Seqrite

Endpoint Protection

SEQRITE

Release Notes

EPP 8.3

www.seqrite.com

Copyright Information

Copyright © 2008–2024 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 prior permission of Quick Heal Technologies Limited, Marvel Edge, 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 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

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Revision History

Doc Version	Date	Comment
1.0	July 1, 2024	Seqrite Endpoint Protection 8.3 Initial Release.
2.0	July 30, 2024	Seqrite Endpoint Protection 8.3 Subsequent Release.

What's New: Initial Release (July 1, 2024)

This release introduces the following features in Endpoint Protection version 8.3:

New Brand Name and Logo

The brand name has transitioned from Seqrite Endpoint Security to Seqrite Endpoint Protection, accompanied by a redesigned logo reflecting a modern, industry-focused approach.

Control Center

The Control Center acts as the centralized hub for overseeing all Site Servers. Each Site Server manages local clients (endpoints) deployed across various geographical locations.

Feature highlights

- Offers a **comprehensive dashboard** view, including customizable pages.
- Facilitates **onboarding** and management of **Site Servers**.
- Allows **license management** for site servers directly from the Control Center.
- Enables **Policy enforcement** from Control Center to Site Server:
  - Supports **single** as well as **multiple** policy enforcement.
  - Identifies all inherited policies, configurations, and users with an 'i' icon.
  - Prevents SSR users from deleting CC synced/inherited policies, configurations, and users.
- Allows overriding enforced policy on the SSR side using the feature policy.
- Supports **Single Sign-On** for any onboarded site servers.
- Provides a **Reports Drill Down** facility from the dashboard to the Control Center report section.
- **User Management Facility:** Facilitates creation, modification, duplication, import, and deletion of roles for different types of user roles.
- **Alerts:** Ensure that users are aware of critical alerts related to Site Server onboarding, Control Center protection, and feature policy details.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

- **Audit Logging**: This helps you check the activity logs of all the incidents occurred on the server.
- **Offline activation:** This helps activating Control Center in the air gap network.
- Ensures **Import/Export** of configured **policies**.
- The **search policy** list facilitates quick and easy policy searches.
- Supports **migration of policy** from EPS/7.2/7.4/7.6 to Seqrite Endpoint Protection 8.3.
- Offers Reports for various features on multiple categories generated from the Control Center.

EPP 8.3 Server/Site Server

Seqrite Endpoint Protection is designed to provide flexible, centralized management and control for over a thousand endpoints. It brings all the essential security features under a single management console.

One single agent that consolidates firewall, IDS/IPS, application and advanced device control, rule-based web filtering to provide robust protection, monitoring and control of endpoint security. It also allows scanning of mobile devices. It provides multiple scanning methodologies to detect threats to safeguard workstations and deploy BYOD policies effectively within the network.

Feature Highlights

- Endpoint Detection and Response (EDR)
  Our EDR platform deployed on your infrastructure protects endpoints from potential cyber threats, detecting and responding to threats that traditional antivirus solutions may miss.
- User Management Facility
  - Facilitates creation, modification, duplication, import, and deletion of roles for different types of user roles.
  - User sync from Control Server to Site Server.
- Boot Scan Protection

  Add password protection for skipping boot scans, enhancing security measures.
- Reports
  - **Mac Address and IP Address** added for the reports.
  - Access advanced device control features with added the columns **Manufacturer Name.**
- Encryption

  Seqrite encryption policy lets you encrypt sensitive data and protect it from unauthorized access.

  Data on a lost or stolen device is vulnerable to unauthorized access, either by running a software-attack tool against it, or by transferring the device's hard drive to a different device. Seqrite encryption feature helps mitigate unauthorized data access by performing volume encryptions using Microsoft BitLocker.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

This feature enables you to:

- encrypt or decrypt OS drive.
- encrypt or decrypt fixed data drives.

- Data Loss Prevention (DLP)
  - Custom Action addition

    This option gives us more freedom to report or block (for example, now only PDF can be blocked and other file formats like word, excel can work freely and vice versa.
  - Custom Apps
    - Custom Applications: This feature lets you add the applications that you need to monitor or exclude from the DLP.
    - User can now customize the block report action on multiple data types.
    - Users can Block and report multiple data types and can customize the block all and report only files respectively.
  - Custom Classifiers

    A custom list of classifiers is meant for monitoring data transfer through a channel. It is a tailored set of rules or criteria used to identify and categorize specific types of data as they move through communication channels within a network.
- Proxy Support for Endpoints

  Simplify deployments and management across all endpoints, regardless of proxy configurations, streamlining workflows.

- 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 and 23
  - Trellix Endpoint Security 10
  - Trellix Agent 5
  - VIPRE Endpoint Security Agent 13
  - CylancePROTECT 3
- RHEL 9 Support

  Effortlessly deploy EPP across Linux machines with seamless RHEL 9 support, ensuring compatibility with the latest Red Hat Enterprise Linux versions.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Mac

- **Advanced Device Control Support for macOS ARM64 Systems:** The latest update introduces support for Advanced Device Control on Mac OS ARM64-based systems, enhancing device management capabilities.
- **Enhanced System Integrity Protection (SIP) Integration**:

  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 is exclusively available for Mac clients.
  - Users can activate Asset Management logs within the product installation directory.

