

Collibra Data Intelligence Cloud

# Collibra Protect

Collibra Data Intelligence CloudCollibra Data Governance Center - Collibra Protect

Release date: Thursday, January 5, 2023

Revision date: Thu Jan 05, 2023

You can find the most up-to-date technical documentation on our Documentation Center at  
[https://productresources.collibra.com/docs/collibra/latest/Content/to\\_collibra-protect.htm](https://productresources.collibra.com/docs/collibra/latest/Content/to_collibra-protect.htm)

# Contents

Contents .....	ii
About Collibra Protect .....	i
Install Collibra Protect .....	ii
Configure Collibra Protect .....	iv
Essentials for Collibra Protect .....	ix
Overview of Collibra Protect .....	xvii
Data protection standards .....	xix
Data access rules .....	xxv
Data source policies .....	xxxiii
Groups .....	xxxv
Audit .....	xxxvii
Why rules or standards fail .....	xxxix
Reference .....	xlviii
Collibra Protect .....	lviii
About Collibra Protect .....	i
Install Collibra Protect .....	ii
Configure Collibra Protect .....	iv
Essentials for Collibra Protect .....	ix
Overview of Collibra Protect .....	xvii
Data protection standards .....	xix
Data access rules .....	xxv
Data source policies .....	xxxiii
Groups .....	xxxv



Audit .....	xxxvii
Why rules or standards fail .....	xxxix
Reference .....	xlvi

## About Collibra Protect

Collibra Protect is a capability of the Data Intelligence Cloud created to protect sensitive data and make it available, or partially available, to specified groups of users.

Collibra Protect solves the problem of protecting sensitive data in an organization. Different groups of people may need varying access levels to the same data set. With Collibra Protect, access rules and data protection standard capabilities allow you to grant access to individuals and protect sensitive information. These rules and standards with different data access levels are managed through the Collibra platform and pushed to the data source. Our aim is to promote a safe data-open culture in organizations.

The goal of Collibra Protect is to centralize and simplify access governance and remove the need of repetitive action and approval. Data access and privacy management promotes an ethical company standard giving permission to view information only to those that need it. Collibra Protect allows you to perform these actions accordingly.

An example use case of Collibra Protect is a data steward giving everyone access to a data set, but only allowing certain access to groups of people based on data categories. This is known as differential access. It is suggested that rules/standards are grouped together, for example by business processes, so you do not have to make a rule or standard for every data set.



# Install Collibra Protect

This procedure guides you through a first time installation of Collibra Protect.

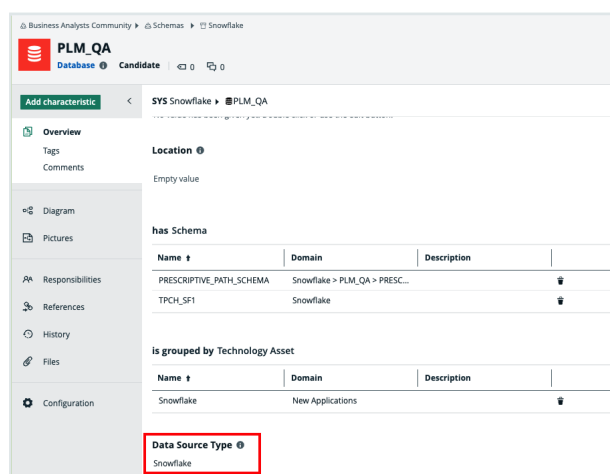
## Prerequisites

You must add the [Snowflake capability on Edge](#) as well as perform a catalog ingestion.

Configure the Collibra Protect for Snowflake capability on Edge. Settings → (Edge) Sites → Your site → Capability → Add capability → fill in the needed parameters:

- For "Capability template" choose "Collibra Protect for Snowflake".
- The "Snowflake Connection" can be the same connection used for doing catalog ingestion. Make sure that the Snowflake user/role has enough permissions to create/alter/drop grants, tags, etc.

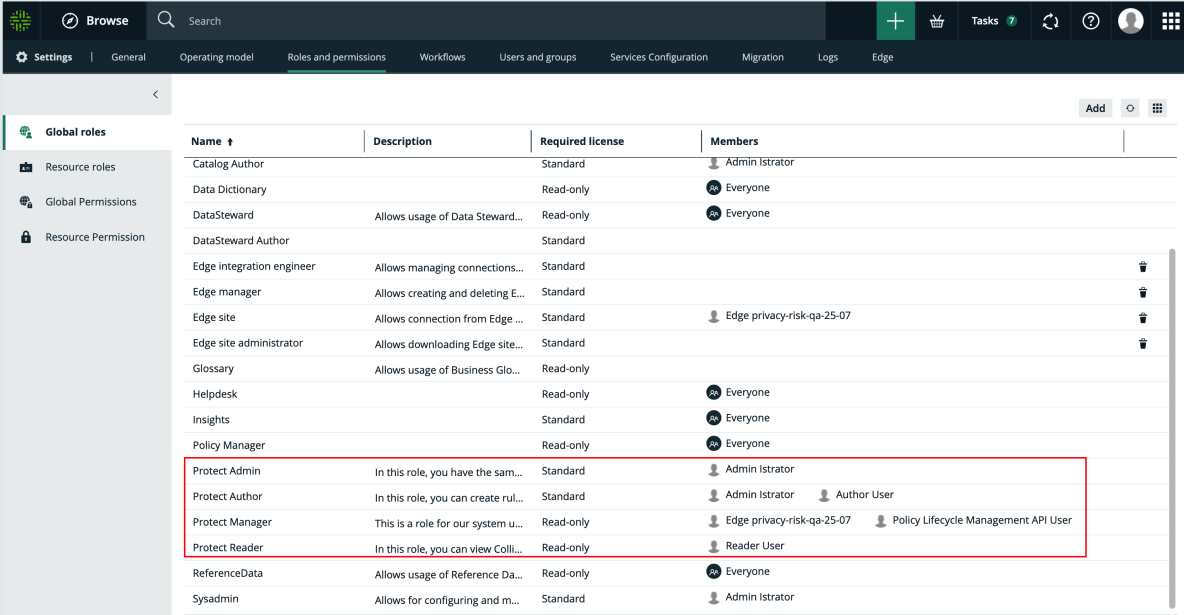
An ingested Snowflake database should look like the example below.




**Note** The Data Source Type attribute on the database asset should be present. This attribute is automatically added in database assets, after the catalog ingestion process.

## Steps

1. Contact a Collibra support or your representative to enable Collibra Protect on your Collibra environment.
2. Ensure [global roles and permissions](#) for Collibra Protect are set correctly.



Name	Description	Required license	Members
Catalog Author		Standard	Admin Istrator
Data Dictionary		Read-only	Everyone
DataSteward	Allows usage of Data Steward...	Read-only	Everyone
DataSteward Author		Standard	
Edge integration engineer	Allows managing connections...	Standard	
Edge manager	Allows creating and deleting E...	Standard	
Edge site	Allows connection from Edge ...	Standard	Edge privacy-risk-qa-25-07
Edge site administrator	Allows downloading Edge site...	Standard	
Glossary	Allows usage of Business Glo...	Read-only	
Helpdesk		Read-only	Everyone
Insights		Standard	Everyone
Policy Manager		Read-only	Everyone
Protect Admin	In this role, you have the sam...	Standard	Admin Istrator
Protect Author	In this role, you can create rul...	Standard	Admin Istrator, Author User
Protect Manager	This is a role for our system u...	Read-only	Edge privacy-risk-qa-25-07, Policy Lifecycle Management API User
Protect Reader	In this role, you can view Coll...	Read-only	Reader User
ReferenceData	Allows usage of Reference Da...	Read-only	Everyone
Sysadmin	Allows for configuring and m...	Standard	Admin Istrator

3. Collibra Protect is installed.
  - » You can now access and start using Collibra Protect via the  menu.

# Configure Collibra Protect

Configuring within Collibra Protect is an important part of understanding and using Collibra Protect to its highest ability.


## Prerequisites

- You need to have Data Catalog permissions. If not, you cannot see any classification in either standards or rules.
- You need to have a Data Steward role within Collibra. If not, you cannot see the classification page when selecting a classification in Collibra Protect.



## Roles in Collibra Protect

It is possible to assign different roles to Collibra users that use Collibra Protect. The roles are provided and have pre-defined permissions that restrict the usage of the application.

Roles	Description
Protect Reader	Users in this role can view Collibra Protect with read-only access to the content. This role is assigned to 'Everyone' and grants the users the 'protect' permission. Without this permission, users cannot see 'Protect' as an application in the  menu. They also cannot navigate to protect related URLs or access protect endpoints.
Protect Author	Users in this role can create <a href="#">rules</a> and <a href="#">standards</a> , view <a href="#">imported policies</a> and <a href="#">groups</a> , and generate <a href="#">audits</a> as an individual contributor. This role grants the product right permission 'protect' and the 'protect_edit' permission. Authors can only modify rules and standards they own. This role is not assigned to anyone automatically.
Protect Admin	Users in this role have the same permissions as the Protect Author role as well as the ability to edit other user's rules and standards. This role grants the product right permission 'protect', 'protect_edit', and an extra 'protect_administration' permission. This role is not assigned to anyone automatically.
Protect Manager	This role is restricted to our system user to manage background processes and setup configurations for Collibra Protect and it should not be assigned to other Collibra users.

## Configure groups

Before you start working in Collibra Protect, you need to configure your groups. Collibra Protect groups are the basis of all the actions performed in Collibra Protect.

## Associate a Protect group with Snowflake

Each Snowflake user is assigned to one or more Snowflake roles. Permissions are based on these roles. View the example below of the roles page in Snowflake. Any/all roles can be correlated to a Collibra Protect group.

Role	Creation Time	Owner	Comment
ACCOUNTADMIN	9/18/2019, 1:47:25 ...		Account administrator can manage all aspects of the account.
ANTONIO	6/27/2022, 10:10:4...	SBI_TEMPLATE_SN...	
BILLING	6/2/2022, 4:07:43 ...	ACCOUNTADMIN	
CERTIFICATION	4/15/2020, 2:12:24 ...	ACCOUNTADMIN	
CUSTOMER_SERVICE	6/2/2022, 4:05:29 ...	ACCOUNTADMIN	
DATALIFT_ROLE	5/6/2020, 9:56:54 ...	ACCOUNTADMIN	
Direct Marketing	6/27/2022, 10:12:4...	SBI_TEMPLATE_SN...	
FIVETRAN_ROLE	1/27/2022, 10:27:58...	SECURITYADMIN	
GLOBAL_PS	9/27/2021, 2:36:19 ...	ACCOUNTADMIN	
HR	10/22/2021, 1:38:44...	ACCOUNTADMIN	
LAW	3/3/2022, 9:00:27 ...	ACCOUNTADMIN	
MARKETING	9/29/2021, 1:59:26 ...	ACCOUNTADMIN	
MARKETING2	9/29/2021, 2:36:17 ...	ACCOUNTADMIN	
MARKETING3	9/30/2021, 3:56:47 ...	ACCOUNTADMIN	
PC_DBT_ROLE	5/6/2022, 9:08:33 ...	ACCOUNTADMIN	System created role for partner elt integration.
PLM	10/22/2021, 1:30:58...	ACCOUNTADMIN	
PLM_QA_HR	2/24/2022, 3:38:20...	ACCOUNTADMIN	PLM QA HR Read Only Role

## How to create Collibra Protect groups?

When you initially go to the **Groups** tab in Collibra Protect, there are no groups created. There is a link at the top of the page to the Groups API that creates new groups in Collibra Protect. Use this API link to create new groups and associate it with a specific role in Snowflake.

## Groups

Adding Groups  
 To add a group, you have to use the [Collibra Protect Group API](#). Currently, only Snowflake data sources are supported.

Group Name	System Reference	Created By	Created Date
------------	------------------	------------	--------------

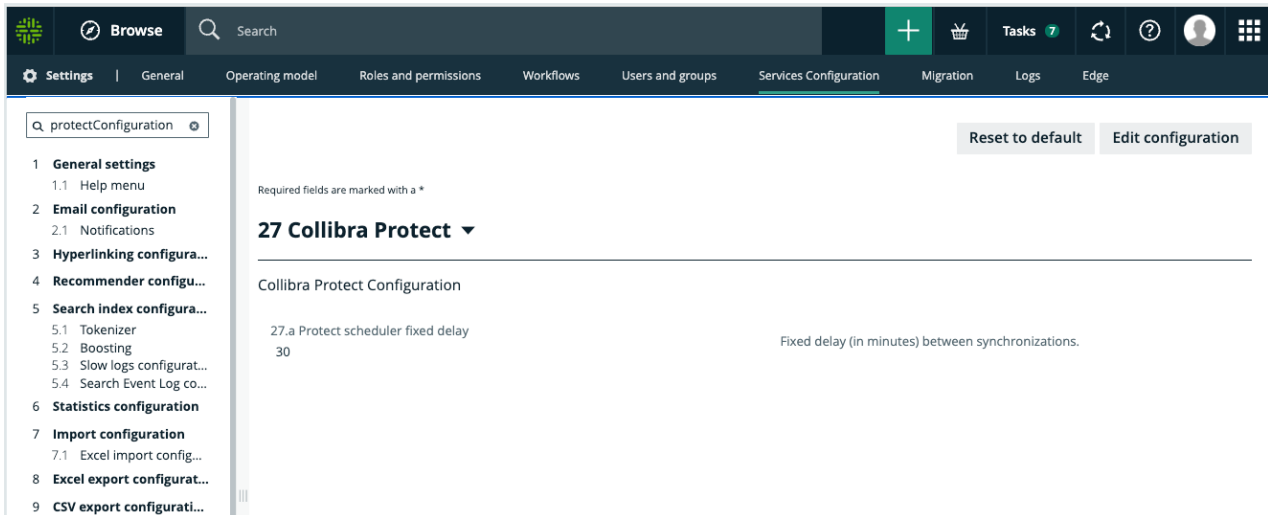
  

The screenshot shows the Snowflake web interface. At the top, there's a navigation bar with icons for Databases, Shares, Marketplace, Warehouses, Worksheets, History, and Account. Below this, a toolbar contains buttons for Run, All Queries, and Saved 10 seconds ago. The main query editor shows the command 'SHOW roles;'. Below the editor, the 'Results' tab is active, displaying a table with 37 rows. The table has columns: Row, created\_on, name, is\_default, is\_current, is\_inherited, assigned\_to\_users, granted\_to\_roles, granted\_roles, owner, and comment. The data lists various roles like ACCOUNTADMIN, ANTONIO, BILLING, CERTIFICATION, CUSTOMER\_SERVICE, DATALIFT\_ROLE, Direct Marketing, FIVETRAN\_ROLE, GLOBAL\_PS, HR, LAW, and MARKETING.

Row	created_on	name	is_default	is_current	is_inherited	assigned_to_users	granted_to_roles	granted_roles	owner	comment
1	2019-09-17 16:47:2...	ACCOUNTADMIN	N	Y	N	35	0	3		Account administrat...
2	2022-06-27 01:10:4...	ANTONIO	N	N	N	1	1	0	SBL_TEMPLATE_SN...	
3	2022-06-02 07:07:...	BILLING	N	N	N	1	0	0	ACCOUNTADMIN	
4	2020-04-15 05:12:2...	CERTIFICATION	N	N	Y	1	1	0	ACCOUNTADMIN	
5	2022-06-02 07:05:...	CUSTOMER_SERVICE	N	N	N	1	0	0	ACCOUNTADMIN	
6	2020-05-06 00:56:...	DATALIFT_ROLE	N	N	Y	1	2	0	ACCOUNTADMIN	
7	2022-06-27 01:12:4...	Direct Marketing	N	N	N	1	0	1	SBL_TEMPLATE_SN...	
8	2022-01-27 13:27:5...	FIVETRAN_ROLE	N	N	Y	3	1	0	SECURITYADMIN	
9	2021-09-27 05:36:1...	GLOBAL_PS	N	N	N	1	0	0	ACCOUNTADMIN	
10	2021-10-22 04:38:4...	HR	N	N	Y	10	1	0	ACCOUNTADMIN	
11	2022-03-03 00:00:...	LAW	N	N	N	0	0	0	ACCOUNTADMIN	
12	2021-09-29 04:59:...	MARKETING	N	N	Y	11	1	0	ACCOUNTADMIN	

## General configuration

Collibra Protect synchronizes standards and rules with the source database(s) at regular intervals. This synchronization runs in the background on a configured frequency. By default, the frequency is every 60 minutes, but this is configurable through Settings → Services Configuration → 27 Collibra Protect.



**Important** If you do not have access to the **Service Configuration** tab, create a support ticket requesting the JVM Parameter be added to your Collibra Infrastructure Configuration: `-DPROTECT_SYNC_SCHEDULER_DELAY=PT60M`. After the parameter is added, restart Collibra so these changes take effect and the policies are now synchronized with the cloud provider.

Synchronization includes:

1. Aggregate all standards and rules computing:
  - which columns need to be masked for which groups.
  - which tables need to have a row filter.
  - which tables and columns need to be granted access.
2. On the source database(s) such as Snowflake:
  - create and apply maskings.
  - create and apply row filters.
  - grant access to groups on tables and/or columns (depending on the underlying database).

# Essentials for Collibra Protect

To use Collibra Protect to the best of its ability, you need to know the following things:

- [How to protect your data](#)
- [Technical background](#)
- [Data protection standards vs. data access rules](#)
- [Prescriptive paths](#)



# How to protect your data

## 1. Access management

The most basic line of protection is to make sure only the right people/groups have access to the data. Data here is referring to the tables and columns in your database. In Collibra Protect, you can grant specific groups access to parts of your data based on Collibra assets.

