Seqrite
Endpoint Protection Cloud

Internal Release Notes

Cloud 6.2 | June 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

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	27 June 2025	Seqrite Endpoint Protection Cloud 6.2 Released

What's New

With this release, the following features are added to EPP Cloud 6.2:

EPP Endpoint Color Theme

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:

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

Seqrite EPP System tray icon is available under 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.

Data Loss Prevention (DLP)

- Support for PDF document scan has been added.
- 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
        - Signal

        - Zoom
        - Webex
    - **File Sharing / Cloud Services**
        - Sync.com
        - Mega.nz
        - Egnyte
        - Resilio Sync
    - **Social Media / Others**
        - Trello

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

Action log notifications will be generated on 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 the 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.

Display Duration of the Quick Update notification

Display duration of the Quick Update notification that appears after successful AV update is reduced from 10 seconds to 2 seconds.

[Windows only]

Consent Based Upgrade and Reboot for Windows

Note: This feature enhancement will be available in phase wise manner.

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.

[Applicable for Windows]

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

- Trend Micro Apex One Security Agent 14.0.12684 and older
- 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

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.

For more details on the features and functionalities, please refer to the online help..

System Requirements

System Requirements for EPP Clients

For Installing Seqrite Endpoint Protection client through client install utility, the System requirements are as follows:

Any one of the following operating systems:

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

macOS

- 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 EPP 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 EPP client:

- Fedora 30, 32, 35
- Linux Mint 19.3, 20, 21.3
- Ubuntu 16.04, 18.04, 20.4, 22.04, 24.04 LTS
- Debian 9, 10
- 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, 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

Note: Linux Client Agent (v10.11) and above supports deployments only on Linux 64-bit OSs. The existing deployed agents on Linux 32-bit (v10.9) will continue to function as expected.

System requirements for configuring Encryption policy

Client Pre-requisites:

- Client version: 10.11 and above.
- License Edition: Premium

Hardware:

- TPM 2.0
- BIOS with UEFI mode

OS:

- Windows 10 64-bit
- Windows 11

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

Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPP 4.0 client.
2. To install EPP 4.0 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 Windows 7 32-bit client, you must upgrade to Internet Explorer version 11.
4. If the administrator initiates tuneup notification for the endpoint and if the endpoint is not logged in, then the tuneup 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, 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. 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.