  In case of any issues related to Asset Management on Mac clients, administrators can enable debug logs for troubleshooting purposes.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

What's New: Subsequent Release (July 30, 2024)

This release introduces the following features in Endpoint Protection version 8.3:

Upgrade from EPS 8.2 to EPP 8.3

Users can seamlessly upgrade from EPS 8.2 to EPP 8.3. The transition will help avail benefits that safeguard all Endpoints. The upgrade can be carried out independently and can be performed in the following ways.

- Server upgrade
- Client upgrade: Supports Windows and Linux (64-bit) only.
- Patch Management Server upgrade

Phase Rollout

A phased rollout supports upgrade, SSP (Special Service Pack), and Service Pack in stages rather than all at once. This approach allows us controlled distribution and careful monitoring at each phase before proceeding to the next, ensuring smoother transition and minimizing potential issues. With this channel we can target specific customers without significant delays as same can now be directly delivered to their environment.

Update Agent upgrade

Users with earlier client versions can perform a server upgrade from 8.2 to 8.3. Post upgrade the Update Agent downloads updates for both 8.2 and 8.3 clients across Windows, Linux, and macOS platforms.

Standalone Update Manager

This Update Manager downloads updates for both 8.2 and 8.3 clients across Windows, Linux, and macOS platforms.

High Availability (HA)

High Availability (HA) refers to the design and implementation of systems and architectures that ensure continuous and uninterrupted access to services, applications, and data, even in the case of hardware failures, software glitches, or other disruptions.
This feature:

- Provides high availability for the Seqrite EPS 8.3 solution.
- Automates deployment of complete clustering components through Ansible.
- Supports directory synchronization for log backups.
- Deploys cluster maintenance and alert scripts using Ansible.

Note: Supports standalone EPP installation.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Linux

Introducing a standalone application, Seqrite Universal Update Manager supporting the Linux operating system.

- Seqrite Universal Update Manager is a standalone tool specifically designed to download and manage updates across a range of Seqrite products, supporting multiple updates.
- It provides the convenience of downloading updates for all Seqrite products on a single machine.
  Note: This Update Manager downloads updates for both 8.2 and 8.3 clients across Windows, Linux, and macOS platforms.

Disaster Recovery for Site Server and Control Center

Backup and Restore Mechanism: The updated backup and restore capabilities allow you to seamlessly restore data either on the original machine or a different machine, ensuring effective recovery and minimal downtime in the event of a system failure.

OVA Support for EPP Server

Added OVA support for EPP 8.3 Server to simplify the server deployment.

For more detail on the Features and functionalities, refer the respective guide/help.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

System Requirements Endpoint Protection Server 8.3

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

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

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.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

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:

- SEPS 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
- Mac OS X 10.9, 10.10, 10.11, macOS 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 Seqrite Endpoint Protection client:
- Debian 9, 10
- Ubuntu 14.04,16.04
- Boss 6.0
- Linux Mint 19.3

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

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

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

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

Note: On EPP Server minimum 20 GB free space is required for Server Upgrade.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

System requirements for Patch Management server

- OS:
  - 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.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Bug Fixes

The following table consists of the customer fixes from previous releases.

Sr. No.	Summary
	Windows
1	Online Protection System service is crashing due to scanexl.dll
2	Websites are not accessible on Chrome browser with Browser Sandbox feature.
3	Tuneup reports are not coming on the console under the Reports section.
4	Schedule scan time is not reflecting on EPP dashboard.
5	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
6	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.
7	Files classified as Confidential are not being effectively blocked within the DLP Application Channel.
8	Software changes reports are not getting generated "No data available".
9	BDS exclusion is not working if excluded through policy from the EPSNG8.1 console
10	File is not getting blocked with the file classification of "Confidential" in DLP Application Channel.
11	Unable to receive the Email with email protection enabled due to UTF8 configuration.
12	Reboot prompt occurs repeatedly on the migrated clients from EPS7.6 to EPSNG8.2 due to pending rename.
13	Facing issue during downloading large reports FAM.
14	Patch download failed on Patch server with error [INTERNAL FAILURE] cause due to multiple languages selected in metadata of few Win 11 patches.
	Mac
1	Mac systems getting into hang state while closing the client dashboard.
2	The process com.quickheal.sysextcontainer.ggc is consuming excessive memory usage on macOS.
3	Emlprod port 5432 is conflicting with Postgresql database.
4	Unable to open Mac Client Dashboard on macOS Ventura ARM64-Architecture.
	Linux
1	Asset DB parsing response is not sent to endpoints, due to which asset details like Software and Hardware info not reflected on console.
2	Asset details such as Software and Hardware are not showing for recently installed Linux clients.
3	Unable to browse websites and Exclamatory mark on the network icon on Linux systems due to qhwebsec service.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Known Issues

Here are the known issues in version 8.3:

- 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 EPS 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.
- EPS 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.
    - System performance may get degraded while accessing certain applications on macOS Sonoma.
    - 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.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

- 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.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only

Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPP 8.3 client.
2. 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
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. 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.

Copyright © 2008–2024 Quick Heal Technologies Ltd. Confidential – For internal circulation only