For example, it is easy to grant the HR team access to the US customers' data set. But, what if some parts of the US customers' data set need to be hidden from the HR team, because it contains restricted information, such as personally identifiable information (PII)? In that case, you can further protect your data by applying column-based protection or row-based protection.

**Note** Collibra Protect only grants access. It cannot revoke access from people/groups.

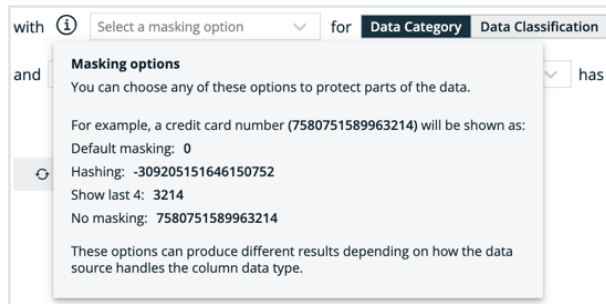
## 2. Column-based protection

Column based protection allows you to target specific columns and mask their content. By masking the column's data, the group cannot see the content as it is. They will see a masked version of it instead.

For example, you can mask a column of credit card numbers, so the individual group cannot see the full credit card numbers.

We currently support four masking options. They include:

- **Default masking:** Shows the value as 0.
- **Hashing:** Converts the value into a variety of different letters, numbers, and symbols.
- **Show last:** Displays the last letters, numbers, and symbols in the value. You can choose to show the last 1 through 20 of the value. The most common choice is Show last 4.
- **No masking:** Displays the data value as it is originally written.



Collibra Protect allows you to choose to mask columns that are part of a **data category** or a **data classification**. While granting access to a certain asset, you can choose to apply this masking on only a subset of that asset if it is also part of a data category or data classification.

### 3. Row-based protection

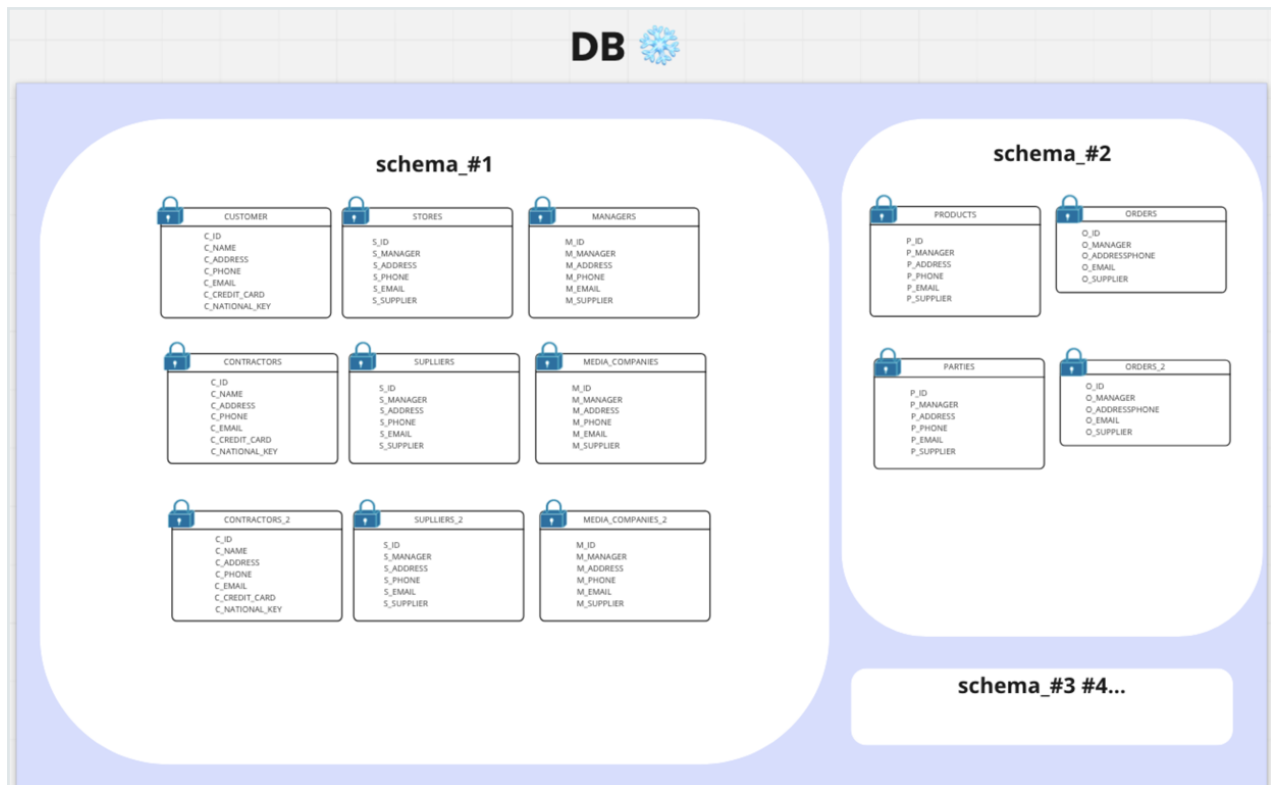
Another way to protect your data is to filter rows of a specific table. If you do not want to expose all of the existing items in a table because one of the columns is part of a certain data classification, you can easily leverage the Collibra operating model to do so.

When creating a rule that impacts certain tables in the source database, filter rows on tables by using the row filtering option for tables where one of their columns is part of a data classification. The filtering is based on what value is stored in the cell of that particular column. For instance, in a table that has a column that is classified as **country-code**, you can hide or show all items that have the value of **US**.

## Technical background

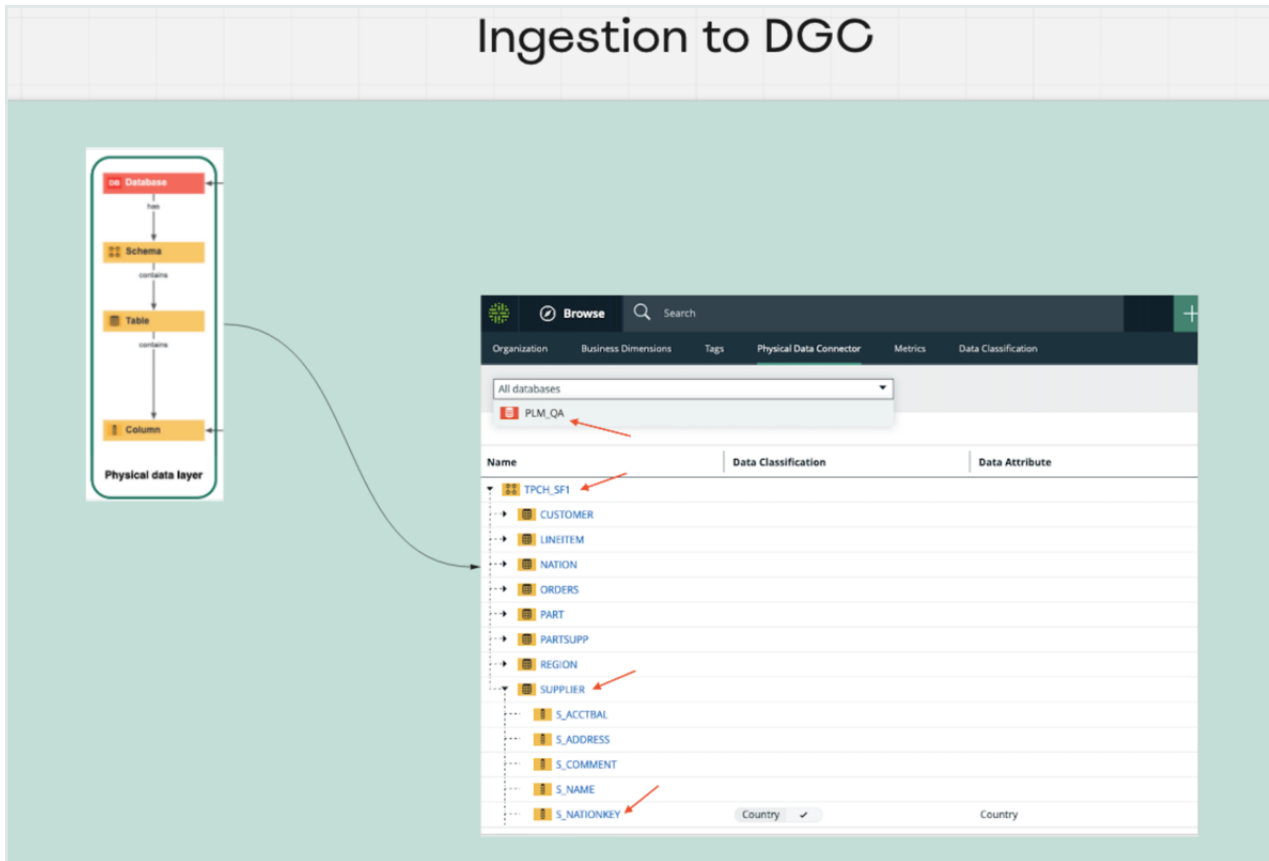
The technical background of Collibra Protect explains the connection of the data as it is in the database (DB) with the physical layer (equivalent assets in Collibra Data Intelligence Cloud) and the logical layer (the out of the box model).

Imagine you have this database:



When ingesting this DB to Collibra Data Intelligence Cloud, the physical layer is created as well as an asset for each of the schemas, tables, and columns.





Once there is a physical layer established in our Collibra environment, start creating the logical layer on top of it.

- In this phase, take any column and classify it as any data classification available, or let the platform classify it for you.
- Also, assign a column to a data attribute.

From here, create additional assets or use existing assets of different types (data set, data category, or business process) to establish a relation to these columns.

## Data protection standards vs. data access rules

Collibra Protect has both standards and rules to govern your data with ease and clarity.

<b>Standards</b>	<p>Data protection standards create a layer of protection for similar types of data by masking them wherever they are.</p> <p>For example, if columns with first and last names are a part of the PII data category, regardless what tables, schemas, and databases they are part of, create a standard that targets all of these columns by choosing the PII data category and masking it.</p>
<b>Rules</b>	<p>After establishing this primary layer (blanket) of protection to your most sensitive data, use data access rules to manage access and enhance protection for specific usages.</p> <p>For example, create a rule that grants access to a specific group, for a specific data set, while knowing that all PII within this data set will be masked by the standard we created before.</p>

## FAQs

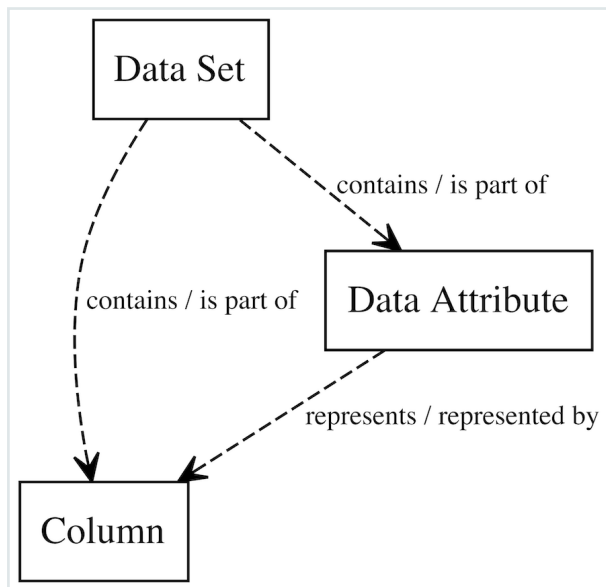
1. What if I want to grant access to a group without having the PII masked?
  - » When creating a rule for an asset that contains data masked by a standard, choose to override it by unmasking it or changing its masking type.
2. What If I want to grant access to a group, but the protection from the standard is not enough because there might also be other sensitive data within this supported asset?
  - » When creating a rule, add additional layers of protection over the ones that were set by any existing standard. Further protect the data by applying additional masking on or by filtering the data.

## Prescriptive paths

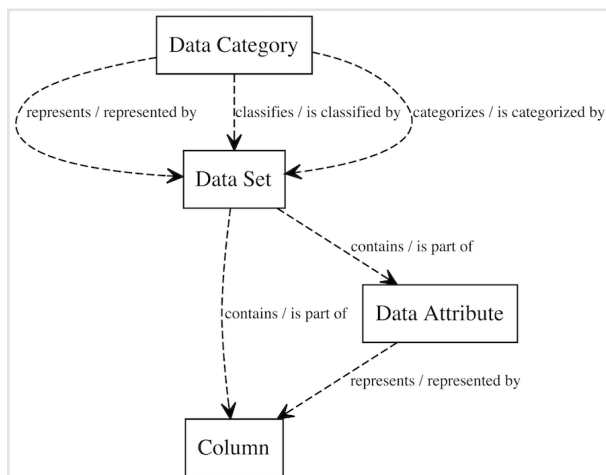
When creating a standard or rule, you select which asset(s) you want to protect and/or grant access to. By default, you can grant access to a data set, a data category, and a business process. Collibra Protect searches the knowledge graph, through relationships and/or intermediate assets, to find which set of physical data layer assets, such as columns and tables, this resolves.

The traversal of the knowledge graph is done through a set of prescriptive paths. For each type of asset, there is a set of prescriptive paths to traverse to the column assets. See the images below for more details.

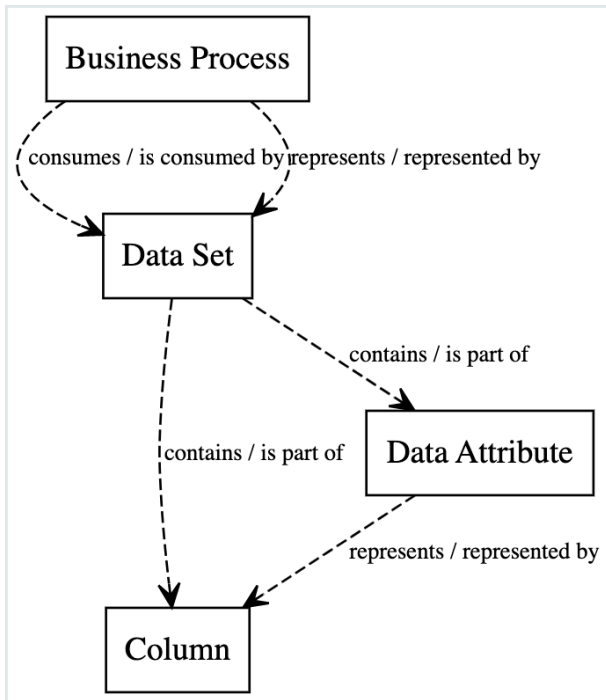
#### Prescriptive path for data set



#### Prescriptive path for data category



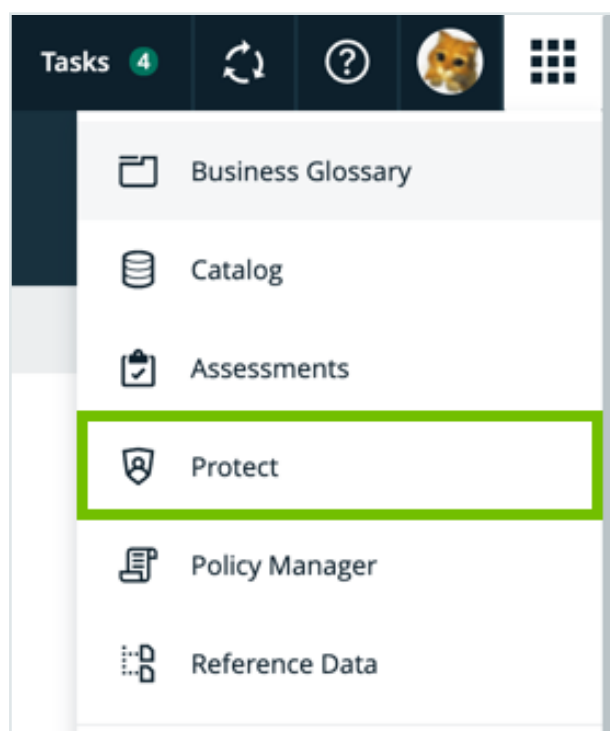
#### Prescriptive path for business process



# Overview of Collibra Protect

To work with Collibra Protect, ensure that you have a global role that has the Protect global permission and that it is [enabled](#) in your environment.

You will find, Collibra Protect, in the main menu . Click **Protect**.



If Collibra Protect is not shown on the menu, the feature is not enabled.

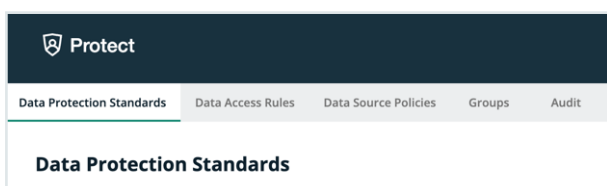
The landing page displays five tabs at the top of the page: **Data Protection Standards**, **Data Access Rules**, **Data Source Policies**, **Groups**, and **Audit**.

 Protect				
Data Protection Standards	Data Access Rules	Data Source Policies	Groups	Audit

Tab	Description
Data Protection Standards	<p>Define default data source access to data types based on data categories, data attributes, or classes/classifications through data protection standards</p> <p>Note Data access rules for particular groups can override created standards.</p>
Data Access Rules	Use data access rules to grant groups different access to the same data in data sets, in business processes, or identified by data categories.
Data Source Policies	View a list of policies that are currently active in the source data tables. You can also import policies from your source database using the Collibra Protect Data Source Policies API.
Groups	<p>Add groups through custom code via the Data Access API link and view existing current data access groups.</p> <p>Note You must add at least one group before you can create a standard or a rule.</p>
Audit	Generate an audit log for a preview of the last hour of ingested data from the data source.

