Release Notes

Privitar Data Security Platform, version 1.5.3

Publication date November 3, 2023

Privitar Data Security Platform, version 1.5.3

Table of Contents

Welcome

Welcome to the release notes for the Privitar Data Security Platform. This document describes:

1. Product Documentation

To learn more about all the features discussed in these release notes, please refer to the product documentation at https://docs.privitar.com.

2. New Features in This Release

Integrations

Your organization can use the Privitar SDK to embed Privitar policy enforcement into a variety of tools. The Privitar SDK is a Java library that facilitates the interaction with Privitar's control plane and the enforcement of policies within an application. To date, we have seen customer integrations with the following:

- Apache Kafka Connect
- Apache NiFi
- AWS Lambda functions
- Azure Functions
- DataBricks
- Delta Lake
- Informatica
- Google BigQuery
- Snowflake

There are more integrations planned for subsequent releases.

Data Proxy Compatibility

- Added support for Delta Lake 2.4.x running in Spark 3.4.x
- Added ability to provide an external correlation ID for data proxy connections and queries.

  To learn more see Allow External Configuration of Correlation ID Queries in the DSP Installation and Administration Guide.
- Added compatibility with the data proxy for Denodo's Presto database adapter when used with a Trino data proxy data source for the following Denodo VQL functions:

```
abs, avg, avg, cast, ceil, coalesce, countcount, exp, floor, instr, ln,
lower, max, min, mod, nullif, position, power, sqrt, stdev, stdevp, substr/
substring, sum, trim, upper
```

3. Known Issues and Limitations

Asset Registration

- Names are case-sensitive when registering an asset, schema, or table.
- If you change a previously registered asset (such as changing the data type of a field), when subsequently updating the asset on the platform, the change will not appear. However, if you update the asset a second time, the change will appear, allowing you to modify the asset on the platform.

Business Information

- You cannot edit or remove any data classes, terms, or tags that are in use.

Datasets and Assets

- Only an exchange administrator or the dataset owner (creator) may modify or delete a dataset.
- If the dataset membership is restricted, only an exchange administrator, a member of the dataset, or the dataset owner (creator) may register, modify, or delete an asset within the specified dataset.
- When registering an asset, the platform interprets Boolean data types as integer data types.

Dynamic Query Access (Data Proxy)

- If there is an error when authenticating a connection, the error message may not contain enough information to indicate the exact cause of the problem. Please validate the connection URL, credentials, and TrustStore certificate are correct.

Nested LDAP Groups

- You must explicitly add all LDAP user groups and give them a role on the platform. This includes all nested groups.

Policies and Rules

- Upon deployment of the platform, we recommend that you immediately configure the behavior of access control rules to allow or deny access. If however, you wish to change this behavior at a later stage, you must delete all access control rules prior to making this change.
- The platform does not support Boolean data types and interprets them as integer data types upon asset registration. Therefore, you may only use the transformation types of Retain, Drop, and Redact with Null when accessing these data types. You may not use cell-level transformations nor access control policies with these data types.

Projects

- Only an exchange administrator or the project owner (creator) may modify, delete, add assets to, or remove assets from a project.
- When searching for users and user groups to add as members of a project or dataset, the search returns all enterprise users and user groups, including those who may not have access to the data exchange. The platform performs against the internal registry or the LDAP registry.
- If a user who is not a member of a project attempts to query data in it, the platform may return a generic error that does not inform the user that they are not authorized to access the data.
- When a project owner edits a published project, the project moves to *In Draft* status, preventing data consumers from being able to consume data until a data guardian re-approves the project.
- When editing a rejected project, a data consumer can remove all but one asset. A rejected project requires at least one asset so a data consumer can re-submit it for approval.

REST APIs

- When a data owner uses the REST API to create a new asset, the platform creates the asset in *In Draft* status, and a data guardian must approve it.
- If you have an LDAP group with no users, the User Group API will return an error message.
- Only an exchange administrator or the project owner (creator) may modify, delete, add assets to, or remove assets from a project.
- Only an exchange administrator or the dataset owner (creator) may modify or delete a dataset.
- Only an exchange administrator, a member of the dataset, or the dataset owner (creator) may register, modify, or delete an asset within the specified dataset.

Upgrading

- If you already have LDAP configured to work with the platform, when upgrading from DSP v1.4.0 to DSP v1.5.1, set `upgradeKeycloakFrom140` to `true` in the `control-plane-values.yaml` file as follows:

```
## Flag to patch ldap deployed 1.4.0 to 1.5.0
upgradeKeycloakFrom140: true
```

User Role Assignment

- When changing the user role assignment of a user or group, it may take a few moments for the change to take effect. You should log in to the platform again for the changed role assignment to take effect.

4. Compatibility

The Privitar Data Security Platform is compatible with the following component versions:

- Helm v3.8.x
- Kubernetes v1.25

  Note that for Kubernetes components, the version difference between client (1.xx) and server (1.xx) shouldn't exceed the supported minor version skew of +/-1. To learn more, see https://kubernetes.io/releases/version-skew-policy/.

Note that Istio requires port 15017 in order to inject a configuration into Keycloak and RabbitMQ.

Data Proxy Data Sources

- Apache Hive v3.1.2+
- Apache Spark v3.0.1+
- Delta Lake 2.4.x on Spark 3.4.x
- PostgreSQL v13.0+

Denodo v8.x Database Adapters

- Hive Server 2 with Apache Hive v3.1.2+ as a data proxy data source
- Spark SQL 2.x with the following data proxy data sources:
  - Apache Spark v3.0.1+
  - Delta Lake 2.4.x on Spark 3.4.x
- Google BigQuery with Google BigQuery data proxy data source
- Presto with Trino v420 as a data proxy data source