



Release Notes

EPP 8.6

Sep 2026

www.seqrite.com

Copyright Information

Copyright © 2008–2026 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media, or transmitted in any form without the prior permission of Quick Heal Technologies Limited, Solitaire Business Hub, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution, or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

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

Revision History.....	2
New Enhancements EPP 8.6	3
Known Issues	8
System Requirements	11
Client Requirements	12
Usage Information	14

Revision History

Doc Version	Date	Comment
1.0	Sep 2026	Seqrite Endpoint Protection 8.6 Released

New Enhancements EPP 8.6

Data Loss Prevention

Shadow Copy

Introduced **Shadow Copy** to store an evidence copy of files involved in DLP events on central server.

Granular Print Shadow Logging

Added support for configuring **shadow logging at the individual channel level**, allowing administrators to selectively enable logging for specific channels based on organizational security and compliance requirements.

Watermarking

Added support for configuring the font name and font size of watermarks to provide greater flexibility in watermark customization.

Print Whitelisting

Introduced application-based print whitelisting to allow printing from specified applications, such as Microsoft Word, even when the Print channel is blocked.

Path Access Control

Introduced **Path Access Control** to protect administrator-defined files, folders, and registry paths from unauthorized access or modification. It allows administrators to control which trusted processes can access protected paths, helping prevent unauthorized tampering with sensitive files and critical system settings.

Remote Shell

Introduced Remote Shell to enable administrators to remotely access and troubleshoot endpoints.

A secure, license-controlled Remote Shell feature with **role-based and command-level access controls, configurable command allow lists, active session monitoring, and CSV/PDF export**. Remote Shell activity and command logs are also captured for **auditing, compliance, and SIEM integration**.

Policy Preview

Added a **Policy Preview** page to view complete policy settings and associated groups on a single page. Administrators can also export the policy settings in PDF format.

Dashboard Group Filter

Added the ability to filter dashboard data by **group**. The **Filter by Group** option allows administrators to select a specific group and view data relevant to that group. The filter affects only the dashboard view and does not modify group assignments, policies, or endpoint configurations.

Advanced Device Control - CD/DVD Encryption

Added support for enforcing encryption when transferring data through CD/DVD devices. This helps prevent unauthorized access to confidential information if the media is lost, stolen, or accessed by an unintended user.

Upgrade and Migration

Introduced support for force-upgrading clients without requiring user intervention.

Import/Export Modules

Added support for importing and exporting settings for the supported features. This functionality allows administrators to **add or update multiple entries in bulk**, reducing the effort required to configure settings individually. Added support for the following features:

- **Policy:** Scan, Email, IDS/IPS, Firewall, Web Security, Data Loss Prevention, Update, Miscellaneous, Schedule Settings, and Path Access Control.
- **Configuration:** Device Control, Data Loss Prevention, Application Control, Enterprise File Search, and File Activity Monitor.

File Activity Monitor Enhancements

Enhanced File Activity Monitor (FAM) with improved activity and location-based monitoring capabilities. The enhancements include:

- Added support for monitoring file activities on **removable, local, and network drives**.
- Added **Copy** activity monitoring for local drives and Network Drive support.
- Added **Rename** and **Extension Change** activities, with Extension Change automatically enabled when Rename is selected.
- FAM reports now include both **source and destination** paths, providing better visibility into file movement and activity.
- Updated the **FAM configuration interface**, including UI layout, tooltips, and policy operations, for improved usability.

Group Update Agent

Enhanced the update mechanism to allow endpoints to automatically download updates from a **Group Update Agent** or a **custom URL**. Added a new update mode, **Download using the fastest-responding Group & Custom Update Agents**, which enables endpoints to:

- Select the **fastest-responding Update Agent** from the configured Group Update Agents or Custom Update Agents.
- Re-evaluate the available Update Agents when the update policy changes.
- Fall back to downloading updates from the **Internet** when no configured Update Agent is available or present in the local group.

Groupwise Service Pack Upgrade

Enhanced the groupwise client upgrade action to support **Service Pack (SP) deployment** based on tenant eligibility and client version. If an applicable SP is available, it is prioritized over minor or major upgrades, while clients on older versions are first upgraded to the latest version before receiving the SP. The enhancement also supports SP deployment through both **Client Action and Group Action**.

Secure API for Endpoint Status and Reporting

With this release, Seqrite will be exposing on-demand Secure APIs. These APIs can be used to integrate with any 3rd party tool, such as ITSM, Log management, Analytics tools etc.