## Data protection standards


The Data Protection Standards page contains an overview of the available standards in your environment.



Page Section	Description
Standards summary	Under the heading, there is a summary about data protection standards. Click the <b>Create a Data Protection Standard</b> button to <a href="#">create a standard</a> and get started in Collibra Protect.
Recently Modified Standards	This section shows the five most recently modified standards.
Standards table	This table displays a detailed view of the created data protection standards.

In the **Synchronization status** column of the standards table, there are five status options that can appear. To view the status of the standard in the data source, go to the source database.

Synchronization Status	Description
Active	This standard is currently active in Collibra Protect and in the data source.
Pending	This standard has been created or edited, and is pending synchronization.

Synchronization Status	Description
Failed	The synchronization of this standard has failed. Click the  icon next to the failed status to view additional information about the error.
Delete Pending	This standard will be deleted from the data source in the next synchronization.
Not Deleted	The deletion of this standard has failed.

**Note** Collibra Protect periodically synchronizes with the data source and statuses will be updated along with the synchronization. To learn more, go to the [general configuration](#) page.



# Create a data protection standard

Data protection standards create a layer of protection by masking data wherever they appear. Create a data protection standard to get started using Collibra Protect.

Create a Data Protection Standard

Data protection standards apply default data source access to types of data based on data categories or data classifications. Data Access Rules for particular groups will override these defaults.

Standard Name\*

Description

for the group\*  + -

protect\* Data Category Data Classification

with\* ⓘ

**Summary**  
 For the Group Human Resources  
 protect [Personal Information](#)  
 with Hashing

Cancel

Save Standard

## Steps

1. In Collibra Protect, go to the **Data Protection Standards** tab.
2. Click the green **Create a Data Protection Standard** button.
  - » The **Create Data Protection Standard** dialog box appears.
3. Enter the required information. It is important to note that when selecting assets, user permissions are defined in Collibra. If an asset is not visible for you, it will not appear as an option in the drop down menus.

Field	Description
Standard name	Name of the standard being created.

Field	Description
Description (optional)	Description of the standard.
Group	Group(s) for which the standard is created.
Data Category / Data Classification	A data category or data classification to apply the protection on.
Masking	Masking option for the standard.  <div> Note Click ⓘ to learn more about the masking options for standards. </div>

**Note** Click the plus sign to add more to each field where applicable. For example, after selecting a group, click + to add another group into the standard, and click – to delete a selected group. When entering the required information, you can view the selections you made in the **Summary** section.

4. Click the green **Save Standard** button.
  - » The saved data protection standard appears in the standards table.

## Modify a data protection standard


You can edit or delete a data protection standard after it has been created.

### Edit a standard

Editing a data protection standard might be necessary in certain situations. For example, change the masking method from default masking to hashing.

**Important** You will only be able to edit standard assets if you have view asset permissions. If one of the assets in the standard is unauthorized, you will not be able to edit the standard until the view access permission is granted.

## Steps

1. In the standards table, click the standard name, and then click the **Edit** button or click  in the appropriate row
  - » The **Edit a Data Protection Standard** dialog box appears.
2. Edit the [required information](#).
3. Click the green **Save Standard** button.
  - » The updated data protection standard appears in the standards table.

Edit a Data Protection Standard

Data protection standards apply default data source access to types of data based on data categories or data classifications. Data Access Rules for particular groups will override these defaults.


Standard Name \*

Description

for the group \*  + -

and the group  + -

protect \* **Data Category** **Data Classification**

with \* 

**Summary**  
 For the Group Human Resources and Marketing  
 protect [GDPR data related to criminal convictions and offences](#)  
 with Default masking


Cancel

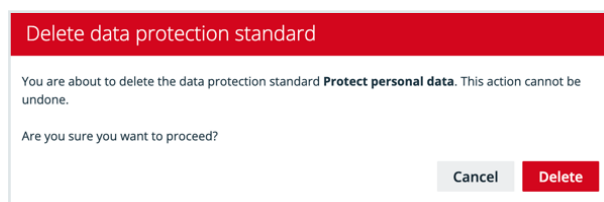
Save Standard

## Delete a standard

If you have an [author/admin role](#), delete a data protection standard that is no longer necessary.

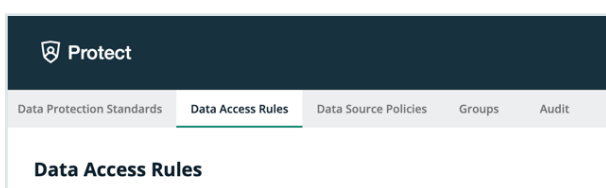
### Steps

1. In the standards table, click the  icon in the appropriate row  
» The **Delete data protection standard** dialog box appears.
2. Click the red **Delete** button.



## Data access rules


The Data Access Rules page contains an overview of the available rules in your environment.



Page Section	Description
Rules summary	Under the heading, there is a summary about data access rules. Click the <b>Create a Data Access Rule</b> button to <a href="#">create a standard</a> .
Recently Modified Rules	This section shows the five most recently modified rules.
Rules table	This table displays a detailed view of the created data access rules.

In the **Synchronization status** column, there are five status options that can appear. To view the status of the rule in the data source, go to the source database.

Synchronization Status	Description
Active	This rule is currently active in Collibra Protect and in the data source.
Pending	This rule has been created or edited, and is pending synchronization.

Synchronization Status	Description
Failed	The synchronization of this rule has failed. Click the  icon next to the failed status to view additional information about the error.
Delete Pending	This rule will be deleted from the data source in the next synchronization.
Not Deleted	The deletion of this rule has failed.

**Note** Collibra Protect periodically synchronizes with the data source and statuses will be updated along with the synchronization. To learn more, go to the [general configuration](#) page.

# Create a data access rule

After establishing a primary layer (blanket) of protection to your most sensitive data using standards, create data access rules to manage access to the data sources and enhance protection for specific usages.

Create a Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category and you can also conditionally filter rows based on code set values.

Rule Name \*

Marketing GI Rule

Description

Set rule for the marketing group for the geographic information asset  
Apply default masking for genetic data

Set rule for

group \* Marketing

asset \* Geographic Information

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ Default masking for Data Category Data Classification Genetic data

and Select an action rows where Unauthorized has Select a code set Select a code value

**Summary**

Grant access to Marketing  
for [Geographic Information](#)  
with Default masking for [Genetic data](#)

Generate Preview


Cancel Save Rule

## Steps

1. In Collibra Protect, go to the **Data Access Rules** tab.
2. Click the green **Create a Data Access Rule** button.
  - » The **Create a Data Access Rule** dialog box appears.
3. Enter the required information. It is important to note that when selecting assets, user permissions are defined in Collibra. If an asset is not visible for you, it will not appear as an option in the drop down menus.

Field	Description
Rule name	Name of the rule being created
Description (optional)	Description of the rule.
Group	Group for which the rule is being created.
Asset Name	Data asset that the rule is protecting. Collibra Protect enables you to protect the following asset types: Business process, data set, and data category. Learn more in <a href="#">technical background</a> and <a href="#">prescriptive paths</a> .



Field	Description
Masking (optional) <ul style="list-style-type: none"> <li>Data Category / Data Classification</li> </ul>	Masking option for the rule. Click the  to learn more about masking options. <ul style="list-style-type: none"> <li>Select a data category or a data classification to apply masking to.</li> </ul>
Action (optional) <ul style="list-style-type: none"> <li>Data Classification</li> <li>Code Set</li> <li>Code Value</li> </ul>	Filter the data by selecting hide or show. <ul style="list-style-type: none"> <li>Select data classification that is either hidden or shown</li> <li>Code set to set up row filtering in the tables. A code set must be selected to filter by a code value.</li> <li>Code value of the code set selected.</li> </ul>

**Important** The grant access checkbox is selected by default. By leaving this checkbox selected, you are granting access to the tables in the database with columns linked to the selected assets to the selected group(s). If you do not

want to grant this kind of access to these groups, clear the grant access checkbox.

**Note** Click the plus sign to add more to each field where applicable. For example, after selecting a group, click **+** to add another group into the standard, and click **–** to delete a selected group. When entering the required information, you can view the selections you made in the **Summary** section.

4. Click **Generate Preview** to see a preview of the new rule.

**Summary**

Grant access to Marketing  
for [Geographic Information](#)  
with Default masking for [Genetic data](#)

**Generate Preview**

**Geographic Information** ▼

Column ↑	Access	Masking Agent	Masking	Code Value
C_ADDRESS_sdfxgxfhcjhvjvbkjbkjbjhgxfz...	Masked	Genetic data	0	
C_NAME	Masked	Genetic data	0	
DS_TBL0001_COL0001	Masked	Genetic data	0	

Cancel **Save Rule**

**Tip** Use the preview to verify the data access rule is set up correctly. The preview only shows the first 1,000 affected columns. The drop-down below the **Generate Preview** button is used to switch between the different selected assets in the rule. Each asset has its own preview table.

5. Click the green **Save Rule** button.
  - » The saved data access rule appears in the rules table.

## Modify a data access rule


You can edit or delete a data access rule after it has been created.

## Edit a rule

Editing a data access rule might be necessary in certain situations. For example, change the code set value from BE to US.

**Important** You will only be able to edit rule assets if you have view asset permissions. If one of the assets in the rule is unauthorized, you will not be able to edit the rule until the view access permission is granted.

### Steps

1. In the rules table, click the rule name, and then click the **Edit** button or click  in the appropriate row
  - » The **Edit a Data Access Rule** dialog box appears.
2. Edit the [required information](#).
3. Click the green **Save Rule** button.
  - » The updated data access rule appears in the rules table

Edit a Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category and you can also conditionally filter rows based on code set values.

Rule Name \*

MH Rule 1

Description

Set rule for

group \* Marketing

asset \* Customer Data

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with Hashing for Data Category Data Classification Personal Information

and Select an action rows where Unauthorized has Select a code set Select a code value

**Summary**

Grant access to Marketing  
for Customer Data  
with Hashing for Personal Information


Generate Preview

Cancel Save Rule

## Delete a rule

If you have an [author/admin role](#), delete a data access rule that is no longer necessary.

## Steps

1. In the rules table, click the  icon in the appropriate row
  - » The **Delete data access rule** dialog box appears.
2. Click the red **Delete** button.

Delete data access rule

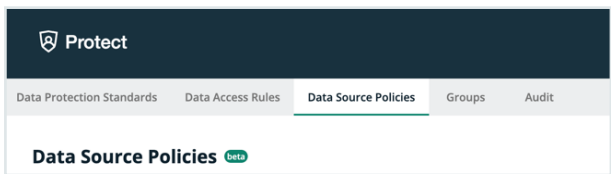
You are about to delete the data access rule **Rule 1**. This action cannot be undone.

Are you sure you want to proceed?

Cancel Delete

# Data source policies

The Data Source Policies page contains an overview of the available policies in your environment.



The data protection policy table displays a list of policies that are currently active in the source data tables. This includes policies that were created via Collibra Protect as well as policies that were created in the data source manually.

**Note** Collibra Protect currently only supports the Snowflake data source.

The table columns include:

Column name	Description
Data Protection Policy Name	Policies that originated in Collibra Protect have this structure: [DB name].[SCHEMA name].[policy type*].[asset id].  *Policy type can also be masking/row-filtering
Policy Logic	This column contains the SQL command that is executed in Snowflake whenever the user tries to access the protected object and will determine how to display the data to the user.
Tags	For policies that originated in a standard, this column lists the name of the attached tag. The convention is that each tag has the name of the asset that is included in that standard.

The screenshot shows the Collibra Protect web application. The top navigation bar includes 'Browse', 'Search', and a 'Tasks' section. The main header is 'Protect'. Below it, a sub-header shows 'Data Protection Standards', 'Data Access Rules', 'Data Source Policies' (selected), 'Groups', and 'Audit'. The 'Data Source Policies' section has a sub-header 'Data Protection Policy Name' and a description: 'This is a list of policies that are currently active in the source data tables.' Below this is a table with three columns: 'Data Protection Policy Name', 'Policy Logic', and 'Tags'. The table lists several policies, all of which are 'create or replace masking policy' statements. The policies are named 'PROTECT\_QA.MASKING.COLLIBRA.MASKING.POLICY/380323eb-eb2f-46c4-9d46-19a8532827b6...' and 'PROTECT\_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...'. The policy logic for each is a SQL statement that creates or replaces a masking policy. The tags for each policy are 'PROTECT\_QA.MASKING.Personally Identifiable Information'.

Data Protection Policy Name	Policy Logic	Tags
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/380323eb-eb2f-46c4-9d46-19a8532827b6...	create or replace masking policy "COLLIBRA/MASKING_POLICY/380323eb-eb2f-46c4-9d46-19a8532827b6/INTDGER" as (VAL NUMBER(38,0)) ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/ARRAY" as (VAL ARRAY) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/ARRAY" as (VAL ARRAY) returns ...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BOOLEAN" as (VAL BOOLEAN) retu...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BOOLEAN" as (VAL BOOLEAN) retu...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING.POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	

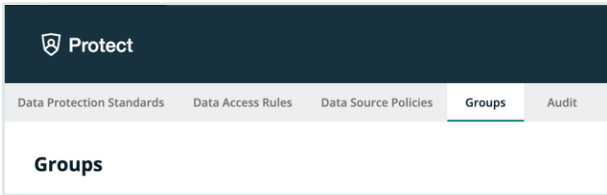
# Types of policies on Snowflake

There are three types of policies on Snowflake: Column-based policies, row access policies, and tag-based policies. Each type can be created in Collibra Protect or on Snowflake.

For rules, policies are created directly on the column level. Row access policies are created when row filters are specified. For standards, the policy is created, attached to a Snowflake tag, and attached to the tab on any affected column.

# Groups

The Groups page contains an overview of the created Collibra Protect groups in your environment.



The groups table displays a list of groups that are currently active in the data source.

Protect			
Data Protection Standards	Data Access Rules	Data Source Policies	Groups
Audit			
Groups			
<div><div>Adding Groups</div><div>To add a group, you have to use the <a href="#">Collibra Protect Group API</a>. Currently, only Snowflake data sources are supported.</div></div>			
Group Name	System Reference	Created By	Created date
CID	"Snowflake": "string"	Admin Istrator	Jun 16, 2022, 8:52 AM
Human Resources	"Snowflake": "HR"	Admin Istrator	May 11, 2022, 11:39 AM
Marketing	"Snowflake": "MARKETING"	Admin Istrator	May 11, 2022, 11:39 AM

**Note** Collibra Protect currently only supports the Snowflake data source.

The table columns include:

Column name	Description
Group Name	Name of the Collibra Protect group
System Reference	
Created By	User who created the Collibra Protect group
Created Date	Date the group was created

## Adding groups in Collibra Protect

To add a group, use the [Collibra Protect Group API link](#). This action must be done before any data protection standards or data access rules can be created.



# Audit

An audit log contains information about the queries that were run to access the data and the data that was accessed.

## Generate an audit log

You can generate an audit log of access records from the data source on the **Audit** page.

**Note** The time that it takes for the actions performed in a data source to appear in an audit log in Collibra Protect varies from several minutes to hours, depending on the data source.

## Steps

1. In Collibra Protect, click the **Audit** tab.
2. Click one of the following buttons: **Today**, **Yesterday**, **A week ago**, **30 days ago**.

**Tip** The start date corresponding to the button that you clicked is shown in the **Start Date** field. Alternatively, you can enter or select a date in the **Start Date** field, and then click **Generate Log**.

» The audit log is generated.

### Important

- Generating an audit log may take up to a minute. After clicking **Generate Log**, do not navigate away from the **Audit** page because doing so cancels the audit log generation.

- The audit log contains the first 1,000 records from the selected start date. If you want to view the remaining records, contact your data source administrator.

**Audit** data

Today

Yesterday

A week ago

30 days ago

Start Date  
09/29/2022

Generate Log

For audit log generation, data sources may have latency to summarize access records. Logs generated here for today may not contain information for the most recent access.

Query ID	Query Start Time	Source User Name	Direct Objects Accessed	Base Objects Accessed
01a74800-0501-ec9a-0001-000306f6b19e	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.MAIN_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ec9a-0001-000306f6b1a2	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.MAIN_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ea46-0001-000306f69dd2	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.DEPENDS_ON_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ec9a-0001-000306f6b1a6	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.NODES_DEPENDS_ON_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE

# Audit log data

The following table describes the columns that are shown in an audit log.

Column	Description
Query ID	The ID of the query in the source database.
Query Start Time	The date and time of the query in the source database.
Source User Name	The name of the user in the source database who ran the query to access the data.
Direct Object Accessed	The database object (a table or a view) that was used to access the data.
Base Object Accessed	The database object that was accessed.

# Why rules or standards fail

Certain rules or standards may fail due to logical errors. This section describes some of the common scenarios that cause them to fail.



# Different types of masking affecting the same column

This topic contains examples to describe how data protection standards and data access rules behave when different types of masking affect the same column.

**Note** In the topic, the term *agent* refers to a data category or a data classification.

## Masking within a rule

### Scenario

A rule that is set for a group masks multiple agents using different types of masking, and the agents share the same column. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

### Example

Consider a rule that is set for the **Marketing** group. The rule masks the **Personal Information** data category by hashing and masks the **Personal and family details** data category by showing only the last two digits. Suppose that both these data categories share the same column. Then, the rule will fail because the same column cannot be masked using two different masking types for a given group.

