

SEQRITE
HawkkProtect
2.1
Release Notes

20 October 2023

Copyright Information

Copyright © 2023 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India. Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

SEQRITE is a registered trademark of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of licenses to SEQRITE HawkkProtect is subject to end users' unconditional acceptance of the SEQRITE End User License Agreement, which is available at <https://www.seqrите.com/eula>.

Contents

Introducing SEQRITE HawkkProtect	2
What's New	3
Agent-Based App Enhancements.....	3
App Connector Enhancements	3
HawkkAgent Enhancements	4
Device Posture - HawkkScan Risk Score Utilization	4
Enhanced Security with a Forced Logout Feature	4
Download session recordings with ease.....	4
User Portal Idle Session Timeout Configuration	5
Enhanced Security with Two-Factor Authentication (2FA)	5
Enhanced Firewall and DDoS User Experience	5
Expanded Integration for SaaS Applications.....	5
Known Issues	6
Technical Support	7

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.

Agent-Based App Enhancements

- **Enhanced Configuration with Multiport-Protocol Support**
HawkkProtect Administrators now have the provision to associate multiple port-protocol combinations with a single IP/domain entry, expanding configuration options beyond the previous domain-IP setup and single port setup.
- **Auto-Connect**
Users can now enjoy the convenience of automatic application connection establishment upon successful end-user authentication, simplifying the overall user experience.
- **Lock Port Value**
Users now directly connect to the specifically configured port within the application, ensuring consistent and secure access. Previously, without the Lock Port Value configuration, users might have connected to a random port, which was internally redirected to the application's designated port.
- **Secure Access Configuration for Internal Redirects**
Now, with the latest update, the application accessible through the parent domain can be internally redirected to another domain. These internal redirects, previously inaccessible through the HawkkAgent, can now be seamlessly accessed.
- **Relative Path URL Support**
Added support for relative path URLs within agent-based applications.
- **Hide the Auto-Connect Agent-Based Apps in the User Portal**
Simplify the user experience by concealing the applications for which the Auto-Connect option is enabled within the user portal.
Note: This should be enabled for advanced users.

App Connector Enhancements

- **Enhanced Connectivity Testing**
Administrators can now conveniently verify the accessibility of the configured private or agent-based application from the designated app connector group, ensuring seamless connectivity.

- **Improved Active/Passive App Connector Visibility**

Gain valuable insights into the dynamic status of app connectors within a high-availability app connector group. Easily identify the actively serving app connections, empowering administrators with real-time information for efficient management.

- **App Connector Active/Passive State Notifications**

Administrators can opt to receive notifications when the app connector's state changes.

- **Enhanced App Connector Upgrade Retry**

Enabling improved mechanism for retrying app connector upgrades.

HawkkAgent Enhancements

- **Call to Action Button (CTA) in HawkkAgent Screen**

Introducing a call-to-action button on the HawkkAgent screen for improved user engagement.

- **HawkkAgent to Site Connection Status Indication on the HawkkAgent Screen**

- Connected to HawkkAgent: the HawkkProtect Agent Service is operational; however, it has not yet connected to the site.
- Connected to the Site: The agent is linked to the site.

Device Posture - HawkkScan Risk Score Utilization

Administrators now have the option to activate or deactivate an agent-based application on the risk score provided by the HawkkScan agent.

Note: This feature will be available with a valid HawkkScan license.

Enhanced Security with a Forced Logout Feature

Multiple active user sessions are terminated simultaneously, and administrators can permanently block user access through policy configuration or by disabling/deleting the user. All revocation activities are logged in the audit trail.

Download session recordings with ease

Empower administrators to download and store session recordings on their local storage, ensuring data control and easy accessibility for extended periods.

User Portal Idle Session Timeout Configuration

HawkkProtect administrators can configure session timeout intervals for the user portal at the tenant level, allowing flexibility for administrators to set their preferred duration. The idle session timeout functionality ensures automatic logout after the specified period of inactivity (default 30 mins) while enabling users to re-login. The configurable duration ranges from 5 minutes to 1440 minutes (24 hours) for enhanced customization.

Enhanced Security with Two-Factor Authentication (2FA)

Introducing an additional layer of security with the support for Two-Factor Authentication (2FA) implementation for on-prem IdP.

Enhanced Firewall and DDoS User Experience

Providing improved user experience for firewall and DDoS functionalities with updated user interface elements.

Expanded Integration for SaaS Applications

Seamlessly integrating Salesforce, Dropbox, Atlassian, and Slack allows for a more streamlined and user-friendly workflow for users.

Known Issues

Here are the known issues in version 2.1:

- Failure to download session recording video upon the machine transitioning from an extended sleep mode or shutdown state to an online state.
- Changing the status of the HawkProtect Agent from enable to disable does not promptly result in the blocking of SaaS applications; for the changes to take effect, it is necessary to initiate a fresh login.

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.segrite.com/segrite-support-center>