Seqrite Data Privacy

SEQRITE

Release Notes

v2.3 | 30 Jan 2025

www.seqrite.com

Copyright Information

Trademarks

License Terms

Contents

What's New

Seqrite Data Privacy 2.3 includes the following new features and enhancements

Seqrite Data Privacy integration with ServiceNow

Version 2.3 integrates Seqrite Data Privacy with ServiceNow, which enables administrators to automatically create incidents in ServiceNow for predefined critical events detected in the console.

Displaying the scan results in plain text format

Data Protection Officers (DPOs) can now view discovered Personally Identifiable Information (PII) and Personal Data (PD) in plain text format. Previously displayed in an obfuscated manner, this enhancement provides DPOs with clearer visibility into the discovered data, enabling more accurate assessments and streamlined decision-making for compliance and data privacy management.

Enhanced Compliance Dashboard User Experience

The Compliance Dashboard is now renamed simply as 'Dashboard' that offers enhanced insights. In accordance to the Data Compliance tag key, the users now can visualize dashboards for other tag keys such as Data Sensitivity and Impacted Areas. Upon selecting the tag key, it provides an overview dashlet with consolidated data metrics. To view the details, the users have a drill down option available.

This improvement enhances the data visibility with simplified dashboard navigations and makes the user experience more versatile.

Microsoft Access Data Source Connector Integration

Seqrite Data Privacy v2.3 introduces Microsoft Access as a new data source connector. The Data Source Administrators can now add Microsoft Access instances under the available connectors to discover and classify the data stored in the application.

Email Notification Enhancements for Data Privacy Workflows

This feature enhances the workflow efficiency of the email notifications. This mechanism differs based on the deployment model:

- **Cloud Edition**: Utilizes built-in SMTP details.
- **On-Premise Edition**: Uses customer-configured SMTP details.

The key functionalities are:

Events Triggering Email Notifications

- When a Data Subject Request is created, the email notifications are sent to-
  - Data Source Owner
  - Business Owner
  - Approver
- When an Assessment is created, the email notifications are sent to
  - Owner
  - Participant
  - Approver
  - Respondent

Reminder Notifications: Emails are sent 5 days prior to the due date of the task to ensure apt actions.

Personalized Email Content: The email body is now customized based on the recipient's role (e.g., Owner, Participant, Approver), ensuring relevance and precision.

Branding and Professionalism: Email templates obey to the platform's branding guidelines to maintain utmost professionalism.

Content Inspection for Document Uploads

To enhance security within the Data Privacy Management Console, secure file uploads are now enabled with real-time content inspection. This feature ensures that uploaded files are free from malicious content or violations, safeguarding the system and its users.

Key Highlights

1. **Applicable Workflows:**
   - Classifiers (post-classification function)
   - Data Subject Requests (DSR)
   - Assessments
2. **Content Scanning:**
   - Files are scanned for potential threats such as viruses, malware, or other harmful elements.
   - Inspection outcomes include a clear verdict: **Allow** or **Block**.

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