Rule Name \*

Masking within a rule

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

and the asset

Audit & Internal Controls

+

-

☒ Grant access to all data tables linked to these asset columns.  
 By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Hashing

for

Data Category

Data Classification

Personal Information

+

-

with ⓘ

Show last

2

for

Data Category

Data Classification

Personal and family details

+

-

and

Select an action

rows where

Select a data classification

has

Select a code set

Select a code value

Summary

Grant access to Marketing

for Customer Data and Audit & Internal Controls

with Hashing for Personal Information and

with Show last 2 characters for Personal and family details

## Masking between rules

This scenario is similar to the [previous scenario](#) except that this scenario considers two rules, instead of one, that are set for the same group. The masking types for the agents in the two rules are different, and both the agents share the same column. Then, a conflict occurs because the same column cannot be masked using two different masking types for a given group.

When two rules conflict with each other, if the synchronization status of only one of them is **Active**, then the other rule fails. If, however, the synchronization status of both the rules is **Active** or **Pending**, then both of them fail.

This scenario is applicable regardless of whether the agents are the same or different, and regardless of whether the rule applies to a single asset or multiple assets.

Rule Name \*

Masking between rules - 1

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with

i

Hashing

for

Data Category

Data Classification

Personal Information

+

-

and

Select an action

rows where

Select a data classification

has

Select a code set

Select a code value

Summary

Grant access to Marketing  
for [Customer Data](#)  
with Hashing for [Personal Information](#)

Rule Name \*

Masking between rules - 2

Description

Set rule for

group \*

Marketing

+

-

asset \*

Audit & Internal Controls

+

-

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with

i

Show last

2

for

Data Category

Data Classification

Personal and family details

+

-

and

Select an action

rows where

Select a data classification

has

Select a code set

Select a code value

Summary

Grant access to Marketing  
for [Audit & Internal Controls](#)  
with Show last 2 characters for [Personal and family details](#)

Masking between standards

Scenario

Two standards mask different agents, and the agents share the same column. This scenario is applicable regardless of whether the groups and the masking types are the same or different.

## Example

Consider two standards. The first standard masks the **Personal Information** data category, and the second standard masks the **Name** data classification. Suppose that both the agents share the same column. Then, a conflict occurs because more than one standard cannot be applied to the same column via different agents.

**Note** This is a limitation on how Collibra Protect implements standards on Snowflake.

If two standards affect the same column, you may not be able to view the column data in the data source.

Standard Name \*  
Masking between standards - 1

Description

for the group \* Marketing
+ -

protect \*

Data Category
Data Classification

Personal Information

with \* ⓘ Hashing

**Summary**  
For the Group Marketing  
protect [Personal Information](#)  
with Hashing

Standard Name \*

Masking between standards - 2

Description

for the group \*

Human Resources

+

-

protect \*

Data Category

Data Classification

Name

with \*

i

Show last

2

Summary

For the Group Human Resources

protect [Name](#)

with Show last 2

## Conflicting filters affecting the same column

This topic contains examples to describe how data protection standards and data access rules behave when conflicting filters affect the same column.

### Filtering within a rule for the same data classification

#### Scenario

A rule that is set for a group contains conflicting filters for the same data classification. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

#### Example

Consider a rule that is set for the **Marketing** group and the **Customer Data** asset. The rule contains two filters for the **Country** data classification.



Rule Name \*

Filtering within a rule for the same data classification

Description

Set rule for

group \* Marketing

asset \* Customer Data

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ Select a masking option for Data Category Data Classification Select a data category

and Show rows where Country has Country code BE

and Hide rows where Country has Country code PL

**Summary**

Grant access to Marketing  
for Customer Data  
and Show rows where Country has Country code: BE  
and Hide rows where Country has Country code: PL

If any of the tables in the asset contain a column that is classified as **Country**:

- The first filter shows the rows that contain **BE** in that column.
- The second filter hides the rows that contain **PL** in that column.

Then, this rule will fail because two conflicting filters affect the same column.

When applying a filter for a specific data classification, you must select only one type of action. That is, you can choose to either show rows based on one or more values or hide rows based on one or more values. You must not use the show and hide filter actions together for the same data classification.

## Filtering within a rule for different data classifications

### Scenario

A rule that is set for a group contains conflicting filters for different data classifications that share the same column. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

## Example

Consider a rule that is set for the **Marketing** group and the **Customer Data** asset. The rule contains two filters: one for the **Country** data classification, and another for the **State** data classification.

Rule Name \*

Filtering within a rule for different data classifications

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

☒ Grant access to all data tables linked to these asset columns.  
By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category

Data Classification

Select a data category

and

Show

rows where

Country

has

Country code

BE

+

-

and

Hide

rows where

State

has

Country code

PL

+

-

Summary

Grant access to Marketing for Customer Data and Show rows where Country has Country code: BE and Hide rows where State has Country code: PL

If any of the tables in the asset contain columns that are classified as **Country**, the first filter shows only the rows that contain **BE** in those columns.

If any of the tables in the asset contain columns that are classified as **State**, the second filter hides only the rows that contain **PL** in those columns.

Suppose that a column is classified as both **Country** and **State**. That is, data classifications **Country** and **State** share the same column. Then, this rule will fail because two conflicting filters affect the same column.

### Filtering between rules for same or different data classifications

This scenario is similar to the [previous scenarios](#) except that this scenario considers two rules, instead of one, that are set for the same group. The filter in one rule is different from the filter in the other rule, and both the filters affect the same column. Then, a conflict occurs because two conflicting filters affect the same column.

When two rules conflict with each other, if the synchronization status of only one of them is **Active**, then the other rule fails. If, however, the synchronization status of both the rules is **Active** or **Pending**, then both of them fail.

Rule Name \*

Filtering between rules for same or different data classifications - 1

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category

Data Classification

Select a data category

and

Show

rows where

Country

has

Country code

BE

+

-

Summary

Grant access to Marketing

for Customer Data

and Show rows where Country has Country code: BE

Rule Name \*

Filtering between rules for same or different data classifications - 2

Description

Set rule for

group \*

Marketing

+

-

asset \*

Personal Information

+

-

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category

Data Classification

Select a data category

and

Hide

rows where

Country

has

Country code

PL

+

-

Summary

Grant access to Marketing

for Personal Information

and Hide rows where Country has Country code: PL

# Reference

Collibra Protect periodically synchronizes with an aggregation of all data protection standards and data access rules. These standards and rules form a data source-agnostic representation containing all databases, schemas, tables, and columns, as well as their protections and accesses. The synchronization process then triggers the [Edge capabilities](#), such as Collibra Protect for Snowflake. These Edge capabilities are responsible for translating the representation to actions toward the data source provider using their technology. This process might involve JDBC and REST calls to perform low-level operations to guarantee that the protections and accesses are applied.

## Protect for Snowflake

Data protection standards in Collibra Protect rely on the [tag-based masking policies](#) of Snowflake. The name of the data category or data classification selected in a standard becomes a tag with the same name. The tag is applied to all the affected columns to enforce data protection. For more information, go to [Example](#).

## Example

This topic contains an example to describe how Snowflake behaves in relation to certain data protection standards and data access rules.

### Introduction

This example describes the behavior in Snowflake when a standard is applied to a data category and a rule is applied to a data set with categorized columns in Protect.

The example considers the following:

- A standard created for the **Everyone**, **Human Resources**, **Marketing**, and **Sales** groups, to protect the columns in the **Personally Identifiable Information** data category by default masking.

Set rule for

group \* Everyone

and the group Human Resources

and the group Marketing

and the group Sales

protect \* Data Category Data Classification Personally Identifiable Information

with \* Default masking

- A rule created for the **Human Resources** group and the **Employee Data** asset, without any protection applied to the columns in the **Personally Identifiable Information** data category.

Set rule for

group \* Human Resources

asset \* Employee Data

☒ Grant access to all data tables linked to these asset columns.  
By checking this box, access will be given to the tables in the database with columns linked to the selected assets. If this box is unchecked, no access will be given to these columns.

with \* No masking

for Data Category Data Classification Personally Identifiable Information

## Standard

When the **standard** is synchronized and active, the standard results in 14 masking policies—one policy for each **Snowflake data type**. The masking policies are created at the schema level with the following naming convention: **COLLIBRA/MASKING\_POLICY/<asset ID>/<snowflake type>**.

Results Data Preview						
<div> <span>Query ID</span> <span>SQL</span> <span>84ms</span> <span>18 rows</span> </div> <div> <input type="text" value="Filter result..."/> <span>Download</span> <span>Copy</span> </div>						
Row	created_on	name	database_name	schema_name	kind	owner
1	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/ARRAY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
2	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/BINARY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
3	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/BOOLEAN	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
4	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/DATE	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
5	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/FLOAT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
6	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/GEOGRAPHY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
7	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/NUMBER	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
8	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/OBJECT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
9	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/STRING	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
10	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIME	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
11	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
12	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP_LTZ	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
13	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP_TZ	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
14	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/VARIANT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN

All the masking policies are then associated with the **Personally Identifiable Information** tag, which is created at the schema level and assigned to those columns that need to be protected. At runtime, Snowflake fetches the right masking policy based on the **column data type**.

Row	created_on	name	database_name	schema_name	owner	comment
1	2022-09-06 03:46:10.054...	Personally Identifiable Information	PROTECT_QA	DEMO	ACCOUNTADMIN	Generated by Collibra: 28d226cc-0ab0-4d23-b912-985312fb36b1

The following image shows a masking policy for the STRING data type. The data that is shown in the policy depends on the masking type selected in the standard. In the policy, `val` indicates the value as it is stored in the table.

```

1 CASE
2   WHEN CURRENT_ROLE() = 'PUBLIC' THEN '*'
3   WHEN CURRENT_ROLE() = 'HR' THEN '*'
4   WHEN CURRENT_ROLE() = 'MARKETING' THEN '*'
5   WHEN CURRENT_ROLE() = 'SALES' THEN '*'
6   ELSE val
7 END

```

## Rule

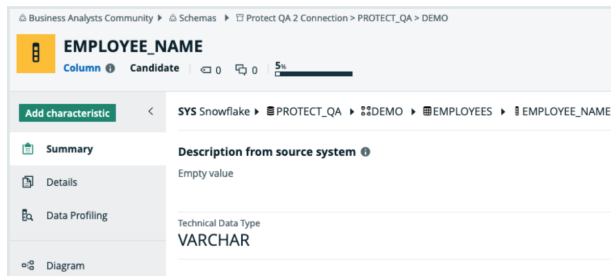
A rule results in a combination of [grant instructions](#), [dynamic masking](#), and [row access policies](#).

Suppose that the **Employee Data** data set selected in the [rule](#) contains sensitive columns categorized as **Personally Identifiable Information**.

#	Name	is part of
1	EMPLOYEE_NAME	EMPLOYEES
2	EMP_ID	EMPLOYEES
7	DEPT_ID	EMPLOYEES
10	SALARY	EMPLOYEES

The [rule](#) grants access of the **Employee Data** data set to the **Human Resources** group, as indicated by the selected **Grant access...** checkbox in the rule. Then, the corresponding Snowflake role for the group can access each database, schema, and table in the data set. In addition, the column masking policy is applied to those columns that need to be protected.

Consider the **EMPLOYEE\_NAME** column in the **Employee Data** data set. This column belongs to the **EMPLOYEES** table within the **DEMO** schema in the **PROTECT\_QA** database.



In Snowflake, each column that is categorized as **Personally Identifiable Information** within the **Employee Data** dataset inherits the masking policy that is applied to the column in Protect. The masking policies created at the schema level use the following naming convention: **COLLIBRA/MASKING\_POLICY/<asset ID>**.

Row	created_at	name	database_name	schema_name	role	owner
16	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c6845d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
17	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c6845d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
18	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c6845d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
19	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c6845d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
20	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c6845d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN

The following image shows the masking policy created for the **EMPLOYEE\_NAME** column.

Details	
1	CASE
2	WHEN CURRENT_ROLE() = 'HR' THEN val
3	WHEN CURRENT_ROLE() = 'PUBLIC' THEN '*'
4	WHEN CURRENT_ROLE() = 'MARKETING' THEN '*'
5	WHEN CURRENT_ROLE() = 'SALES' THEN '*'
6	ELSE val
7	END

## Behavior

According to the [standard](#), the **Everyone**, **Human Resources**, **Marketing**, and **Sales** groups have masked access to the data. However, according to the [rule](#), the **Human Resources** group has unmasked access to the data. As a result, the **EMPLOYEE\_NAME** column has both a policy tag and a column masking policy applied to it via the standard and the rule, respectively.

In Snowflake, if both a policy tag and a column masking policy exist for a column, the column masking policy takes precedence and the policy tag is not assigned to the column. To mitigate this behavior and ensure that the protection defined in the standard is not ignored, the column masking policy also considers the conditions defined in the standard (policy tag).

Thus, when a standard is created for the **Human Resources**, **Marketing**, and **Sales** groups to mask the **Personally Identifiable Information** column by default masking, and when a rule is created for the **Human Resources** group to not mask the same column, the result is as follows:

- The column is not masked for the **Human Resources** group.
- The column is masked for the **Marketing** and **Sales** groups via default masking.



## Masking and data types

Snowflake provides several functions to transform the data. This topic describes how Snowflake transforms the data for a given Protect masking type.

- **Default masking:** Snowflake does not support this masking type. Protect, however, uses the default masking type to apply protection to a wide range of data types. A default masking value is applied to each column according to the data type of the column.

### Default masking values for data types

Column data type	Snowflake data type	Default masking value
NUMBER	NUMBER	0
DECIMAL	NUMBER	0
NUMERIC	NUMBER	0
INT	NUMBER	0
INTEGER	NUMBER	0
BIGINT	NUMBER	0
SMALLINT	NUMBER	0
TINYINT	NUMBER	0
BYTEINT	FLOAT	0
FLOAT	FLOAT	0
FLOAT4	FLOAT	0
FLOAT8	FLOAT	0
DOUBLE	FLOAT	0

Column data type	Snowflake data type	Default masking value
DOUBLE PRECISION	FLOAT	0
REAL	FLOAT	0
VARCHAR	VARCHAR	*
CHAR	VARCHAR	*
CHARACTER	VARCHAR	*
STRING	VARCHAR	*
TEXT	VARCHAR	*
BINARY	BINARY	00
VARBINARY	BINARY	00
BOOLEAN	BOOLEAN	false
DATE	DATE	1970-01-01
DATETIME	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIME	TIME	00:00:00
TIMESTAMP	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIMESTAMP_LTZ	TIMESTAMP_LTZ	1969-12-31 16:00:00.000-0800  <div>Note This may change depending on the time zone.</div>

Column data type	Snowflake data type	Default masking value
TIMESTAMP_NTZ	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIMESTAMP_TZ	TIMESTAMP_TZ	1969-12-31 16:00:00.000-0800  <div>Note This may change depending on the time zone.</div>
VARIANT	VARIANT	0
OBJECT	OBJECT	{}
ARRAY	ARRAY	[]
GEOGRAPHY	GEOGRAPHY	{"coordinates": [0,0], "type": "Point"} (aka point(0, 0) and visualization can change based on user preferences)

- **Hashing:** Uses the following Snowflake functions:
  - *SHA2* (for strings)
  - *HASH* (for numbers)
- **Show last:** Uses the following expressions:
  - *substr(to\_varchar(value), length(value) - n, n)* (for strings)
  - *mod(value, power(10,n))* (for numbers)

Tip In the expressions, *value* indicates the content and *n* indicates the number of characters to be shown.

- **No masking:** Returns the raw content.

**Note**

- You can apply the **Hashing** and **Show last** masking types to only the following Snowflake data types: FLOAT, NUMBER, and STRING.
- If a selected masking type cannot be applied to a certain data type—for example, when you attempt to apply the **Hashing** masking type to the DATE data type—the **Default masking** type is applied to the data type to guarantee protection.

## Snowflake privileges

To perform actions in Snowflake, Collibra Protect uses an Edge connection that must be configured with a user and a role that can manage grants; create and assign masking policies, row access policies, and tags; and manage usage access on databases and schemas involved in the protection. This enforcement role requires the following Snowflake privileges.

Snowflake privilege	Description
[APPLY MASKING], [APPLY ROW ACCESS], [APPLY TAG], [MANAGE GRANTS], [IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE]	Required for the role performing the actions.
[USAGE]	Required on each database and schemas where policies are applied to the role performing the actions.

Snowflake privilege	Description
[CREATE MASKING POLICY], [CREATE ROW ACCESS POLICY], [CREATE TAG]	Required on each schema where policies are applied to the role performing the actions.

## Example

Suppose that a role named PROTECT exists in Snowflake and is responsible for managing access on all schemas within a database named DEMO. Then, the following statements can be used to enable the Snowflake PROTECT role to perform the enforcement.

```
GRANT APPLY MASKING POLICY ON ACCOUNT TO ROLE PROTECT;
GRANT APPLY ROW ACCESS POLICY ON ACCOUNT TO ROLE PROTECT;
GRANT APPLY TAG ON ACCOUNT TO ROLE PROTECT;
GRANT MANAGE GRANTS ON ACCOUNT TO ROLE PROTECT;
GRANT IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE TO ROLE PROTECT;
GRANT USAGE ON DATABASE DEMO TO ROLE PROTECT;
GRANT USAGE ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE MASKING POLICY ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE ROW ACCESS POLICY ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE TAG ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
```

# Collibra Protect

## About Collibra Protect

Collibra Protect is a capability of the Data Intelligence Cloud created to protect sensitive data and make it available, or partially available, to specified groups of users.

