Seqrite
Endpoint Protection Cloud

# Release Notes

Cloud 4.0 | 06 Apr 2024

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 | 06 Apr2024 | Seqrite Endpoint Protection Cloud 4.0 Released |

# Features and Enhancements

With this release, the following features are added to EPP Cloud 4.0.

- New Brand Name and Logo
    - The brand name has now changed from Seqrite Endpoint Security to **Seqrite Endpoint Protection**.
    - The product logo has been redesigned to align with a contemporary, industry-focused approach.
- Encryption Policy: Seqrite encryption policy lets you encrypt sensitive data and protect it from unauthorized access using Microsoft BitLocker.
  This feature enables you to encrypt or decrypt:
    - Windows operating system Volumes.
    - fixed data volumes.
- Data Loss Prevention
    - Custom Applications - This feature lets you add the applications that you need to monitor or exclude from the DLP.
- Migration: Users have the capability to transition from EPS versions 7.6, 7.4 and 7.2 to EPP Cloud 4.0.
- The users can view the Windows Client AV build version along with the CA version on the **Endpoint Status** screen: Status > Endpoint Name > Endpoint Status > **Product Version.**
  For example: 18.00 (13.0.0.1)
  Additionally, this information is also included in the exported csv file.
- The following new third-party antivirus detection are added while installing Windows Client AV:
    - F-Secure Client Security Premium 15
    - Coro 2
    - TotalAV 5
    - Cybereason ActiveProbe Antimalware 22 & 23
    - Cybereason ActiveProbe 22 & 23
    - Trellix Endpoint Security 10
    - Trellix Agent 5
    - VIPRE Endpoint Security Agent 13
    - CylancePROTECT 3

    - Sophos Endpoint Agent 2023
    - Avast Business Security 23
- For Mac:
    - Provided support for Advance Device Control on Mac OS ARM64 base system. These are the supported devices:
        - Storage Devices:
            - USB Storage Device
            - CD/DVD
        - Wireless & Wired:
            - Wi-Fi
            - Bluetooth
        - Others:
            - Local Printers
        - Device Exception
        - Allow Temporary Device Access
    - With System Integrity Protection (SIP) enabled on Mac OS, Full System scan and Schedule scan will encompass folders that are not safeguarded by SIP. Conversely, with SIP disabled on Mac OS, scanning will encompass all folders.
    - Provided logging support for Mac for Asset Management
        - This feature allows you to enable Asset Management logs under the product installation directory.
        - If any issue occurs on the Mac client related to Asset Management, then you can enable debug log.
        - This feature is applicable to only Mac clients.

*For more detail on the Features and functionalities, please refer the help/manual.*

 

# 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

**MAC**

Processor

- Intel core or Apple's M1, M2, M3 chip compatible

Mac OS

- MacOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13 and 14

**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
- 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, 8.8 Enterprise
- SUSE Linux 12. SP4 / Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0 (Desktop), 8.0 (Server)
- Oracle Linux 7.1, 7.9 and 8.1

**Note**: EPP Cloud 4.0 supports EPP Agent (v10.11) 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
- 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 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

# Bug Fixes

The following is a list of bugs that have been addressed and fixed in the EPP Cloud 4.0 release.

| Sr.No. | Summary |
|---|---|
| **Windows** | |
| 1 | Folders inside the cloud drives are not accessible due to OverlayIcon.dll. |
| 2 | Online Protection System service is crashing due to scanexl.dll. |
| 3 | Websites are not accessible on Chrome browser with Browser Sandbox feature. |
| 4 | Tuneup reports are not coming on the console under the Reports section. |
| 5 | Schedule scan time is not reflecting on EPP dashboard. |
| 6 | The installation of the EPP cloud client Anti-Virus (AV) is encountering an issue when proxy settings are configured during the creation of the Windows Client Packager. |
| 7 | Excessive temporary files are being generated within the Seqrite folder due to the combination of DLP, OCR and Clipboard functions, leading to disk space exhaustion. |
| 8 | Files classified as **Confidential** are not being effectively blocked within the DLP Application Channel. |
| 9 | Seqrite vulnerability scan detecting Openssl vulnerability within its own module. |
| **Mac** | |
| 10 | Mac systems getting into hang state while closing the client dashboard. |
| 11 | The process **com.quickheal.sysextcontainer.ggc** is consuming excessive memory usage on Mac OS |
| 12 | Emlprod port 5432 is conflicting with Postgresql database. |
| 13 | Asset details are not getting populated on the console's endpoint status page for Mac endpoints. |

| Linux | |
|---|---|
| 14 | Due to a garbage value in the **qhupdate** time structure, the expiry calculation was inaccurate, leading to the creation of the expiry file exp.conf. |

# 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.
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.