2022, 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 chip compatible
- 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 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 4.16 and earlier
- Supported Distributions for Seqrite Endpoint Protection client:
  - Fedora 30, 32
  - Linux Mint 19.3, 20
  - Ubuntu 16.04, 18.04, 20.4, 22.04
  - 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
  - SUSE Linux 12. SP4 / Enterprise Desktop 15
  - Rocky Linux 8.4
  - Boss 6.0, 8.0, 9.0
  - 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 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 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 GBs 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

- Antivirus registration fails and shows a status of "Failed, reboot required" in case of Online to Roaming Clients.
- The watermark in XLSX files is not centrally aligned, unlike in DOCX and PPTX files where the watermark is properly centered.
- Malware detected at a long path (over 260 characters) is displayed in the complete file path in Virus Protection and Scanner Reports on a client, but in a truncated format in Virus Scan Reports on EPP Console.
- If CNTRL+C is pressed on the terminal at the time of installation (GUI mode) then rollback may fail to initiate and installation need to be initiated again.
- Application Control: Allowed and Opened exe is not getting terminated after changing its policy (status) to block.
- Unable to Block recently downloaded files in DLP for all applications majorly for web browsers.
- File Activity Monitor (FAM): Copy events are not captured when the file is copied from Removable Drive to Local Drive.
- EPP Clients are not compatible if Smart App Control is Turned-On on Windows
- Application Control: User can add duplicate entry for %WINDIR% in Allowed Directories.
- Mac
    - Data Loss Prevention (DLP) block functionality will not work on macOS Catalina 10.15 and above if the attachment is sent through any mail application through the Safari browser.
    - File downloading is getting blocked through the browser if DLP is enabled.
    - File Activity Monitor:
        - The ‘Delete’ event is created with some temporary file name while 'creating' or performing the 'Save/Save As' file on the Local Drive or Removable Drive
        - If we compress files using any compressing tool, then a Delete event is captured for all the compressed files.
        - The events are not captured if we drag and drop or move the file using the terminal command mv on the same Removable and Local drive.
- Linux: Linux Tray icons and notifications are not supported on systems using the Wayland display protocol.
- Linux: Web Security: Web categorization and block specified feature currently not supported on RHEL 8.6.
- Site server: If we unassign the feature policy then that policy is still shows as applied in policy status if group policy is assigned for same feature.
- Team viewer is not getting launched on scanner of 8.3 server.

  Work Around: If we logged in as root user, then TeamViewer is launching successfully and we can successfully take the remote access of EPP 8.3 server system.

- 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 EPP 8.3 client.

3. To install EPP 8.3 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 Windows 7 32-Bit client, you must upgrade to Internet Explorer version 11.

5. If the administrator initiates 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, Administrator will need to add the device again in Device Control and configure the policies accordingly.

7. To use Browser Sandbox, turn off the Secure Boot feature of the system from BIOS Configuration.

8. By default, Spam Protection is disabled. So, a red exclamation mark appears on the client Dashboard.

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.