Collibra Protect solves the problem of protecting sensitive data in an organization. Different groups of people may need varying access levels to the same data set. With Collibra Protect, access rules and data protection standard capabilities allow you to grant access to individuals and protect sensitive information. These rules and standards with different data access levels are managed through the Collibra platform and pushed to the data source. Our aim is to promote a safe data-open culture in organizations.

The goal of Collibra Protect is to centralize and simplify access governance and remove the need of repetitive action and approval. Data access and privacy management promotes an ethical company standard giving permission to view information only to those that need it. Collibra Protect allows you to perform these actions accordingly.

An example use case of Collibra Protect is a data steward giving everyone access to a data set, but only allowing certain access to groups of people based on data categories. This is known as differential access. It is suggested that rules/standards are grouped together, for example by business processes, so you do not have to make a rule or standard for every data set.



# Install Collibra Protect

This procedure guides you through a first time installation of Collibra Protect.

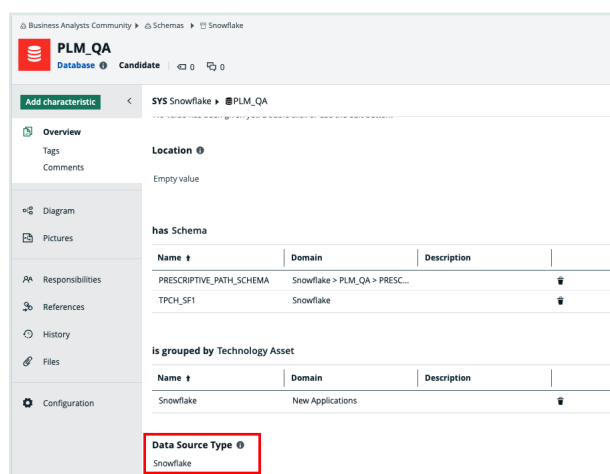
## Prerequisites

You must add the [Snowflake capability on Edge](#) as well as perform a catalog ingestion.

Configure the Collibra Protect for Snowflake capability on Edge. Settings → (Edge) Sites → Your site → Capability → Add capability → fill in the needed parameters:

- For "Capability template" choose "Collibra Protect for Snowflake".
- The "Snowflake Connection" can be the same connection used for doing catalog ingestion. Make sure that the Snowflake user/role has enough permissions to create/alter/drop grants, tags, etc.

An ingested Snowflake database should look like the example below.

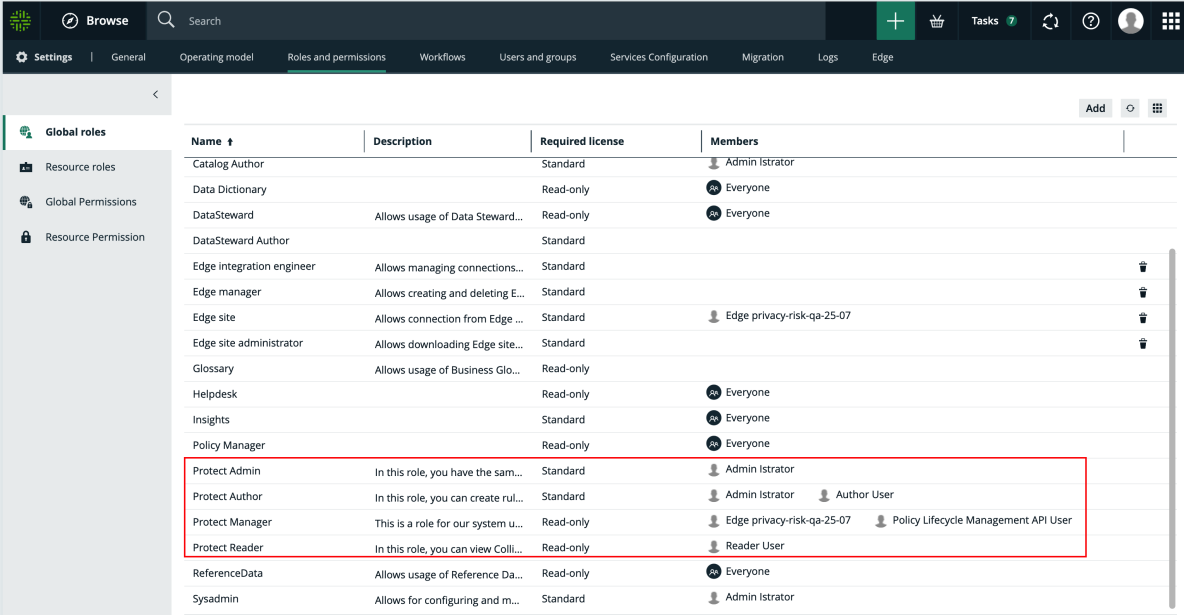





**Note** The Data Source Type attribute on the database asset should be present. This attribute is automatically added in database assets, after the catalog ingestion process.

## Steps

1. Contact a Collibra support or your representative to enable Collibra Protect on your Collibra environment.
2. Ensure [global roles and permissions](#) for Collibra Protect are set correctly.



Name	Description	Required license	Members
Catalog Author		Standard	Admin Istrator
Data Dictionary		Read-only	Everyone
DataSteward	Allows usage of Data Steward...	Read-only	Everyone
DataSteward Author		Standard	
Edge integration engineer	Allows managing connections...	Standard	
Edge manager	Allows creating and deleting E...	Standard	
Edge site	Allows connection from Edge ...	Standard	Edge privacy-risk-qa-25-07
Edge site administrator	Allows downloading Edge site...	Standard	
Glossary	Allows usage of Business Glo...	Read-only	
Helpdesk		Read-only	Everyone
Insights		Standard	Everyone
Policy Manager		Read-only	Everyone
Protect Admin	In this role, you have the sam...	Standard	Admin Istrator
Protect Author	In this role, you can create rul...	Standard	Admin Istrator, Author User
Protect Manager	This is a role for our system u...	Read-only	Edge privacy-risk-qa-25-07, Policy Lifecycle Management API User
Protect Reader	In this role, you can view Coll...	Read-only	Reader User
ReferenceData	Allows usage of Reference Da...	Read-only	Everyone
Sysadmin	Allows for configuring and m...	Standard	Admin Istrator

3. Collibra Protect is installed.
  - » You can now access and start using Collibra Protect via the  menu.

# Configure Collibra Protect

Configuring within Collibra Protect is an important part of understanding and using Collibra Protect to its highest ability.


## Prerequisites

- You need to have Data Catalog permissions. If not, you cannot see any classification in either standards or rules.
- You need to have a Data Steward role within Collibra. If not, you cannot see the classification page when selecting a classification in Collibra Protect.



## Roles in Collibra Protect

It is possible to assign different roles to Collibra users that use Collibra Protect. The roles are provided and have pre-defined permissions that restrict the usage of the application.

Roles	Description
Protect Reader	Users in this role can view Collibra Protect with read-only access to the content. This role is assigned to 'Everyone' and grants the users the 'protect' permission. Without this permission, users cannot see 'Protect' as an application in the  menu. They also cannot navigate to protect related URLs or access protect endpoints.
Protect Author	Users in this role can create <a href="#">rules</a> and <a href="#">standards</a> , view <a href="#">imported policies</a> and <a href="#">groups</a> , and generate <a href="#">audits</a> as an individual contributor. This role grants the product right permission 'protect' and the 'protect_edit' permission. Authors can only modify rules and standards they own. This role is not assigned to anyone automatically.
Protect Admin	Users in this role have the same permissions as the Protect Author role as well as the ability to edit other user's rules and standards. This role grants the product right permission 'protect', 'protect_edit', and an extra 'protect_administration' permission. This role is not assigned to anyone automatically.
Protect Manager	This role is restricted to our system user to manage background processes and setup configurations for Collibra Protect and it should not be assigned to other Collibra users.

## Configure groups

Before you start working in Collibra Protect, you need to configure your groups. Collibra Protect groups are the basis of all the actions performed in Collibra Protect.

## Associate a Protect group with Snowflake

Each Snowflake user is assigned to one or more Snowflake roles. Permissions are based on these roles. View the example below of the roles page in Snowflake. Any/all roles can be correlated to a Collibra Protect group.

Role	Creation Time	Owner	Comment
ACCOUNTADMIN	9/18/2019, 1:47:25 ...		Account administrator can manage all aspects of the account.
ANTONIO	6/27/2022, 10:10:4...	SBI_TEMPLATE_SN...	
BILLING	6/2/2022, 4:07:43 ...	ACCOUNTADMIN	
CERTIFICATION	4/15/2020, 2:12:24 ...	ACCOUNTADMIN	
CUSTOMER_SERVICE	6/2/2022, 4:05:29 ...	ACCOUNTADMIN	
DATALIFT_ROLE	5/6/2020, 9:56:54 ...	ACCOUNTADMIN	
Direct Marketing	6/27/2022, 10:12:4...	SBI_TEMPLATE_SN...	
FIVETRAN_ROLE	1/27/2022, 10:27:58...	SECURITYADMIN	
GLOBAL_PS	9/27/2021, 2:36:19 ...	ACCOUNTADMIN	
HR	10/22/2021, 1:38:44...	ACCOUNTADMIN	
LAW	3/3/2022, 9:00:27 ...	ACCOUNTADMIN	
MARKETING	9/29/2021, 1:59:26 ...	ACCOUNTADMIN	
MARKETING2	9/29/2021, 2:36:17 ...	ACCOUNTADMIN	
MARKETING3	9/30/2021, 3:56:47 ...	ACCOUNTADMIN	
PC_DBT_ROLE	5/6/2022, 9:08:33 ...	ACCOUNTADMIN	System created role for partner elt integration.
PLM	10/22/2021, 1:30:58...	ACCOUNTADMIN	
PLM_QA_HR	2/24/2022, 3:38:20...	ACCOUNTADMIN	PLM QA HR Read Only Role

## How to create Collibra Protect groups?

When you initially go to the **Groups** tab in Collibra Protect, there are no groups created. There is a link at the top of the page to the Groups API that creates new groups in Collibra Protect. Use this API link to create new groups and associate it with a specific role in Snowflake.

## Groups

Adding Groups  
 To add a group, you have to use the [Colibra Protect Group API](#). Currently, only Snowflake data sources are supported.

Group Name	System Reference	Created By	Created Date
------------	------------------	------------	--------------

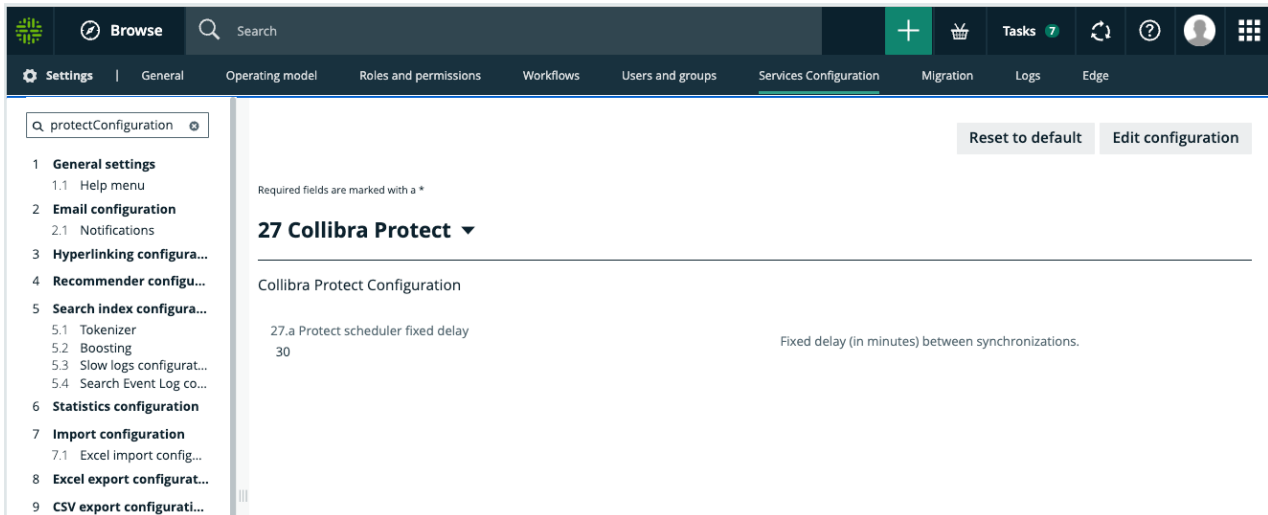
  

The screenshot shows the Snowflake web interface. At the top, there's a navigation bar with icons for Databases, Shares, Marketplace, Warehouses, Worksheets, History, and Account. Below this, a toolbar contains buttons for 'Run', 'All Queries', and 'Saved 10 seconds ago'. The main query editor shows the command 'SHOW roles;'. Below the editor, the 'Results' tab is active, displaying a table with 37 rows. The table has columns: Row, created\_on, name, is\_default, is\_current, is\_inherited, assigned\_to\_users, granted\_to\_roles, granted\_roles, owner, and comment. The data lists various roles like ACCOUNTADMIN, ANTONIO, BILLING, CERTIFICATION, CUSTOMER\_SERVICE, DATALIFT\_ROLE, Direct Marketing, FIVETRAN\_ROLE, GLOBAL\_PS, HR, LAW, and MARKETING.

Row	created_on	name	is_default	is_current	is_inherited	assigned_to_users	granted_to_roles	granted_roles	owner	comment
1	2019-09-17 16:47:2...	ACCOUNTADMIN	N	Y	N	35	0	3		Account administrat...
2	2022-06-27 01:10:4...	ANTONIO	N	N	N	1	1	0	SBL_TEMPLATE_SN...	
3	2022-06-02 07:07:...	BILLING	N	N	N	1	0	0	ACCOUNTADMIN	
4	2020-04-15 05:12:2...	CERTIFICATION	N	N	Y	1	1	0	ACCOUNTADMIN	
5	2022-06-02 07:05:...	CUSTOMER_SERVICE	N	N	N	1	0	0	ACCOUNTADMIN	
6	2020-05-06 00:56:...	DATALIFT_ROLE	N	N	Y	1	2	0	ACCOUNTADMIN	
7	2022-06-27 01:12:4...	Direct Marketing	N	N	N	1	0	1	SBL_TEMPLATE_SN...	
8	2022-01-27 13:27:5...	FIVETRAN_ROLE	N	N	Y	3	1	0	SECURITYADMIN	
9	2021-09-27 05:36:1...	GLOBAL_PS	N	N	N	1	0	0	ACCOUNTADMIN	
10	2021-10-22 04:38:4...	HR	N	N	Y	10	1	0	ACCOUNTADMIN	
11	2022-03-03 00:00:...	LAW	N	N	N	0	0	0	ACCOUNTADMIN	
12	2021-09-29 04:59:...	MARKETING	N	N	Y	11	1	0	ACCOUNTADMIN	

## General configuration

Colibra Protect synchronizes standards and rules with the source database(s) at regular intervals. This synchronization runs in the background on a configured frequency. By default, the frequency is every 60 minutes, but this is configurable through Settings → Services Configuration → 27 Colibra Protect.



**Important** If you do not have access to the **Service Configuration** tab, create a support ticket requesting the JVM Parameter be added to your Collibra Infrastructure Configuration: `-DPROTECT_SYNC_SCHEDULER_DELAY=PT60M`. After the parameter is added, restart Collibra so these changes take effect and the policies are now synchronized with the cloud provider.

Synchronization includes:

1. Aggregate all standards and rules computing:
  - which columns need to be masked for which groups.
  - which tables need to have a row filter.
  - which tables and columns need to be granted access.
2. On the source database(s) such as Snowflake:
  - create and apply maskings.
  - create and apply row filters.
  - grant access to groups on tables and/or columns (depending on the underlying database).

# Essentials for Collibra Protect

To use Collibra Protect to the best of its ability, you need to know the following things:

- [How to protect your data](#)
- [Technical background](#)
- [Data protection standards vs. data access rules](#)
- [Prescriptive paths](#)



# How to protect your data

## 1. Access management

The most basic line of protection is to make sure only the right people/groups have access to the data. Data here is referring to the tables and columns in your database. In Collibra Protect, you can grant specific groups access to parts of your data based on Collibra assets.

For example, it is easy to grant the HR team access to the US customers' data set. But, what if some parts of the US customers' data set need to be hidden from the HR team, because it contains restricted information, such as personally identifiable information (PII)? In that case, you can further protect your data by applying column-based protection or row-based protection.

**Note** Collibra Protect only grants access. It cannot revoke access from people/groups.

## 2. Column-based protection

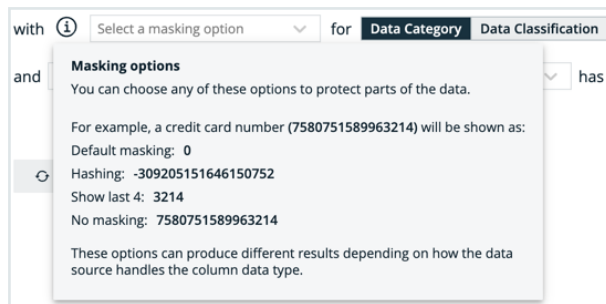
Column based protection allows you to target specific columns and mask their content. By masking the column's data, the group cannot see the content as it is. They will see a masked version of it instead.

For example, you can mask a column of credit card numbers, so the individual group cannot see the full credit card numbers.

We currently support four masking options. They include:

- **Default masking:** Shows the value as 0.
- **Hashing:** Converts the value into a variety of different letters, numbers, and symbols.
- **Show last:** Displays the last letters, numbers, and symbols in the value. You can choose to show the last 1 through 20 of the value. The most common choice is Show last 4.
- **No masking:** Displays the data value as it is originally written.





