SEQRITE

SEQRITE HawkkProtect 1.9

Release Notes

21 January 2023

Copyright Information

Trademarks

License Terms

Contents

Introducing SEQRITE HawkkProtect

HawkkProtect from SEQRITE helps organizations enforce the zero trust user access paradigm, where an organization by default does not trust any employee, contractor, or vendor staff with access to its systems and applications whether from within or outside the corporate network. It also replaces the complexity of VPN management.

Starting your zero-trust journey with HawkkProtect:

- Create a zero-trust ecosystem with controlled set of users and applications.
- Deploy an agent-less solution and expand as per security appetite.
- Plug in your security requirements and deploy HawkkProtect within minutes.
- Integrate HawkkProtect with your existing IT infrastructure for identity management.

What's New

SEQRITE HawkkProtect includes the following features.

SMS-based OTP Support for Local User Authentication

Added support of SMS OTP on Mobile along with existing Email-based OTP for end-user authentication and authorization.

Support for Agent-based Applications

Manage who has access to private applications and services with the help of an agent. HawkkProtect will not grant access to private applications if the agent is not installed. Supported protocols: HTTP, HTTPS, RDP, SSH, Telnet, SMB.

Device Posture Check

To ensure only safe, known devices can connect to your resources, evaluate device posture through multiple attributes such as the presence of SEQRITE EPS client, MAC/IP Address, device serial number, domain name, hostnames, etc., before granting access to an enterprise application.

HawkkProtect Agent and Device Management

Maintain device inventory to see the activity of the installed HawkkProtect agent and other important device-related information.

180 days Log Retention

Log retention has been increased to 180 days. Now the admin can fetch the data for 180 days for Visibility, Audit trail, and Dashboard through the custom filter.

Known Issues

Some of the important known issues in version 1.9 are as follows.

- The Entity ID and Reply URL are not auto populated for the site deployment of an existing tenant.

  Workaround: Administrator must manually enter the values in this field.
- After deleting a site, all the applications are marked as inactive.
- Unable to upload a file bigger than 100 MB in the application after adding it on the admin portal.
- After closing the user portal without properly logging out, a user tries to log in again. This creates a duplicate active session.
- Loading a large number of connections on the Visibility page is CPU intensive on the administrator computer.
- For ADFS IdP, logout request fails intermittently and an error is displayed.
- The application location is displayed as Undefined on globe view for blocked connections.
- In Google workspace IDP, User portal SAML logout is not supported due to technical limitation from Google.
- Admin portal is not supported on Safari browser.
- If users are deleted in AD, the policy access rules related to deleted users are not getting flushed.
- You cannot edit the RDP application when you have two or more applications with the same domain name or IP address.

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