Linux Endpoint Enhancements

- **File and Folder Exclusions:** Added support for excluding files and folders from scanning on Linux endpoints. MD5 checksum-based exclusions are not supported.
- **First Scan:** Files and folders added to the exclusion list are not considered during the first scan performed after installation.
- **Real-Time Protection for Network Drives:** Real-Time Protection now dynamically monitors mounted network drives on Linux endpoints.
- **New Linux OS Support:** Added support for the following operating systems:
 - RHEL 9.6, 9.7, and 10
 - AlmaLinux 9.6, 10
 - BOSS 10
 - CentOS 9, 10
 - Linux Mint 22.04 LTS
 - Oracle Linux 10
- **Firefox Extension Support:** Added Firefox extension support on Linux for GAC/YAC to enable security inspection and control of TLS and QUIC traffic in Firefox.

macOS Enhancements

- **Seamless Uninstallation:** Added support for uninstalling the product on macOS without displaying System Extension unload permission prompts.
- **System Extension Permission Notification:** If the required System Extensions are not approved, the Client Agent displays an alert/notification prompt asking the user to approve the required System Extensions.

Backup and Restore to support Disaster recovery

EPP now introduces enhanced backup and restore compatibility, ensuring smoother data recovery and improved reliability during backup restoration processes.

Administrators can now create on-demand backups or schedule backups for Endpoint Protection Server deployments. This enhancement helps ensure business continuity by enabling quick restoration of server data and configurations in the event of a system failure or outage, supporting disaster recovery requirements.

Archive file Protection for post scan level

Now, archive file scanning upto 25 levels or quarantine file if archive file is more than X level. Currently we are scanning archive files upto 16 levels only.

Temporary (Time-Based) Feature/Custom Policy Assignment

Added support for **temporary assignment of Feature/Custom Policies** through the existing **Assign Custom Policy** client action. Administrators can now assign one or more custom policies to selected endpoints for a specified period.

- Custom policies can be assigned **permanently or temporarily** with an expiry date and time.
- A temporarily assigned custom policy **overrides the container policy** for the specified duration.
- The custom policy is **automatically unassigned when it reaches the configured expiry date and time**.
- Administrators can assign custom policies to selected endpoints from **Status > Client Actions > Assign Custom Policy**.

Report

User Name column in console Report displays as "SYSTEM" instead of the actual username for all the client reports

Policy Update Notification

Email Alert is sent to All the email Ids configured in Admin Notifications Screen.

Notification

Immediate Server Notification for USB Device Control Policy Breach Events.

On-Demand Remote Support

To enhance security in restricted environments, Remote support binaries are no longer shipped by default. Remote support components are now downloaded and available only when explicitly initiated from within the product.

Asset Management

Asset Management scheduled scan now can be run daily.

Manual Report Download

Added support for manually downloading client module reports in **PDF and CSV formats** directly from the EPP console, reducing dependency on SMTP configuration and enabling easier access to reports for audits, compliance, and sharing.

Enhanced Group and Policy Scalability

Increased the supported limits for **Groups and Policies to 1700 each** and optimized the EPP Console for large-scale deployments. Enhancements include **group and policy search with wildcard matching, CSV export for groups, improved large-data dropdown handling, enhanced policy assignment, and optimized group hierarchy operations**. Drag-and-drop group movement has also been removed to improve performance and scalability.

Client Support for Linux 32 Deprecated

The Linux 32-bit Client build has been deprecated and is no longer available.

Customers using Linux 32-bit systems are advised to migrate to supported 64-bit Linux platforms.

Known Issues

Data Loss Protection

- DLP does not support Microsoft Store applications such as **WhatsApp**, **OneDrive**, **Microsoft Outlook**, and **Microsoft Teams**. Therefore, content shared through these applications is not blocked or scanned. **File attachments** shared through these applications are monitored and scanned by DLP.
- DLP currently does not detect **embedded files**. For example, an image of a PAN card embedded in a Word document is not detected.
- **DLP alerts** are not generated for activities performed over **RDP**.
- **Data-At-Rest Scan**: DAR Scan may fail when the amount of data to be scanned exceeds **12 GB**.

Shadow Logging

- Changing the **Shadow Copy Storage Server** configuration triggers a policy push.
- Shadow Logging does not work for **Data-at-Rest (DAR)** scans.
- **Print Shadow Logging** does not work when the action is set to **Block and Report**.
- Shadow Logging does not support uploading **read-only** files.
- Does not support cut-and-paste operations.

Print Whitelist

- For **Block and Report** action, the report displays the file name instead of the complete source path.
- For **Report only** action, files printed by applications added to the exception list display the file name instead of the complete source path.
- Files printed using **Command Prompt** or **PowerShell** and **OneDrive** or **SharePoint** display only the file name in reports. The source path displays the file name instead of the full path.
- For files printed from a **web browser**, the source path displays the browser tab name instead of the file path.
- In some cases, when the document name is reported as **Anonymous File**, the **Source Path** and **Source Destination** fields might remain blank.
- The source path is not captured for:
 - files with paths exceeding **260 characters**.
 - notepad files printing from removable devices.