Collibra Protect allows you to choose to mask columns that are part of a **data category** or a **data classification**. While granting access to a certain asset, you can choose to apply this masking on only a subset of that asset if it is also part of a data category or data classification.

### 3. Row-based protection

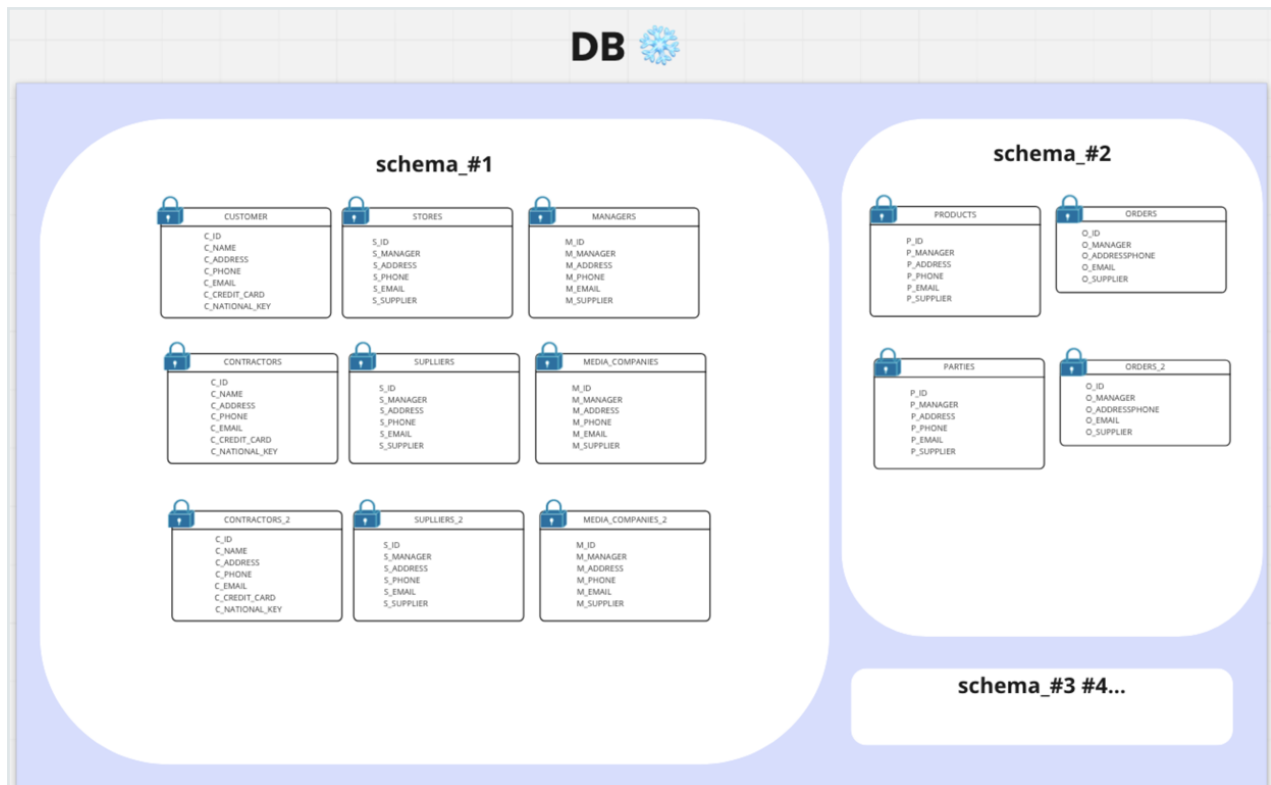
Another way to protect your data is to filter rows of a specific table. If you do not want to expose all of the existing items in a table because one of the columns is part of a certain data classification, you can easily leverage the Collibra operating model to do so.

When creating a rule that impacts certain tables in the source database, filter rows on tables by using the row filtering option for tables where one of their columns is part of a data classification. The filtering is based on what value is stored in the cell of that particular column. For instance, in a table that has a column that is classified as **country-code**, you can hide or show all items that have the value of **US**.

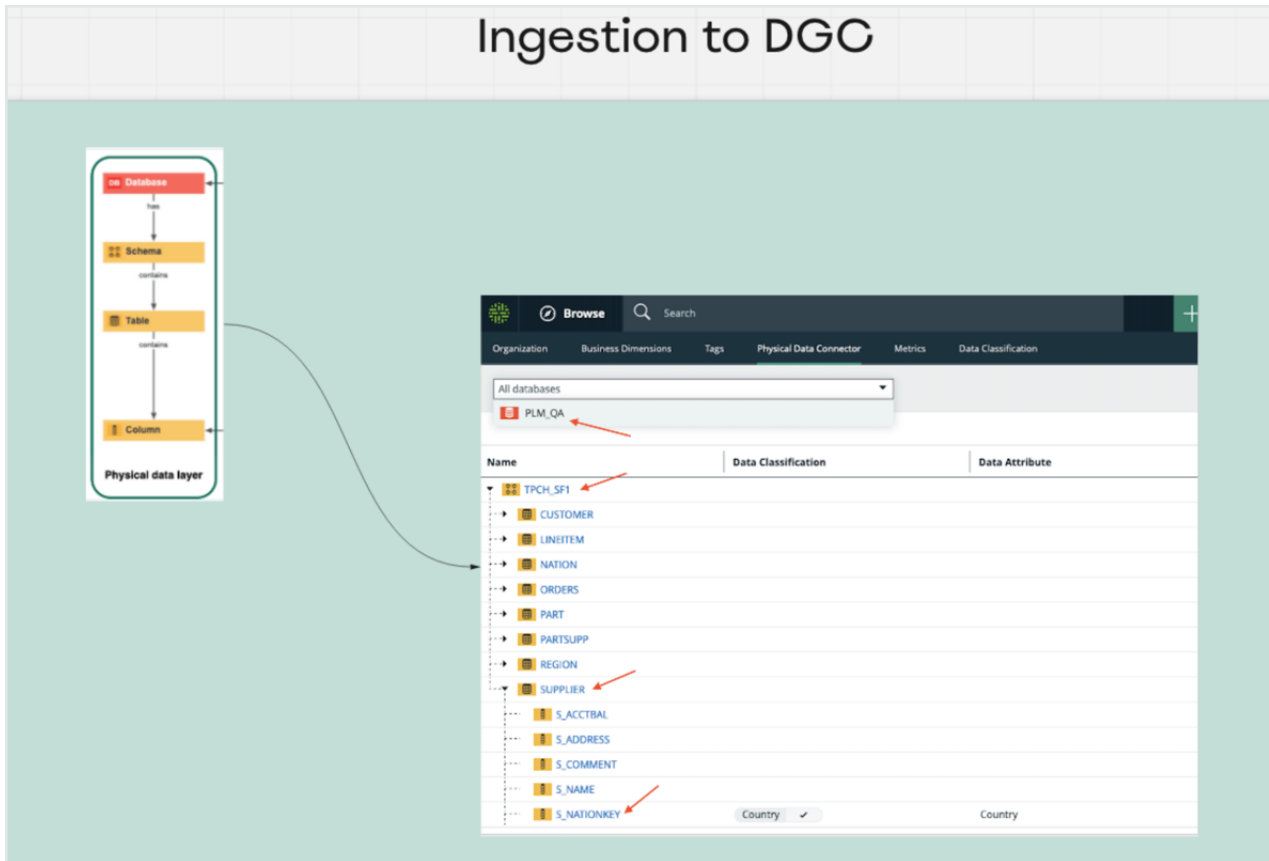
## Technical background

The technical background of Collibra Protect explains the connection of the data as it is in the database (DB) with the physical layer (equivalent assets in Collibra Data Intelligence Cloud) and the logical layer (the out of the box model).

Imagine you have this database:



When ingesting this DB to Collibra Data Intelligence Cloud, the physical layer is created as well as an asset for each of the schemas, tables, and columns.



Once there is a physical layer established in our Collibra environment, start creating the logical layer on top of it.

- In this phase, take any column and classify it as any data classification available, or let the platform classify it for you.
- Also, assign a column to a data attribute.

From here, create additional assets or use existing assets of different types (data set, data category, or business process) to establish a relation to these columns.

## Data protection standards vs. data access rules

Collibra Protect has both standards and rules to govern your data with ease and clarity.

<b>Standards</b>	<p>Data protection standards create a layer of protection for similar types of data by masking them wherever they are.</p> <p>For example, if columns with first and last names are a part of the PII data category, regardless what tables, schemas, and databases they are part of, create a standard that targets all of these columns by choosing the PII data category and masking it.</p>
<b>Rules</b>	<p>After establishing this primary layer (blanket) of protection to your most sensitive data, use data access rules to manage access and enhance protection for specific usages.</p> <p>For example, create a rule that grants access to a specific group, for a specific data set, while knowing that all PII within this data set will be masked by the standard we created before.</p>

## FAQs

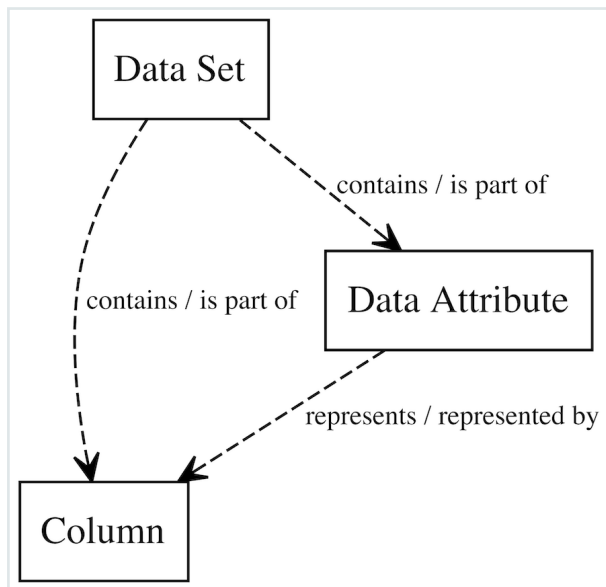
1. What if I want to grant access to a group without having the PII masked?
  - » When creating a rule for an asset that contains data masked by a standard, choose to override it by unmasking it or changing its masking type.
2. What If I want to grant access to a group, but the protection from the standard is not enough because there might also be other sensitive data within this supported asset?
  - » When creating a rule, add additional layers of protection over the ones that were set by any existing standard. Further protect the data by applying additional masking on or by filtering the data.

## Prescriptive paths

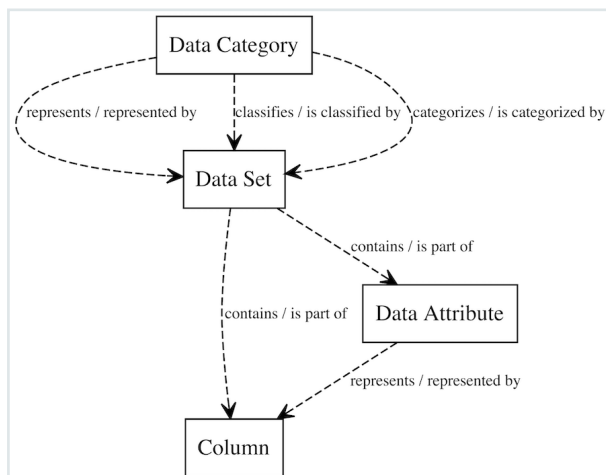
When creating a standard or rule, you select which asset(s) you want to protect and/or grant access to. By default, you can grant access to a data set, a data category, and a business process. Collibra Protect searches the knowledge graph, through relationships and/or intermediate assets, to find which set of physical data layer assets, such as columns and tables, this resolves.

The traversal of the knowledge graph is done through a set of prescriptive paths. For each type of asset, there is a set of prescriptive paths to traverse to the column assets. See the images below for more details.

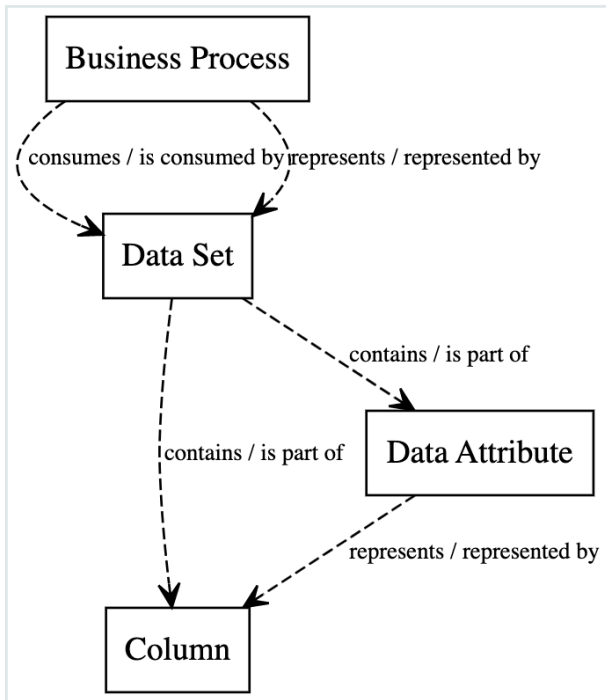
#### Prescriptive path for data set



#### Prescriptive path for data category



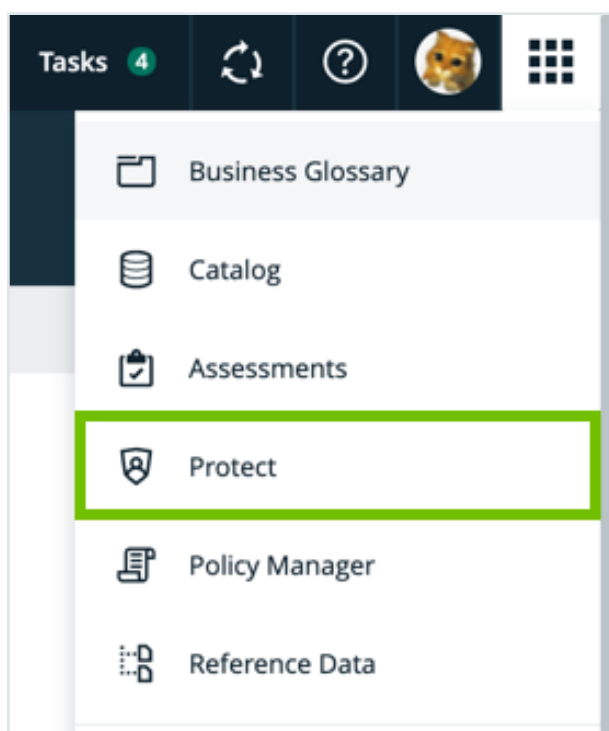
#### Prescriptive path for business process



# Overview of Collibra Protect

To work with Collibra Protect, ensure that you have a global role that has the Protect global permission and that it is [enabled](#) in your environment.

You will find, Collibra Protect, in the main menu . Click **Protect**.



If Collibra Protect is not shown on the menu, the feature is not enabled.

The landing page displays five tabs at the top of the page: **Data Protection Standards**, **Data Access Rules**, **Data Source Policies**, **Groups**, and **Audit**.

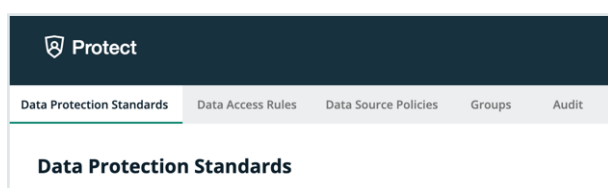
 Protect				
Data Protection Standards	Data Access Rules	Data Source Policies	Groups	Audit

Tab	Description
Data Protection Standards	<p>Define default data source access to data types based on data categories, data attributes, or classes/classifications through data protection standards</p> <p>Note Data access rules for particular groups can override created standards.</p>
Data Access Rules	Use data access rules to grant groups different access to the same data in data sets, in business processes, or identified by data categories.
Data Source Policies	View a list of policies that are currently active in the source data tables. You can also import policies from your source database using the Collibra Protect Data Source Policies API.
Groups	<p>Add groups through custom code via the Data Access API link and view existing current data access groups.</p> <p>Note You must add at least one group before you can create a standard or a rule.</p>
Audit	Generate an audit log for a preview of the last hour of ingested data from the data source.



## Data protection standards


The Data Protection Standards page contains an overview of the available standards in your environment.



Page Section	Description
Standards summary	Under the heading, there is a summary about data protection standards. Click the <b>Create a Data Protection Standard</b> button to <a href="#">create a standard</a> and get started in Collibra Protect.
Recently Modified Standards	This section shows the five most recently modified standards.
Standards table	This table displays a detailed view of the created data protection standards.

In the **Synchronization status** column of the standards table, there are five status options that can appear. To view the status of the standard in the data source, go to the source database.

Synchronization Status	Description
Active	This standard is currently active in Collibra Protect and in the data source.
Pending	This standard has been created or edited, and is pending synchronization.

Synchronization Status	Description
Failed	The synchronization of this standard has failed. Click the  icon next to the failed status to view additional information about the error.
Delete Pending	This standard will be deleted from the data source in the next synchronization.
Not Deleted	The deletion of this standard has failed.

**Note** Collibra Protect periodically synchronizes with the data source and statuses will be updated along with the synchronization. To learn more, go to the [general configuration](#) page.

# Create a data protection standard

Data protection standards create a layer of protection by masking data wherever they appear. Create a data protection standard to get started using Collibra Protect.

Create a Data Protection Standard

Data protection standards apply default data source access to types of data based on data categories or data classifications. Data Access Rules for particular groups will override these defaults.

