SEQRITE HawkkProtect 2.0.5

Release Notes

25 August 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 new features.

Seamless Integration of SaaS applications

Introducing integration for SaaS applications along with extended access. Administrators can now:

- Control Enterprise Application Access for managed HawkkProtect Devices.
- Restrict Enterprise Application Access for Android users outside the mSuite workspace container, provided that mSuite is enabled.

While currently supporting Google Workspace, Zoho, and Office 365 applications, this enhancement empowers effortless expansion of the supported application suite.

Email Notifications for Critical Events

Presenting prompt email notifications for critical events. Administrators receive timely inbox alerts, staying updated about significant occurrences in the HawkkProtect ecosystem. This enhancement keeps you connected and responsive to events in real time.

User Portal Personalization

Providing enhanced customization options for the user portal. Administrators can now upload custom logos, favicons, and background images, as well as fine-tune the browser window title. Tailor the user portal's look to match your brand identity with ease.

Enhanced Device Posture Rule and List Management

- Introducing an upgraded device posture rules feature that utilizes both AND and OR operators and provides you with increased control over conditions, to root out non-compliant devices.
- Enabling improved device posture list experience with convenient add and search functionality.

Note

For optimal utilization of the HawkkProtect Agent and App Connectors, we encourage you to update them to the most recent version. By doing so, you will gain access to the latest features, enhancements, and security advantages. Furthermore, please be aware that we offer support for the two versions preceding the latest one, creating a supported range referred to as ‘Latest-2’.

Known Issues

Here are the known issues in version 2.0.5.

- During the HawkkProtect onboarding process, the SaaS Application tab does not display onboarding steps as expected, unlike the App-Connector and Policy pages.
- User portal login experiences looping behavior with Azure and Google IdPs.
- The agent-based app fails to connect on the first click, intermittently.
- Changing the status of the HP agent from enable to disable does not promptly result in the blocking of SaaS apps; a relog is necessary.
- Deleted SaaS applications remain accessible even after removal through the Admin UI.
- Logging out from the user portal doesn't prevent continued access to SaaS apps.
- File copying encounters failures during the process of uploading and downloading a substantial number of files.
- The file transfer data size does not appear on the dashboard.
- Intermittent failure of logout requests accompanied by a "CORS" error.
- In the globe view, the location of the blocked application appears as “undefined”.
- Connectivity of agent-based applications on Linux Mint OS is compromised when using the Firefox browser. It is recommended to use the Chrome browser instead.
- Elevated CPU utilization is observed on the client machine when attempting to load connections on the visibility page.
- Upon clearing the "Sign SAML Request" checkbox on the site page for ADFS, the user portal becomes inaccessible.

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