Seqrite Endpoint Security Cloud 1.4

Release Notes

Copyright Information

Trademarks

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

1. Introducing Seqrite Endpoint Security Cloud 2
2. New Features and Enhancements..... 3
3. Known Issues 5
4. Technical Support 6

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 three flavors of Standard, Advanced, and 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	✓	✓	✓
Antispam		✓	✓
Web Security		✓	✓
Advanced Device Control		✓	✓
Application Control		✓	✓
Asset Management			✓
Tuneup			✓
Data Loss Protection	**Available as add-on pack with Advanced and Premium**		

New Features and Enhancements

Seqrite Endpoint Security Cloud

- Provision to exclude MD5 checksum from Scan policy. To do this, go to Scan > Exclude File and Folders.
- In the Scan, Archive Scan Level supports up to 16 levels. Archive Scan Level is increased to 16 level in on demand Client action for Scan, Scheduled Client Scan.
- Provision to select Scan Priority for Application Control, Scan, DAR Scan Schedule / On Demand Scan. The Scan priority values are 'High', 'Normal' and 'Low'.
- Endpoint Status column on the Status page provides information whether the endpoint is online or offline. Endpoint status is changed to offline as per the configured missed heartbeat count to turn endpoint offline.
- Provision to Perform Boot Time Scan in Schedule Settings and Scan.
- Provision to store data backup in a customized way. You can add custom extensions to the custom list. Provision to generate customized backup reports. Provision to Delete old/current backup data.
- On Virus Scan report page, provision to view the statistics of unscanned endpoints since last 1, 3, 7, 15, and 30 days.
- Group Admin User Role
    - Provision to create Group Admin for each group. You can assign multiple Group Admins to one group.
    - Super Admin and Admin user can create/edit/delete the Group Admin user and assign/unassign the Group Admin to any group.
    - Group Admin can generate reports in table /chart formats for endpoints assigned to its group only.
    - When Group Admin logs on, the Status page is displayed by default. The Group Admin has limited access to pages of Seqrite Endpoint Security Cloud.
    - The policy created by Super Admin or Admin when applied on the group is read only for Group Admin.
    - If you delete the Group Admin, the policies created by the Group Admin can be deleted if the policies are not assigned to any group and endpoints.
    - If you delete the Group Admin, the policies created by the Group Admin cannot be deleted if the policies are assigned to any group and endpoints.
- Provision to download Active Directory Tool. With Active Directory Tool you can synchronize the EPS server group with active directory organizational unit

(OU)/container/computer. After synchronization, the clients will be installed on all the endpoints of your domain network. A periodic check is carried out to find if any new endpoint is added to your network. When a new endpoint is added, the client gets automatically installed on that endpoint. You can also exclude certain endpoints from the EPS server group so that the client is not installed on these endpoints.

- Seqrite Endpoint Security Cloud supports Windows 10 Nov 2019 Update (19H2).
- Seqrite Endpoint Security Cloud supports macOS Catalina.
- Major Upgrade for MAC
- UA will provide updates to old versions of Windows, Mac, and Linux clients.

MSSP

- Apart from UEM if the admin is associated with other Seqrite Cloud Products then on the MSSP's product selection page, the admin would see all the associated products.

Known Issues

File is not getting excluded from scanning on MAC client if it is present in any of archive(.zip) type and that file name is added into the exclusion list.

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