Standard Name\*

Description

for the group\*  + -

protect\* Data Category Data Classification

with\* ⓘ

**Summary**  
 For the Group Human Resources  
 protect [Personal Information](#)  
 with Hashing

Cancel

Save Standard

## Steps

1. In Collibra Protect, go to the **Data Protection Standards** tab.
2. Click the green **Create a Data Protection Standard** button.
  - » The **Create Data Protection Standard** dialog box appears.
3. Enter the required information. It is important to note that when selecting assets, user permissions are defined in Collibra. If an asset is not visible for you, it will not appear as an option in the drop down menus.

Field	Description
Standard name	Name of the standard being created.

Field	Description
Description (optional)	Description of the standard.
Group	Group(s) for which the standard is created.
Data Category / Data Classification	A data category or data classification to apply the protection on.
Masking	Masking option for the standard.  <div> Note Click ⓘ to learn more about the masking options for standards. </div>

**Note** Click the plus sign to add more to each field where applicable. For example, after selecting a group, click + to add another group into the standard, and click – to delete a selected group. When entering the required information, you can view the selections you made in the **Summary** section.

4. Click the green **Save Standard** button.
  - » The saved data protection standard appears in the standards table.

## Modify a data protection standard


You can edit or delete a data protection standard after it has been created.

### Edit a standard

Editing a data protection standard might be necessary in certain situations. For example, change the masking method from default masking to hashing.

**Important** You will only be able to edit standard assets if you have view asset permissions. If one of the assets in the standard is unauthorized, you will not be able to edit the standard until the view access permission is granted.

## Steps

1. In the standards table, click the standard name, and then click the **Edit** button or click  in the appropriate row
  - » The **Edit a Data Protection Standard** dialog box appears.
2. Edit the [required information](#).
3. Click the green **Save Standard** button.
  - » The updated data protection standard appears in the standards table.

Edit a Data Protection Standard

Data protection standards apply default data source access to types of data based on data categories or data classifications. Data Access Rules for particular groups will override these defaults.


Standard Name \*

Description

for the group \*  + -

and the group  + -

protect \* **Data Category** **Data Classification**

with \* 

**Summary**  
 For the Group Human Resources and Marketing  
 protect [GDPR data related to criminal convictions and offences](#)  
 with Default masking


Cancel

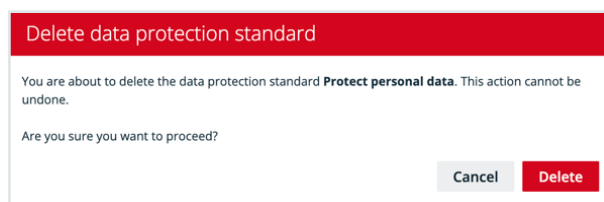
Save Standard

## Delete a standard

If you have an [author/admin role](#), delete a data protection standard that is no longer necessary.

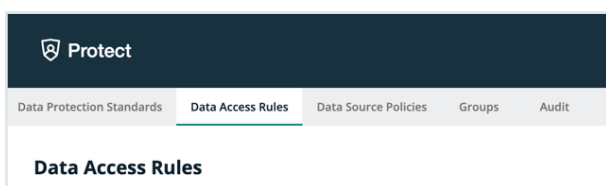
### Steps

1. In the standards table, click the  icon in the appropriate row  
» The **Delete data protection standard** dialog box appears.
2. Click the red **Delete** button.



## Data access rules


The Data Access Rules page contains an overview of the available rules in your environment.



Page Section	Description
Rules summary	Under the heading, there is a summary about data access rules. Click the <b>Create a Data Access Rule</b> button to <a href="#">create a standard</a> .
Recently Modified Rules	This section shows the five most recently modified rules.
Rules table	This table displays a detailed view of the created data access rules.

In the **Synchronization status** column, there are five status options that can appear. To view the status of the rule in the data source, go to the source database.

Synchronization Status	Description
Active	This rule is currently active in Collibra Protect and in the data source.
Pending	This rule has been created or edited, and is pending synchronization.

Synchronization Status	Description
Failed	The synchronization of this rule has failed. Click the  icon next to the failed status to view additional information about the error.
Delete Pending	This rule will be deleted from the data source in the next synchronization.
Not Deleted	The deletion of this rule has failed.

Note Collibra Protect periodically synchronizes with the data source and statuses will be updated along with the synchronization. To learn more, go to the [general configuration](#) page.



# Create a data access rule

After establishing a primary layer (blanket) of protection to your most sensitive data using standards, create data access rules to manage access to the data sources and enhance protection for specific usages.

Create a Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category and you can also conditionally filter rows based on code set values.

Rule Name \*

Marketing GI Rule

Description

Set rule for the marketing group for the geographic information asset  
Apply default masking for genetic data

Set rule for

group \* Marketing

asset \* Geographic Information

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ Default masking for Data Category Data Classification Genetic data

and Select an action rows where Unauthorized has Select a code set Select a code value

**Summary**

Grant access to Marketing  
for [Geographic Information](#)  
with Default masking for [Genetic data](#)


Generate Preview

Cancel Save Rule

## Steps

1. In Collibra Protect, go to the **Data Access Rules** tab.
2. Click the green **Create a Data Access Rule** button.
  - » The **Create a Data Access Rule** dialog box appears.
3. Enter the required information. It is important to note that when selecting assets, user permissions are defined in Collibra. If an asset is not visible for you, it will not appear as an option in the drop down menus.

Field	Description
Rule name	Name of the rule being created
Description (optional)	Description of the rule.
Group	Group for which the rule is being created.
Asset Name	Data asset that the rule is protecting. Collibra Protect enables you to protect the following asset types: Business process, data set, and data category. Learn more in <a href="#">technical background</a> and <a href="#">prescriptive paths</a> .

Field	Description
Masking (optional) <ul style="list-style-type: none"> <li>Data Category / Data Classification</li> </ul>	Masking option for the rule. Click the  to learn more about masking options. <ul style="list-style-type: none"> <li>Select a data category or a data classification to apply masking to.</li> </ul>
Action (optional) <ul style="list-style-type: none"> <li>Data Classification</li> <li>Code Set</li> <li>Code Value</li> </ul>	Filter the data by selecting hide or show. <ul style="list-style-type: none"> <li>Select data classification that is either hidden or shown</li> <li>Code set to set up row filtering in the tables. A code set must be selected to filter by a code value.</li> <li>Code value of the code set selected.</li> </ul>

**Important** The grant access checkbox is selected by default. By leaving this checkbox selected, you are granting access to the tables in the database with columns linked to the selected assets to the selected group(s). If you do not

want to grant this kind of access to these groups, clear the grant access checkbox.

**Note** Click the plus sign to add more to each field where applicable. For example, after selecting a group, click **+** to add another group into the standard, and click **–** to delete a selected group. When entering the required information, you can view the selections you made in the **Summary** section.

4. Click **Generate Preview** to see a preview of the new rule.

**Summary**

Grant access to Marketing  
for [Geographic Information](#)  
with Default masking for [Genetic data](#)

**Generate Preview**

**Geographic Information** ▼

Column ↑	Access	Masking Agent	Masking	Code Value
C_ADDRESS_sdfxgxfhcjhvjvbkjbkjbjhgxdfs...	Masked	Genetic data	0	
C_NAME	Masked	Genetic data	0	
DS_TBL0001_COL0001	Masked	Genetic data	0	

Cancel **Save Rule**

**Tip** Use the preview to verify the data access rule is set up correctly. The preview only shows the first 1,000 affected columns. The drop-down below the **Generate Preview** button is used to switch between the different selected assets in the rule. Each asset has its own preview table.

5. Click the green **Save Rule** button.
  - » The saved data access rule appears in the rules table.

## Modify a data access rule


You can edit or delete a data access rule after it has been created.

## Edit a rule

Editing a data access rule might be necessary in certain situations. For example, change the code set value from BE to US.

**Important** You will only be able to edit rule assets if you have view asset permissions. If one of the assets in the rule is unauthorized, you will not be able to edit the rule until the view access permission is granted.

### Steps

1. In the rules table, click the rule name, and then click the **Edit** button or click  in the appropriate row
  - » The **Edit a Data Access Rule** dialog box appears.
2. Edit the [required information](#).
3. Click the green **Save Rule** button.
  - » The updated data access rule appears in the rules table

Edit a Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category and you can also conditionally filter rows based on code set values.

Rule Name\*  
MH Rule 1

Description

Set rule for

group\* Marketing

asset\* Customer Data

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with Hashing for Data Category Data Classification Personal Information

and Select an action rows where Unauthorized has Select a code set Select a code value

**Summary**  
Grant access to Marketing  
for Customer Data  
with Hashing for Personal Information


Generate Preview

Cancel Save Rule

## Delete a rule

If you have an [author/admin role](#), delete a data access rule that is no longer necessary.

## Steps

1. In the rules table, click the  icon in the appropriate row
  - » The **Delete data access rule** dialog box appears.
2. Click the red **Delete** button.

Delete data access rule

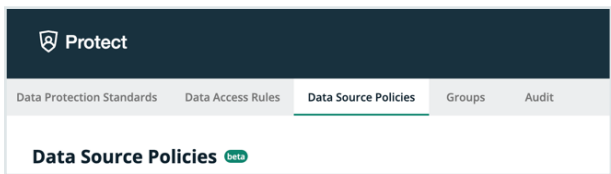
You are about to delete the data access rule **Rule 1**. This action cannot be undone.

Are you sure you want to proceed?

Cancel Delete

# Data source policies

The Data Source Policies page contains an overview of the available policies in your environment.



The data protection policy table displays a list of policies that are currently active in the source data tables. This includes policies that were created via Collibra Protect as well as policies that were created in the data source manually.

**Note** Collibra Protect currently only supports the Snowflake data source.

The table columns include:

Column name	Description
Data Protection Policy Name	Policies that originated in Collibra Protect have this structure: [DB name].[SCHEMA name].[policy type*].[asset id].  *Policy type can also be masking/row-filtering
Policy Logic	This column contains the SQL command that is executed in Snowflake whenever the user tries to access the protected object and will determine how to display the data to the user.
Tags	For policies that originated in a standard, this column lists the name of the attached tag. The convention is that each tag has the name of the asset that is included in that standard.

The screenshot shows the Collibra Protect web application. At the top is a navigation bar with 'Protect' and tabs for 'Data Protection Standards', 'Data Access Rules', 'Data Source Policies' (selected), 'Groups', and 'Audit'. Below the tabs, the 'Data Source Policies' section is active, displaying a list of policies. The table has three columns: 'Data Protection Policy Name', 'Policy Logic', and 'Tags'. The policies listed are all of type 'PROTECT\_QA.MASKING.COLLIBRA.MASKING\_POLICY' with various IDs. Each policy's logic is 'create or replace masking policy' followed by a complex SQL expression. The tags for most policies include 'PROTECT\_QA.MASKING.Personally Identifiable Information'.

Data Protection Policy Name	Policy Logic	Tags
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/380323eb-eb2f-46c4-9d46-19a8532827b...	create or replace masking policy "COLLIBRA/MASKING_POLICY/380323eb-eb2f-46c4-9d46-19a8532827b6/INTDGE..." as (VAL NUMBER(38,0)) ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/ARRAY" as (VAL ARRAY) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/ARRAY" as (VAL ARRAY) returns ...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BINARY" as (VAL BINARY(8388608...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BOOLEAN" as (VAL BOOLEAN) retu...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/BOOLEAN" as (VAL BOOLEAN) retu...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/DATE" as (VAL DATE) returns DA...	"PROTECT_QA.MASKING.Personally Identifiable Information"
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	
PROTECT_QA.MASKING.COLLIBRA.MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd...	create or replace masking policy "COLLIBRA/MASKING_POLICY/52e3b47a-0fda-43f0-9a00-4212c0b089dd/FLOAT" as (VAL FLOAT) returns ...	

# Types of policies on Snowflake

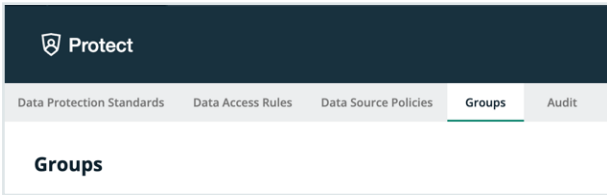
There are three types of policies on Snowflake: Column-based policies, row access policies, and tag-based policies. Each type can be created in Collibra Protect or on Snowflake.

For rules, policies are created directly on the column level. Row access policies are created when row filters are specified. For standards, the policy is created, attached to a Snowflake tag, and attached to the tab on any affected column.



# Groups

The Groups page contains an overview of the created Collibra Protect groups in your environment.



The groups table displays a list of groups that are currently active in the data source.

Protect			
Data Protection Standards	Data Access Rules	Data Source Policies	Groups
Audit			
Groups			
<div><div>Adding Groups</div><div>To add a group, you have to use the <a href="#">Collibra Protect Group API</a>. Currently, only Snowflake data sources are supported.</div></div>			
Group Name	System Reference	Created By	Created date
CID	"Snowflake": "string"	Admin Istrator	Jun 16, 2022, 8:52 AM
Human Resources	"Snowflake": "HR"	Admin Istrator	May 11, 2022, 11:39 AM
Marketing	"Snowflake": "MARKETING"	Admin Istrator	May 11, 2022, 11:39 AM

**Note** Collibra Protect currently only supports the Snowflake data source.

The table columns include:

Column name	Description
Group Name	Name of the Collibra Protect group
System Reference	
Created By	User who created the Collibra Protect group
Created Date	Date the group was created

## Adding groups in Collibra Protect

To add a group, use the [Collibra Protect Group API link](#). This action must be done before any data protection standards or data access rules can be created.

# Audit

An audit log contains information about the queries that were run to access the data and the data that was accessed.

## Generate an audit log

You can generate an audit log of access records from the data source on the **Audit** page.

**Note** The time that it takes for the actions performed in a data source to appear in an audit log in Collibra Protect varies from several minutes to hours, depending on the data source.

## Steps

1. In Collibra Protect, click the **Audit** tab.
2. Click one of the following buttons: **Today**, **Yesterday**, **A week ago**, **30 days ago**.

**Tip** The start date corresponding to the button that you clicked is shown in the **Start Date** field. Alternatively, you can enter or select a date in the **Start Date** field, and then click **Generate Log**.

» The audit log is generated.

### Important

- Generating an audit log may take up to a minute. After clicking **Generate Log**, do not navigate away from the **Audit** page because doing so cancels the audit log generation.

- The audit log contains the first 1,000 records from the selected start date. If you want to view the remaining records, contact your data source administrator.

**Audit** Data

Today

Yesterday

A week ago

30 days ago

Start Date  
09/29/2022

Generate Log

For audit log generation, data sources may have latency to summarize access records. Logs generated here for today may not contain information for the most recent access.

Query ID	Query Start Time	Source User Name	Direct Objects Accessed	Base Objects Accessed
01a74800-0501-ec9a-0001-000306f6b19e	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.MAIN_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ec9a-0001-000306f6b1a2	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.MAIN_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ea46-0001-000306f69dd2	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.DEPENDS_ON_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE
01a74800-0501-ec9a-0001-000306f6b1a6	Sep 29, 2022, 2:00 AM	MELIK	TEST_DB.PUBLIC.NODES_DEPENDS_ON_EXAMPLE	TEST_DB.PUBLIC.MAIN_EXAMPLE

# Audit log data

The following table describes the columns that are shown in an audit log.

Column	Description
Query ID	The ID of the query in the source database.
Query Start Time	The date and time of the query in the source database.
Source User Name	The name of the user in the source database who ran the query to access the data.
Direct Object Accessed	The database object (a table or a view) that was used to access the data.
Base Object Accessed	The database object that was accessed.

# Why rules or standards fail

Certain rules or standards may fail due to logical errors. This section describes some of the common scenarios that cause them to fail.



# Different types of masking affecting the same column

This topic contains examples to describe how data protection standards and data access rules behave when different types of masking affect the same column.

**Note** In the topic, the term *agent* refers to a data category or a data classification.

## Masking within a rule

### Scenario

A rule that is set for a group masks multiple agents using different types of masking, and the agents share the same column. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

### Example

Consider a rule that is set for the **Marketing** group. The rule masks the **Personal Information** data category by hashing and masks the **Personal and family details** data category by showing only the last two digits. Suppose that both these data categories share the same column. Then, the rule will fail because the same column cannot be masked using two different masking types for a given group.

Rule Name \*

Masking within a rule

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

and the asset

Audit & Internal Controls

+

-

☒ Grant access to all data tables linked to these asset columns.  
 By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Hashing

for

Data Category

Data Classification

Personal Information

+

-

with ⓘ

Show last

2

for

Data Category

Data Classification

Personal and family details

+

-

and

Select an action

rows where

Select a data classification

has

Select a code set

Select a code value

Summary

Grant access to Marketing

for Customer Data and Audit & Internal Controls

with Hashing for Personal Information and

with Show last 2 characters for Personal and family details

## Masking between rules

This scenario is similar to the [previous scenario](#) except that this scenario considers two rules, instead of one, that are set for the same group. The masking types for the agents in the two rules are different, and both the agents share the same column. Then, a conflict occurs because the same column cannot be masked using two different masking types for a given group.

When two rules conflict with each other, if the synchronization status of only one of them is **Active**, then the other rule fails. If, however, the synchronization status of both the rules is **Active** or **Pending**, then both of them fail.

This scenario is applicable regardless of whether the agents are the same or different, and regardless of whether the rule applies to a single asset or multiple assets.