- image files printing from **Microsoft Store applications (Microsoft Publisher and Microsoft Access).**
- **Horizontal watermarks** may be cropped at the page corners.

Email Notification for Policy Configuration Changes:

- Email notifications are sent when a container policy configuration is changed from the **Control Center**. No email notification is sent when the same configuration is changed from the **Site Server**.

Patch Synchronization Fails When All Filters Are Selected

- Patch synchronization may fail when all product and category filters are selected in Patch Management, particularly those related to Microsoft Windows. Synchronization completes successfully when the default filter settings or filters for non-Microsoft applications are used.
- **Workaround:** Before initiating patch synchronization, navigate to **Configurations > Patch Management > Patch Server > Apply Filters > Products > Microsoft > Windows** and clear the following product filters:
 - Windows 11
 - Windows Insider Pre-release
 - Windows Internet Explorer 7 Dynamic Installer

This issue occurs because some URLs have expired or certain CDN locations are unavailable on the Microsoft side.

FAM Exclusions in Existing Policies

- Newly added or modified FAM exclusions are not available in an existing policy. To view the updated exclusions, create a new policy.

Windows 11 25H2 Update Not Detected by Patch Scan

- Patch Scan does not detect the available **Windows 11 25H2 update** on Windows 11 24H2 endpoints, even though the update is available through Windows Update.

macOS

- On macOS Tahoe 26 and later, Bluetooth blocking functionality does not work, even though Device Control Blocked prompt appears.

Active Directory Configuration Fails:

- Active Directory configuration may fail with an **Active Directory connection is failed** error, even when network connectivity, DNS resolution, and domain trust verification are successful. The issue is associated with an **invalid ID error (QH-ERROR-INVALID-ID)** during AD configuration validation.

Wi-Fi Not Blocked When Wired LAN Is Connected

- On certain Windows endpoints, the **Block Wi-Fi when Wired LAN is connected** policy may detect the wired connection and display the corresponding notification, but the Wi-Fi adapter may remain enabled and continue to provide network access. In the reported environment, the enforcement action was incorrectly associated with the **Bluetooth PAN adapter** instead of the physical Wi-Fi adapter.

System Requirements

Recommended Hardware Configuration – Ubuntu 24.04.3 and above (Average Load)

Endpoints	CPU Cores	RAM (GB)	Storage (GB)	Signed Kernel
1 to 5,000	≥ 8 cores @ 2.6 GHz	≥ 12	≥ 200	6.14 to 7.0
5001 to 10,000	≥ 16 cores @ 2.6 GHz	≥ 18	≥ 250	6.14 to 7.0
10,001 to 15,000	≥ 24 cores @ 2.6 GHz	≥ 24	≥ 350	6.14 to 7.0
15,001 to 20,000	≥ 32 cores @ 2.6 GHz	≥ 30	≥ 450	6.14 to 7.0
20,001 to 25,000	≥ 40 cores @ 2.6 GHz	≥ 36	≥ 550	6.14 to 7.0

Note:

- Additional system resources may be required when FAM and DLP licenses or (add-ons) are enabled.
- The above-mentioned configurations are for Ubuntu Server in non-GUI mode.
- AVX support is needed to install EPP 8.x on Linux/Windows machines.

Client Requirements

Windows OS

- 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

MAC

- Processor:
Intel core or Apple's M1, M2, M3, M4 chip compatible
- Mac OS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13, 14, 15, 26 and 27

Linux 64-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier
- Supported Distributions for Seqrite Endpoint Protection client:
 - Fedora 30,32,35,37, 38, 39,40, 41, 42
 - Linux Mint 19.3, 20, 21.3, 22.04 LTS
 - Ubuntu 16.04, 18.04, 20.4, 22.04, 24.04

- Debian 9, 10, 12, 13
- CentOS 7.8, 8.2, 10
- RHEL 7.5, 7.8 , 8.2, 8.6, 8.8 Enterprise, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10
- 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), 10
- Oracle Linux 7.1, 7.9, 8.1, and 10
- Alma Linux 9.6, 10

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

Usage Information

- 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.
- For Windows 2016, Windows 2019 Server, and Windows 2022 Server, uninstall Windows Defender before installing the EPP 8.4 client.
- To install EPP 8.4.2 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
- To install patches on a Windows 7 32-bit client, you must upgrade to Internet Explorer version 11.
- 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.
- 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.
- By default, Spam Protection is disabled. So, a red exclamation mark appears on the client Dashboard.
- 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, a warning message **Linux client migration is not supported** is displayed.