PRIVITAR

Release Notes

Privitar Data Security Platform, version 2.1.0

Publication date December 13, 2023

Privitar Data Security Platform, version 2.1.0

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Table of Contents

Welcome

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

- Product Documentation
- New Features in This Release
- Known Issues and Limitations
- Compatibility

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

Custom Attributes

- Exchange administrators can now create custom attributes that apply to assets, fields, and requests through the `POST/api/v1/attributes` REST API endpoint.
- Data guardians can now select these new attributes in the the platform user interface (UI) and through a REST API when they create policy triggers and rule conditions.
- Data owners can now set the values for these custom attributes in the the platform user interface (UI) and through the `PUT/api/v1/attributes` REST API endpoint when they register assets.

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.

3. Known Issues and Limitations

Audit Logs

- In this release, you can only view logged policy resolution events in the the platform user interface (UI). Other event types will be available in the UI in future releases. Note that you can route all event types to your security information and event management (SIEM) tool.
- Policy resolution events record whether or not the policies were applied to the query. They do not record the final state of the query. For the latter, review the query log from your query tool.

Business Information

- You cannot edit or remove any data classes, terms, or tags that are in use.
- You cannot edit or remove any custom attribute values that are in use.
- You cannot remove any custom attribute types that are in use.
- You cannot edit the object type of an existing custom attribute. For example, if you originally created a custom attribute for a field, you cannot edit the custom attribute to also apply it to an asset.
- In the platform user interface (UI), you cannot edit custom attributes that require you to enter a value. You can only edit them through the `PUT/api/v1/attributes` REST API endpoint.
- When creating a new custom attribute type through the `POST/api/v1/attributes` REST API endpoint, you must include the set of object types to which the custom attribute will be applied. The list of valid object types are: "ASSET," "FIELD," and "DESTINATION_OBJECT." These case-sensitive entries must be uppercase. The following is an example:

```
   "validContainingObjectTypes":
[      "DESTINATION_ENVIRONMENT", "ASSET", "FIELD"    ]
```

Datasets and Assets

- Only the dataset owner or members of the dataset may register assets or update assets of a dataset.
- You may update masked assets, however the policy for applying privacy enhancing techniques (masking) will not be updated and re-applied to the asset. Hence, new or changed fields may not be protected as expected.
- 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.
- 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.

Installation

- When upgrading the Privitar Data Security Platform (DSP), you must upgrade both the control plane and the data plane to the same version.
- When installing the platform, ensure that you use a valid email address as the administrator username. Keycloak now requires that the administrator username is an email address.

General

- You must explicitly add all LDAP user groups and give them a role on the platform. This includes all nested groups.
- Under certain conditions, using monitors that have a resolution greater than 2,000px wide, action buttons do not display correctly. Hover over the buttons to view a tooltip.

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.

Consumption Projects

- Only an exchange administrator or the project owner (creator) may modify, delete, add assets to, or remove assets from a consumption project.
- When searching for users and user groups to add as members of a consumption 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 consumption 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 consumption 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 consumption project.
- When editing a rejected consumption 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.

Migration Projects

- After a data guardian has approved a migration project, the platform will not apply any subsequent policy or rule changes to the masked assets in that project. If you need to implement such a change, you will need to create a new migration project.
- You may not reuse a connection that you previously used with another migration project.
- You may not edit or delete a published migration project.
- The platform ensures that you only select and include raw assets within a migration project. Masked assets cannot be masked again, nor can they be added to a migration project.
- Use only consistent numeric or text regular expression transformation types for data that you wish to allow a data consumer to reverse to its original value, according to their request and applicable policy. Other transformation types (such as Constant Text Value or Date Generalization) will not allow data to be reversed. The platform will return other transformation types in their transformed form, rather than the original values. For example, if Constant Text Value is the applied transformation type, the platform will return the constant text.

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.
- Project APIs only support consumption projects.

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