Seqrite
Endpoint Protection Cloud

Release Notes

Cloud 5.1 | 19 Oct 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	19 Oct 2024	Seqrite Endpoint Protection Cloud 5.1 Released

What's New

With this release, the following features are added to EPP Cloud 5.1.

Server-Side: Feature Highlights

Migration from Seqrite EPP 8.3 On-Prem to EPP Cloud

EPP Cloud is now migration ready for EPP 8.3. Enhanced the migration feature to support the migration from Seqrite EPP 8.3 On-Prem to EPP Cloud. Located under **Deployment > Migration > Migration to Cloud**, this feature enables users to migrate essential data, including groups, policies, endpoints, admin settings, and global configurations, from Seqrite EPP 8.3 to EPP Cloud. All migration activities are logged under Admin > Activity Logs. Post-migration, systems will be upgraded to version 10.12 from either 10.9 or 10.11. This migration is compatible with both Windows and Linux platforms.

Enhanced Custom Policy Assignment

Users can now select and assign custom policies to multiple endpoints simultaneously, whereas previously only a single endpoint could be selected for policy assignment.

Upgrade Rollout for Client v10.11

A minor upgrade from Client v10.11 to v10.12 is scheduled to be rolled out in phases. This upgrade will provide v10.11 clients with access to the features of EPP Cloud 5.1.

Product Version Display Update

The product version is now displayed for Mac and Linux endpoints in the Cloud Server Web Console under Dashboard > Status > Endpoint Status.

Miscellaneous Feature Highlights

- Enhanced Remote Installation by IP Address with CSV Upload Option (for Windows and Linux)

  CSV Upload Option Added: The Remote Installer Tool now supports uploading a CSV file with IP addresses providing capabilities to install agents on multiple systems with different passwords.

- Policy Page Enhancements

  The Policy Status popup has been renamed to *Policy Insight*. The *View Detail* link now opens the Policy Insight popup, which features an enhanced view that includes:

  - **Applied Groups**: works as is.

- **Policy Status on Endpoints**: Shows the policy status for applied endpoints, including Pending, Applied, and the newly added *AV not installed*, under the status column for better understanding.
- **Search Functionality**: The search feature now allows filtering of endpoints by Endpoint Name, IP Address, and a newly introduced *Status* filter, which includes the option *AV not installed*.

Client-Side: Feature Highlights

Mac

- Mac Client Build Version Update

  The build version will now be visible for Mac endpoints on the 'About Seqrite Endpoint Protection' page.

Linux

- Client Support for Ubuntu 24.04 LTS (64-bit)

  The Seqrite EPP Cloud client is now supported on Ubuntu 24.04 LTS (64-bit).

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

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

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
- 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: 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 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 are fixed in the EPP Cloud 5.1 release:

Server	
1	Resolved an issue where sorting and searching for AV status was not functioning properly.
2	**Issue:** Patch scan reports were experiencing delays in reflecting on the EPS Cloud.
Client	
Windows/Mac/Linux	
1	Addressed high CPU consumption by the qhscanui process during scans on Linux clients in EPS Cloud 4.0.

Known Issues

The following are known issues identified in the EPP Cloud 5.1 release:

- Browser sandbox functionality is not supported on Microsoft Edge.
- Existing clients with a pending policy status will remain in that state when an AV is not present or installed.
- Error 40002 is appearing on the dashboard for the patch scan overview chart in version 5.1. This issue is reproducible only for tenants using a shared database and patch manager.
- When applying a policy on a client with port scan enabled, if a port scan violation occurs, the target IP is blank in the port scanning reports.
- Last Connected Time [EPP v8.3 with Migration SSP to Cloud]: When EPP Server data is imported into the cloud tenant, the default Unix epoch time initially appears as the endpoint's Last Connected Time. This is automatically updated to the actual time once the endpoint first connects to the cloud tenant via a heartbeat.

  Workaround: In the Admin -> Settings, set the "Remove a client if inactive for" option to "Never". This will ensure that imported endpoints are not removed from the cloud tenant if they are not migrated from the EPP Server on the same day the data is imported.
- USB tethering block/allow option may appear Twice in policy.
- 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.
- Mac - File downloading is getting blocked through the browser if DLP is enabled.

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 [7.6/7.4/7.2 to cloud] option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is displayed.