SEQRITE HawkkProtect 1.1.2

Release Notes

30 August 2022

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.

Local User Management

- Manage users locally by importing/adding them through HawkkEye.
- Users get synced automatically in HawkkProtect admin console.
- Admin can send invite to users and users will sign-up first time.
- End users can authenticate and authorize them on a user portal by password less OTP based authentication to access user/gateway portal.

HawkkProtect Generated Certificate

- You can now opt for automatically generated SSL certificate in absence of organizational SSL domain certificate. Certificate will get issued to *.organization_name.hawkkprotect.com .
- Automatic CNAME record verification and HawkkProtect will take care of life cycle management of generated certificate.

Layer 7 Firewall and DDoS

- Create layer 7 firewall policy rules to block application access from connections originating via specific IP addresses or country. You can apply a rule on specific application parameters such as query params, methods, custom paths, etc.
- Create DDoS policy rules to block application access based on the number of requests from a specific IP address or from multiple IP address to a particular application. You can apply a rate limit for a specific timeframe. If the no. of requests exceeds, the connections would get blocked.
- Enable Web Application Firewall (WAF) rules to restrict users accessing applications which are vulnerable to web attacks like SQL injections, Cross Site Scripting, etc.

Other features

- New widgets added on dashboard.
- UI/ UX Improvements
- Bug fixes

Known Issues

Some of the important known issues in version 1.1.2 are as follows.

- Special character '-' cannot be entered in the organization name while adding an auto-generated certificate.
- 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.
- Password based authentication does not work for WebVNC.
- For web RDP port type; after the application is minimized, user is not able to maximize the application.
- If a user closes application browser tab without closing application, and then opens another application of RDP; the user will see both application simultaneously.
- After deleting a site, all the applications are marked as inactive.
- Large application logos are displayed on the user portal when the application name is entered in uppercase letters.
- The HawkkProtect apps portal is also displayed as ZT gateway user portal on some of the pages.
- Policy name is displayed incorrectly in the exported CSV file.
- A custom path '/' gets automatically added while editing a firewall policy.
- During onboarding; while editing certificate, clicking the 'Back to wizard' page results in an error.
- A pinned application gets automatically unpinned after you search for it.
- 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.

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