Seqrite Endpoint Security Cloud 1.6

Release Notes

Seqrite
Endpoint Security Cloud

Copyright Information

Copyright © 2018–2022 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 Security 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

Introducing Seqrite Endpoint Security Cloud

Seqrite Endpoint Security Cloud is an integrated solution that allows the management and regulation of multiple Endpoint Security products deployed at different geographical locations. IT administrators from any location can easily connect to the cloud to view the latest security status, configure product policies, receive notifications, and rectify critical network events from one single dashboard. Seqrite Endpoint Security Cloud also facilitates policy configuration, backup and more on the cloud for Seqrite products.

Available flavors

Seqrite Endpoint Security Cloud is available in the following flavors:

- Standard
- Advanced
- Premium

The following table lists the features that are available in the flavors:

Features / Edition	Standard	Advanced	Premium
Antivirus	✓	✓	✓
Antiransomware	✓	✓	✓
Email Protection	✓	✓	✓
IDS/IPS Protection	✓	✓	✓
Firewall	✓	✓	✓
Antiphishing	✓	✓	✓
Browsing Protection	✓	✓	✓
Vulnerability Scan	✓	✓	✓
Antispam		✓	✓
Web Security		✓	✓
Advanced Device Control		✓	✓
Application Control		✓	✓
Asset Management			✓
Tuneup			✓

Copyright © 2018–2022 Quick Heal Technologies Ltd.

Data Loss Protection	**Available as add-on pack with Advanced and Premium**
Seqrite HawkkHunt	**Available for Trial and Commercial license**

New Features and Enhancements

- **Vulnerability Scan (VS)** is the new feature added to scan vulnerabilities at the client.
    - This feature allows you to scan the known vulnerabilities in the installed applications in your network.
    - You can probe the endpoints for applications and operating system patches for possible vulnerability.
    - VS helps to create security measures against the vulnerabilities and secure the endpoints against data outage.
    - User can filter the reports based on Vendor, and severity of the present vulnerability.
- **Policies**
    - Provision to disconnect infected endpoints from the network in the following scenarios.
        - Non-repairable virus found.
        - DDOS attack is detected.
        - port scan attack is detected.
    - Granular control over groups - A Group Admin now manages all sub-groups of the group to which GA is assigned.
    - Provision to configure ports for Email Scan under Email settings.
    - Provision to control devices other than USB storage under Device Control.
    - Improved efficacy while blocking web categories.
    - On the Status page, 'Last Scanned' time of endpoints is shown.
- **Dashboard**
    - Top 10 reports on the Dashboard.
- **Reports**
    - Provision to schedule monthly or weekly reports to be sent to one or more email recipients.
    - Reports are automatically archived every month and the archives are retained for 15 months.
    - Provision to download reports in the PDF or CSV format.
    - Introduced Host Integrity report to view compliant and non- compliant endpoints.
    - Event logs visible on the endpoint under Reports are now sent to the server too.
- **License**

    - Provision to automatically release licenses being consumed by inactive endpoints or duplicate endpoints.
    - Provision to update a trial license to a commercial EPS Cloud license.
- **Endpoints - OS Support**
    - Seqrite Endpoint Security Cloud supports the following new versions of OS.
        - Windows Server 2022
        - Windows 11
        - Windows 10 21H2
        - Linux Mint 19.x / 20.x
        - CentOS 7.x / 8.x
        - Rocky Linux 8.x
        - RHEL 7.x / 8.x
        - Ubuntu 18.04 / 20.04
        - BOSS Linux 8
        - macOS 12 Monterey

          Note

          From EPS Cloud 1.6 onwards, Apple M1 chip is supported.
- **Other features**
    - Block data transfer over PTP/MTP on Linux.
    - Multi Factor Authentication for users.
    - Provision for EPS clients to synchronize settings from the server.

Recommendation

- Seqrite recommends NOT to add DDOS/PORT scan Features in policy unless the Endpoint is upgraded to v10.6.0.0.

  Else garbage characters appear on the Reports page.
- For seamless experience, use Internet Explorer 10 and above. For details, please refer System Requirements.
- For Linux Antivirus client, Seqrite recommends to disable SELinux for RHEL based distro stream.

Copyright © 2018–2022 Quick Heal Technologies Ltd.

Known Issues

- DLP support on Chromium based Edge browser is limited.
- **Reports**
  - If we select a date range of more than 180 days in reports and generate the report it shows exceptions.
  - In the Vulnerability Scan report, **Vulnerability ID** column shows CVE ID in form of the link. Clicking the CVE ID takes you to the Repository site displaying vulnerability details of the CVE ID. But, for some CVE IDs, the Repository site shows " Unknown Definition ID" message.
- On the **Status page,** under the **User Name** column, only local logged-in user name of the endpoint will be shown.
- On Windows 10 and above system, Remote Installation and Network Enumeration features do not work as expected.

  Resolution

  SMBv1 is not installed by default in Windows 10 and above versions. Enable SBM1 protocol to fix this issue.

  To enable SBM1 protocol, follow these steps:

  1. Go to the Control Panel >>Programs and Features.
  2. From the left pane, select the **Turn Windows Features on or off** link.
  3. Select the **SMB 1.0, SMBv1, CIFS Client** check boxes.
  4. Restart the system.
- **Mac Known Issues**
  - The Device Control feature is not supported on Apple M1 chip.
  - Bluetooth device control is not supported for Monterey Intel.
- **Linux Antivirus**
  - Tray icons and notifications are not supported on systems using the Wayland display protocol.
  - No support for Unicode.
  - For Ubuntu 20.04 LTS, user need to give "allow launching" permission for Seqrite desktop shortcut.

Technical Support

Seqrite provides extensive technical support for its users. In case you face any technical issue, you can contact our Technical Support center using the options available at the following URL:

https://www.seqrite.com/seqrite-support-center