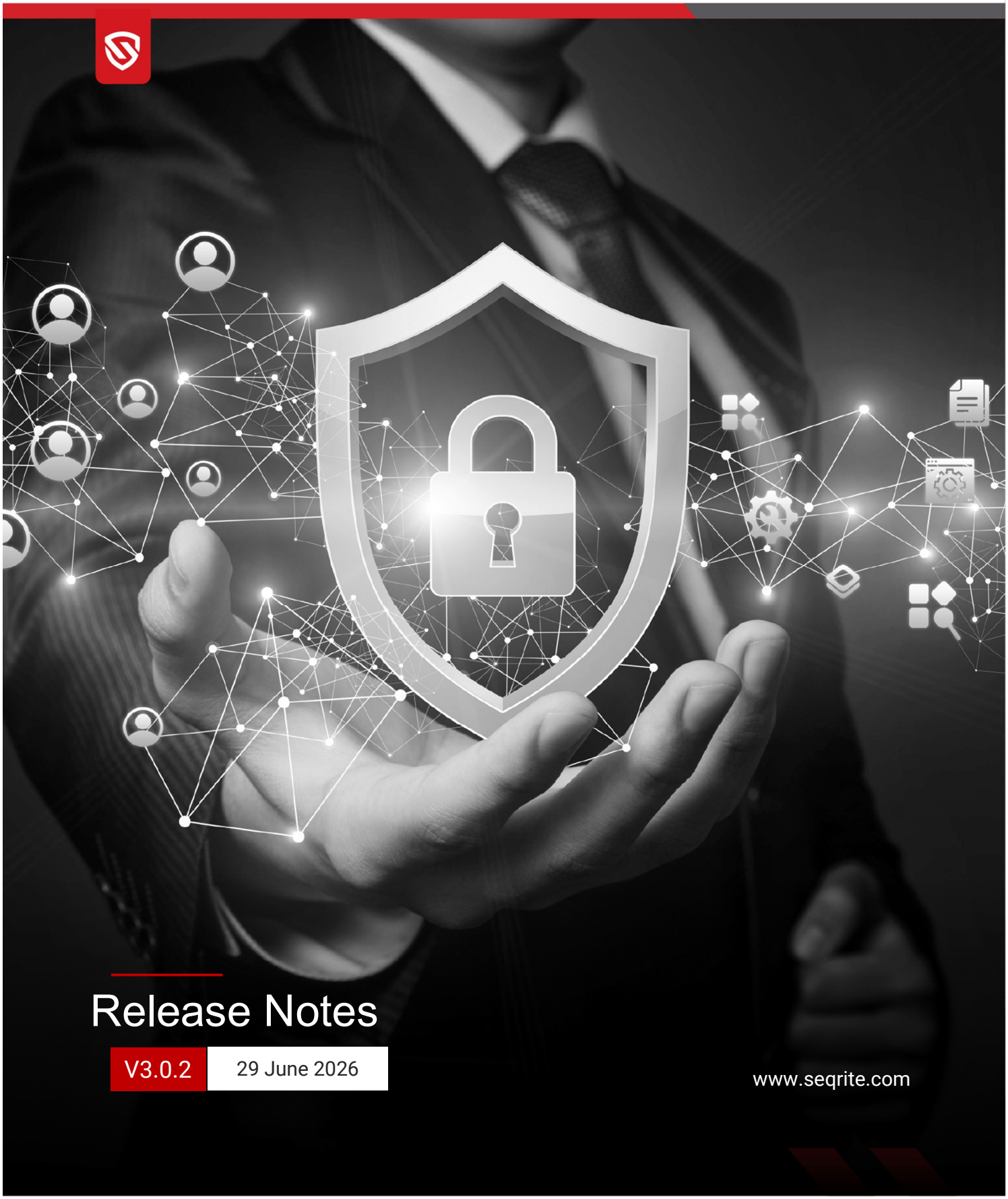
Seqrite Data Privacy

SEQRITE



Release Notes

V3.0.2

29 June 2026

www.seqrite.com

Copyright Information

Trademarks

License Terms

Contents

What's New

Seqrite Data Privacy 3.0.2 includes the following features and enhancements.

Features

- **Introduced Purpose Code Field**
  A new optional **Purpose Code** field has been introduced when creating a purpose. Previously, purposes in SDP were identified only by their name. This field enables organizations to associate standardized purpose codes with their purpose definitions, enabling better alignment with industry standards and regulatory frameworks.

- **Consent Management - Device Details and IP Address Capture**
  Seqrite Date Privacy now automatically captures **device details** and the **IP address** of the data principal at the time of consent submission. This information is stored as part of the consent record, enhancing audit trail capabilities and regulatory compliance.

  Details Captured are:
  - Operating System (For example, Windows 10)
  - Architecture (For example, x64)
  - Browser name and version (For example, Chrome 147)
  - Device type (For example, Desktop)
  - IP Address

- **Consent Management - Tamper-Proof Consent Collection**

  The consent collection process is now secured end-to-end with a tamper-proofing mechanism. While consent records in the database were already immutable, this enhancement ensures that the entire life cycle from serving the consent form to capturing and transmitting the consent payload is protected against tampering**.**

- **Custom Attributes in Consent Record**
  Users can now store custom attributes for individual consent records in the consent database, enabling customer-specific fields to be associated with each record.

- **Consent Management - Consent Mapping with Multiple Purposes**
  Users can now map a single consent statement to multiple purposes, making consent management workflows more flexible and allowing them to create one consent table that covers several purposes.

Enhancements

- **ISO 8601 Format for Timestamps in Consent Record**

  Timestamps in Consent Records are now stored in the internationally recognized ISO 8601 format. This enhancement ensures consistency, interoperability, and compliance with industry requirements.

- **SSO Enhancement for Certificate Management**
    - Seqrite now handles SSO certificate management instead of relying on the customer's own console certificate for SSO authentication.
    - Service certificates are now generated with a 5-year validity period. Seqrite Data Privacy Admins can regenerate certificates on demand, either at expiry or whenever certificate rotation is required. After regeneration, updated SP metadata and public certificate must be uploaded to the IdP to ensure continued authentication.

- **Encryption of Consent Payload**

  The payload generated by the consent form is now encrypted, ensuring secure handling and transmission of consent data.

- **Authenticated API for Consent Management**
  The consent management API is now an authenticated API, triggered through the customer's backend. This ensures better security by preventing tampering of consent data from the client side.

- **API for Additional Data Principal ID**
  Added a new REST API endpoint that allows authorized systems to append additional data principal IDs to an existing consent record after it has been created and stored in the consent database.

- **New Fields in Consent Artifact**
  The following new fields are now captured in the Consent Record and included in the consent webhook payload to meet regulatory requirements (For example, IIB):
    - **Lawful Basis**: This field will fetch and utilise the Lawful Basis associated with the purpose which is currently being captured on the purpose creation screen.
    - **Language Code (ISO 639-3)**: This field will store the language in which the data principal submitted the consent. It will utilise the ISO 639-3 format for capturing language code (For example, **eng** for **English**).
    - **Consent Form Name**: The name of the Consent Form used during submission is now stored in the consent record and included in the webhook payload.
    - **Consent Form Version ID**: The version ID of the published Consent Form used at the time of submission is now captured and passed via webhook**.**

- **Assessment Enhancement UI Improvement**
  Enhanced the assessment interface with UI refinements for improved usability, providing a smoother and more intuitive experience when managing assessments.

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