Rule Name \*  
Masking between rules - 1

Description

Set rule for

group \*  
Marketing

asset \*  
Customer Data

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with 

Hashing

 for 

Data Category

Data Classification

Personal Information

and 

Select an action

 rows where 

Select a data classification

 has 

Select a code set

Select a code value

Summary

Grant access to Marketing  
for [Customer Data](#)  
with Hashing for [Personal Information](#)

Rule Name \*  
Masking between rules - 2

Description

Set rule for

group \*  
Marketing

asset \*  
Audit & Internal Controls

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with 

Show last

 2 for 

Data Category

Data Classification

Personal and family details

and 

Select an action

 rows where 

Select a data classification

 has 

Select a code set

Select a code value

Summary

Grant access to Marketing  
for [Audit & Internal Controls](#)  
with Show last 2 characters for [Personal and family details](#)

Masking between standards

Scenario

Two standards mask different agents, and the agents share the same column. This scenario is applicable regardless of whether the groups and the masking types are the same or different.



## Example

Consider two standards. The first standard masks the **Personal Information** data category, and the second standard masks the **Name** data classification. Suppose that both the agents share the same column. Then, a conflict occurs because more than one standard cannot be applied to the same column via different agents.

**Note** This is a limitation on how Collibra Protect implements standards on Snowflake.

If two standards affect the same column, you may not be able to view the column data in the data source.

Standard Name \*

Masking between standards - 1

Description

for the group \*

Marketing

+

-

protect \*

Data Category

Data Classification

Personal Information

with \*

i

Hashing

**Summary**

For the Group Marketing

protect [Personal Information](#)

with Hashing

Standard Name \*

Masking between standards - 2

Description

for the group \*

Human Resources

+

-

protect \*

Data Category

Data Classification

Name

with \*

i

Show last

2

Summary

For the Group Human Resources

protect [Name](#)

with Show last 2

## Conflicting filters affecting the same column

This topic contains examples to describe how data protection standards and data access rules behave when conflicting filters affect the same column.

### Filtering within a rule for the same data classification

#### Scenario

A rule that is set for a group contains conflicting filters for the same data classification. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

#### Example

Consider a rule that is set for the **Marketing** group and the **Customer Data** asset. The rule contains two filters for the **Country** data classification.

Rule Name \*

Filtering within a rule for the same data classification

Description

Set rule for

group \* Marketing

asset \* Customer Data

☒ Grant access to all data tables linked to these asset columns.

By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ Select a masking option for Data Category Data Classification Select a data category

and Show rows where Country has Country code BE

and Hide rows where Country has Country code PL

**Summary**

Grant access to Marketing  
for Customer Data  
and Show rows where Country has Country code: BE  
and Hide rows where Country has Country code: PL

If any of the tables in the asset contain a column that is classified as **Country**:

- The first filter shows the rows that contain **BE** in that column.
- The second filter hides the rows that contain **PL** in that column.

Then, this rule will fail because two conflicting filters affect the same column.

When applying a filter for a specific data classification, you must select only one type of action. That is, you can choose to either show rows based on one or more values or hide rows based on one or more values. You must not use the show and hide filter actions together for the same data classification.

## Filtering within a rule for different data classifications

### Scenario

A rule that is set for a group contains conflicting filters for different data classifications that share the same column. This scenario is applicable regardless of whether the rule applies to a single asset or multiple assets.

## Example

Consider a rule that is set for the **Marketing** group and the **Customer Data** asset. The rule contains two filters: one for the **Country** data classification, and another for the **State** data classification.

Rule Name \*

Filtering within a rule for different data classifications

Description

Set rule for

group \*

Marketing

+

-

asset \*

Customer Data

+

-

☒ Grant access to all data tables linked to these asset columns.  
By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Collibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category

Data Classification

Select a data category

and

Show

rows where

Country

has

Country code

BE

+

-

and

Hide

rows where

State

has

Country code

PL

+

-

Summary

Grant access to Marketing for Customer Data and Show rows where Country has Country code: BE and Hide rows where State has Country code: PL

If any of the tables in the asset contain columns that are classified as **Country**, the first filter shows only the rows that contain **BE** in those columns.

If any of the tables in the asset contain columns that are classified as **State**, the second filter hides only the rows that contain **PL** in those columns.

Suppose that a column is classified as both **Country** and **State**. That is, data classifications **Country** and **State** share the same column. Then, this rule will fail because two conflicting filters affect the same column.

### Filtering between rules for same or different data classifications

This scenario is similar to the [previous scenarios](#) except that this scenario considers two rules, instead of one, that are set for the same group. The filter in one rule is different from the filter in the other rule, and both the filters affect the same column. Then, a conflict occurs because two conflicting filters affect the same column.

When two rules conflict with each other, if the synchronization status of only one of them is **Active**, then the other rule fails. If, however, the synchronization status of both the rules is **Active** or **Pending**, then both of them fail.

Rule Name \*

Filtering between rules for same or different data classifications - 1

Description

Set rule for

group \*
Marketing
+
-

asset \*
Customer Data
+
-

☒ Grant access to all data tables linked to these asset columns.  
By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category
Data Classification

Select a data category

and
Show
rows where
Country
has
Country code
BE
+
-

**Summary**  
Grant access to Marketing  
for [Customer Data](#)  
and Show rows where [Country](#) has [Country code: BE](#)

Rule Name \*

Filtering between rules for same or different data classifications - 2

Description

Set rule for

group \*
Marketing
+
-

asset \*
Personal Information
+
-

☒ Grant access to all data tables linked to these asset columns.  
By checking this box, access will be given to tables in the database that are linked to the selected assets. If this box is unchecked, no access will be given to the selected tables. Note: Once the rule granting access is saved and synchronized, access to these tables cannot be revoked through Colibra Protect. It can only be revoked by direct action on the data source.

with ⓘ

Select a masking option

for

Data Category
Data Classification

Select a data category

and
Hide
rows where
Country
has
Country code
PL
+
-

**Summary**  
Grant access to Marketing  
for [Personal Information](#)  
and Hide rows where [Country](#) has [Country code: PL](#)

# Reference

Collibra Protect periodically synchronizes with an aggregation of all data protection standards and data access rules. These standards and rules form a data source-agnostic representation containing all databases, schemas, tables, and columns, as well as their protections and accesses. The synchronization process then triggers the [Edge capabilities](#), such as Collibra Protect for Snowflake. These Edge capabilities are responsible for translating the representation to actions toward the data source provider using their technology. This process might involve JDBC and REST calls to perform low-level operations to guarantee that the protections and accesses are applied.

## Protect for Snowflake

Data protection standards in Collibra Protect rely on the [tag-based masking policies](#) of Snowflake. The name of the data category or data classification selected in a standard becomes a tag with the same name. The tag is applied to all the affected columns to enforce data protection. For more information, go to [Example](#).

## Example

This topic contains an example to describe how Snowflake behaves in relation to certain data protection standards and data access rules.

### Introduction

This example describes the behavior in Snowflake when a standard is applied to a data category and a rule is applied to a data set with categorized columns in Protect.

The example considers the following:

- A standard created for the **Everyone**, **Human Resources**, **Marketing**, and **Sales** groups, to protect the columns in the **Personally Identifiable Information** data category by default masking.

- A rule created for the **Human Resources** group and the **Employee Data** asset, without any protection applied to the columns in the **Personally Identifiable Information** data category.

## Standard

When the **standard** is synchronized and active, the standard results in 14 masking policies—one policy for each **Snowflake data type**. The masking policies are created at the schema level with the following naming convention: **COLLIBRA/MASKING\_POLICY/<asset ID>/<snowflake type>**.

Results Data Preview						
<div> <span>Query ID</span> <span>SQL</span> <span>84ms</span> <span>18 rows</span> </div> <div> <input type="text" value="Filter result..."/> <span>Download</span> <span>Copy</span> </div>						
Row	created_on	name	database_name	schema_name	kind	owner
1	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/ARRAY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
2	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/BINARY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
3	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/BOOLEAN	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
4	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/DATE	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
5	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/FLOAT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
6	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/GEOGRAPHY	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
7	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/NUMBER	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
8	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/OBJECT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
9	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/STRING	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
10	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIME	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
11	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
12	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP_LTZ	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
13	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/TIMESTAMP_TZ	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
14	2022-09-06 03:41:13...	COLLIBRA/MASKING_POLICY/28d226cc-0ab0-4d23-b912-985312fb36b1/VARIANT	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN

All the masking policies are then associated with the **Personally Identifiable Information** tag, which is created at the schema level and assigned to those columns that need to be protected. At runtime, Snowflake fetches the right masking policy based on the **column data type**.

35 SHOW TAGS; 36

Results Data Preview

✓ Query ID SQL 48ms 2 rows

Filter result...

Download Copy

Row	created_on	name	database_name	schema_name	owner	comment
1	2022-09-06 03:46:10.054...	Personally Identifiable Information	PROTECT_QA	DEMO	ACCOUNTADMIN	Generated by Collibra: 28d226cc-0ab0-4d23-b912-985312fb36b1

The following image shows a masking policy for the STRING data type. The data that is shown in the policy depends on the masking type selected in the standard. In the policy, `val` indicates the value as it is stored in the table.

Details

1	CASE
2	WHEN CURRENT_ROLE() = 'PUBLIC' THEN '*'
3	WHEN CURRENT_ROLE() = 'HR' THEN '*'
4	WHEN CURRENT_ROLE() = 'MARKETING' THEN '*'
5	WHEN CURRENT_ROLE() = 'SALES' THEN '*'
6	ELSE val
7	END

## Rule

A rule results in a combination of [grant instructions](#), [dynamic masking](#), and [row access policies](#).

Suppose that the **Employee Data** data set selected in the [rule](#) contains sensitive columns categorized as **Personally Identifiable Information**.

Business Analysts Community New Data Sets

Employee Data

Data Set Candidate ☆☆☆☆☆ (0) 0 0 5%

Add characteristic

Summary

Details

Data Elements

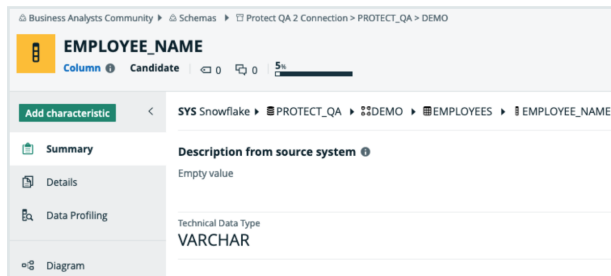
Sample data

<input type="checkbox"/>	# ↑	Name	is part of
<input type="checkbox"/>	1	EMPLOYEE_NAME	EMPLOYEES
<input type="checkbox"/>	2	EMP_ID	EMPLOYEES
<input type="checkbox"/>	7	DEPT_ID	EMPLOYEES
<input type="checkbox"/>	10	SALARY	EMPLOYEES

The [rule](#) grants access of the **Employee Data** data set to the **Human Resources** group, as indicated by the selected **Grant access...** checkbox in the rule. Then, the corresponding Snowflake role for the group can access each database, schema, and table in the data set. In addition, the column masking policy is applied to those columns that need to be protected.



Consider the **EMPLOYEE\_NAME** column in the **Employee Data** data set. This column belongs to the **EMPLOYEES** table within the **DEMO** schema in the **PROTECT\_QA** database.



In Snowflake, each column that is categorized as **Personally Identifiable Information** within the **Employee Data** dataset inherits the masking policy that is applied to the column in Protect. The masking policies created at the schema level use the following naming convention: **COLLIBRA/MASKING\_POLICY/<asset ID>**.

Row	created_at	name	database_name	schema_name	role	owner
16	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c64c5d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
17	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c64c5d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
18	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c64c5d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
19	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c64c5d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
20	2022-09-06 03:48:10.8...	COLLIBRAMASKING_POLICY7620d0b-af3a-41af-af44-c64c5d76d1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN

The following image shows the masking policy created for the **EMPLOYEE\_NAME** column.

Details	
1	CASE
2	WHEN CURRENT_ROLE() = 'HR' THEN val
3	WHEN CURRENT_ROLE() = 'PUBLIC' THEN '*'
4	WHEN CURRENT_ROLE() = 'MARKETING' THEN '*'
5	WHEN CURRENT_ROLE() = 'SALES' THEN '*'
6	ELSE val
7	END

## Behavior

According to the [standard](#), the **Everyone**, **Human Resources**, **Marketing**, and **Sales** groups have masked access to the data. However, according to the [rule](#), the **Human Resources** group has unmasked access to the data. As a result, the **EMPLOYEE\_NAME** column has both a policy tag and a column masking policy applied to it via the standard and the rule, respectively.

In Snowflake, if both a policy tag and a column masking policy exist for a column, the column masking policy takes precedence and the policy tag is not assigned to the column. To mitigate this behavior and ensure that the protection defined in the standard is not ignored, the column masking policy also considers the conditions defined in the standard (policy tag).

Thus, when a standard is created for the **Human Resources**, **Marketing**, and **Sales** groups to mask the **Personally Identifiable Information** column by default masking, and when a rule is created for the **Human Resources** group to not mask the same column, the result is as follows:

- The column is not masked for the **Human Resources** group.
- The column is masked for the **Marketing** and **Sales** groups via default masking.

## Masking and data types

Snowflake provides several functions to transform the data. This topic describes how Snowflake transforms the data for a given Protect masking type.

- **Default masking:** Snowflake does not support this masking type. Protect, however, uses the default masking type to apply protection to a wide range of data types. A default masking value is applied to each column according to the data type of the column.

### Default masking values for data types

Column data type	Snowflake data type	Default masking value
NUMBER	NUMBER	0
DECIMAL	NUMBER	0
NUMERIC	NUMBER	0
INT	NUMBER	0
INTEGER	NUMBER	0
BIGINT	NUMBER	0
SMALLINT	NUMBER	0
TINYINT	NUMBER	0
BYTEINT	FLOAT	0
FLOAT	FLOAT	0
FLOAT4	FLOAT	0
FLOAT8	FLOAT	0
DOUBLE	FLOAT	0

Column data type	Snowflake data type	Default masking value
DOUBLE PRECISION	FLOAT	0
REAL	FLOAT	0
VARCHAR	VARCHAR	*
CHAR	VARCHAR	*
CHARACTER	VARCHAR	*
STRING	VARCHAR	*
TEXT	VARCHAR	*
BINARY	BINARY	00
VARBINARY	BINARY	00
BOOLEAN	BOOLEAN	false
DATE	DATE	1970-01-01
DATETIME	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIME	TIME	00:00:00
TIMESTAMP	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIMESTAMP_LTZ	TIMESTAMP_LTZ	1969-12-31 16:00:00.000-0800  <div>Note This may change depending on the time zone.</div>

Column data type	Snowflake data type	Default masking value
TIMESTAMP_NTZ	TIMESTAMP_NTZ	1970-01-01 00:00:00.000
TIMESTAMP_TZ	TIMESTAMP_TZ	1969-12-31 16:00:00.000-0800  <div>Note This may change depending on the time zone.</div>
VARIANT	VARIANT	0
OBJECT	OBJECT	{}
ARRAY	ARRAY	[]
GEOGRAPHY	GEOGRAPHY	{"coordinates": [0,0], "type": "Point"} (aka point(0, 0) and visualization can change based on user preferences)

- **Hashing:** Uses the following Snowflake functions:
  - *SHA2* (for strings)
  - *HASH* (for numbers)
- **Show last:** Uses the following expressions:
  - *substr(to\_varchar(value), length(value) - n, n)* (for strings)
  - *mod(value, power(10,n))* (for numbers)

Tip In the expressions, *value* indicates the content and *n* indicates the number of characters to be shown.

- **No masking:** Returns the raw content.

**Note**

- You can apply the **Hashing** and **Show last** masking types to only the following Snowflake data types: FLOAT, NUMBER, and STRING.
- If a selected masking type cannot be applied to a certain data type—for example, when you attempt to apply the **Hashing** masking type to the DATE data type—the **Default masking** type is applied to the data type to guarantee protection.

## Snowflake privileges

To perform actions in Snowflake, Collibra Protect uses an Edge connection that must be configured with a user and a role that can manage grants; create and assign masking policies, row access policies, and tags; and manage usage access on databases and schemas involved in the protection. This enforcement role requires the following Snowflake privileges.

Snowflake privilege	Description
[APPLY MASKING], [APPLY ROW ACCESS], [APPLY TAG], [MANAGE GRANTS], [IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE]	Required for the role performing the actions.
[USAGE]	Required on each database and schemas where policies are applied to the role performing the actions.

Snowflake privilege	Description
[CREATE MASKING POLICY], [CREATE ROW ACCESS POLICY], [CREATE TAG]	Required on each schema where policies are applied to the role performing the actions.

## Example

Suppose that a role named PROTECT exists in Snowflake and is responsible for managing access on all schemas within a database named DEMO. Then, the following statements can be used to enable the Snowflake PROTECT role to perform the enforcement.

```
GRANT APPLY MASKING POLICY ON ACCOUNT TO ROLE PROTECT;
GRANT APPLY ROW ACCESS POLICY ON ACCOUNT TO ROLE PROTECT;
GRANT APPLY TAG ON ACCOUNT TO ROLE PROTECT;
GRANT MANAGE GRANTS ON ACCOUNT TO ROLE PROTECT;
GRANT IMPORTED PRIVILEGES ON DATABASE SNOWFLAKE TO ROLE PROTECT;
GRANT USAGE ON DATABASE DEMO TO ROLE PROTECT;
GRANT USAGE ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE MASKING POLICY ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE ROW ACCESS POLICY ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
GRANT CREATE TAG ON ALL SCHEMAS IN DATABASE DEMO TO ROLE PROTECT;
```