SEQRITE
Enterprise Security Solutions by Quick Heal

Seqrite HawkkProtect 1.0.3 GA

Release Notes

28 April 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.

Dedicated Visibility Tab

- Create user and application hierarchy and view real-time connection flow between the users, applications/services across your organizational IT infrastructure.
- Generate graphic presentation of user and connection statistics for all application services.
- View complete details for connection between users and applications/ services such as detection time for attempted connections, source IP address, destination IP address, user details, and applications/ services details. View status for policies applied to users.

Tag Management

- Create static tags using key and value pairs and assign them to users and applications.
- Create dynamic tags using attributes fetched from IdP/ application parameters. These tags are assigned to the users and applications automatically.
- Granular and custom policy rules can be created using tags.

Effective Policy Management

- Create explicit allow policy rules using user and application tags for granting enterprise application access only to required users.
- Create policies with Observe mode ON to monitor specific connection attempts.

Other features

- IdP management: Identity Providers (IdP) are used to manage users and access privileges in organizations.
- Site management: Site is the gateway which is automatically deployed on Seqrite AWS cloud account. You can configure it by choosing appropriate IdP and Certificate details.
- Application catalog: A list of organizational applications and services to which connections are attempted.
- App connector management: App connectors allow the user to safely access private organizational applications and lets you integrate on-premise AD without the use of VPN.

Known Issues

Some of the important known issues in version 1.0.3 are as follows.

- User portal SAML logout with google IDP is not working.
- Admin portal is not supported on Safari browser for HawkkProtect v1.0 release.
- In RDP application, user is able to access all the applications from the file explorer option.
- Work around: The administrator can use AD 2016 options on the UI to configure AD 2019 as an IDP.
- If Entity ID and Reply URL are modified from the UI, reauthorization does not work for Google workspace IdP.
- Names of policies, certificates, and applications is appearing in lowercase across few pages.
- For all the IdPs, if users are deleted, the policy access rules related to the user are not getting removed from HawkkProtect.
- In globe view, incorrect user location might be visible sometimes.
- 'Incorrect username/ password' error is displayed for users for whom Administrator has selected 'user must change password at next logon' option in On-premise AD.
- The relative URL path is not appended to the URL if a user directly accesses the application instead of accessing it via user portal.
- 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.

  Workaround: The user must wait for one minute. After one minute, the user can relaunch the application from the application portal.
- CPU utilization of the client machine is very high when tried to load the connections on the visibility page.

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