

Collibra Data Intelligence Cloud Collibra Protect



Collibra Data Intelligence CloudCollibra Data Governance Center - Collibra Protect

Release date: Thursday, November 3, 2022

Revision date: Thu Nov 03, 2022

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

Contents

Contents ii
About Collibra Protect i
Install Collibra Protect iii
Configure Collibra Protect
Essentials for Collibra Protect
Overview of Collibra Protect
Data protection standards
Data access rules
Data source policies
Groups
Audit
Why rules or standards fail
Reference documentation
Collibra Protect
About Collibra Protect
Install Collibra Protect ii
Configure Collibra Protect
Essentials for Collibra Protect
Overview of Collibra Protect
Data protection standardsxix
Data access rulesxxv
Data source policies
Groups

Audit	xxxviii
Why rules or standards fail	xl
Reference documentation	xlix

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 \rightarrow (Edge) Sites \rightarrow Your site \rightarrow Capability \rightarrow Add capability \rightarrow 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.

Ade	Database Can	didate ⊂ 0 ℃ 0			
1	Overview Tags Comments	Location Empty value			
°	Diagram Pictures	has Schema	Domain	Description	I
АА 90	Responsibilities References	PRESCRIPTIVE_PATH_SCHEMA	Snowflake > PLM_QA > PRESC Snowflake	Description	Ŷ
© &	History Files	is grouped by Technology As	set	Description	
	Configuration	Snowflake	New Applications		÷

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.

$\tfrac{200}{3007}$	🕖 Browse	Q	Search										+	₩	Tasks 🍞	Ç1	?		
¢ s	ettings General		Operating model	Roles and permis	sions V	Vorkflows	Users ar	nd groups	Services Configuration	on	Migration	Logs	Edge						
		<																_	
																	Add	0	
•	Global roles		Name †		Descriptio	'n		Required lic	ense	Me	mbers								
曲	Resource roles		Catalog Author					Standard		1	Admin Istrator								
	Global Parmissions		Data Dictionary					Read-only		A 8	Everyone								
~8	Global Permissions		DataSteward		Allows usa	ge of Data Stev	ward	Read-only		80	Everyone								
â	Resource Permission		DataSteward Auth	nor				Standard											
			Edge integration e	engineer	Allows mai	naging connect	tions	Standard											
			Edge manager		Allows crea	ating and delet	ing E	Standard											
			Edge site		Allows con	nection from E	dge	Standard		1	Edge privacy-ris	k-qa-25-07							
			Edge site administ	trator	Allows dov	vnloading Edge	e site	Standard										Ť	
			Glossary		Allows usa	ge of Business	Glo	Read-only											
			Helpdesk					Read-only		80	Everyone								
			Insights					Standard		A *	Everyone								
			Policy Manager					Read-only		88	Everyone								
			Protect Admin		In this role	, you have the	sam	Standard		1	Admin Istrator								
			Protect Author		In this role	, you can creat	e rul	Standard		1	Admin Istrator	💄 Autho	or User						
			Protect Manager		This is a ro	le for our syste	em u	Read-only		1	Edge privacy-risł	k-qa-25-07	1 Polic	y Lifecycl	e Managemer	nt API Use	r		
			Protect Reader		In this role	, you can view	Colli	Read-only		1	Reader User								
			ReferenceData		Allows usa	ge of Referenc	e Da	Read-only		8	Everyone								
			Sysadmin		Allows for	configuring an	d m	Standard		1	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 III menu. They also cannot navigate to protect related URLs or access protect endpoints.
Protect Author	Users in this role can create rules and stand- ards, view imported policies and groups, and generate audits 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 'pro- tect', 'protect_edit', and an extra 'protect_ administration' permission. This role is not assigned to anyone automatically.

Roles	Description
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. 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.

A Databases Share	Marketplace W	Varehouses Workshee	ts History Account	Partner Connect Help Notifications Snowsight ACCOUNTADMIN
Account				Last refreshed 9:39:49 AM
Usage Billing U	sers Roles	Policies Sessions	s Resource Monitors Reader Accounts	
🕂 Create 🗹 Edit 📿	Drop			
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.	
	10/22/2021, 1:30:58	ACCOUNTADMIN	Di M OL UD David Och Dala	
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.

Group	S									
Adding Gro To add a gr	oups roup, you have to use t	the <mark>Collibra Protect Gro</mark>	up API. <mark>Currently, or</mark>	nly Snowflake data so	urces are supported.					
Group Nam	ne	System	Reference			Created	Ву		Created Date	
*	Databases Shares	Marketplace Warehou	ses Worksheets	Q History Account			Partner Connect	Pelp Notificatio	Snowsight	ACCOUNTADMIN
Reset		HUMAN RESOURCES	SALES		✓ Roles	New Worksheet	Standard	I introspection	BILLING	+ • •
► Run	All Queries Saved	i 10 seconds ago					at AC	COUNTADMIN 🏭	• DEMO_WH (M) 🛢 PLM	_QA 👫 TPCH_SF1 🔹 🚥
Results D Query J Filter result	Data Preview I <u>D SQL</u> 90ms —	37 rows	v							← Open Histor
Results C Query J Filter resul	Data Preview ID SQL 90ms It rested on	37 rows	y is default	is current	is inherited	assigned to users	granted to roles	granted roles	owner	← Open Histor Columns ▼ ↓
Results C Query J Filter resul Row	Data Preview ID SQL 90ms it v created_on 1 2019-09-17 16:47.2	37 rows	y is_default N	is_current Y	is_inherited N	assigned_to_users	granted_to_roles	granted_roles 3	owner	+ Open Histor Columns + J comment Account administrat
Results C Query J Filter resul Row 1 2	Data Preview ID SQL 90ms it v created_on 1 2019-09-17 16:47.2 2 2022-06-27 01:10:4	37 rows 2 Cop name ACCOUNTADMIN ANTONIO	y is,default N	is_current Y	is_inherited N N	assigned_to_users 35 1	granted_to_roles 0 1	granted_roles 3 0	owner SBI_TEMPLATE_SN	+ Open Histor Columns + J comment Account administrat
Results C Query I Filter resul Row 1 2 3	Data Preview JD SQL 90ms itt created_on 2 2019-09-17 16:47.2 2022-06-27 01:10:4 3 2022-06-02 07:07 2022-06-02 07:07	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING	y is_default N N	is_current Y N	is_inherited N N	assigned_to_users 35 1	granted_to_roles 0 1 0	granted_roles 3 0 0	owner SBI_TEMPLATE_SN ACCOUNTADMIN	Open Histor Columns J Columns Account administrat
Results C Cuery J Filter result Row 1 2 3 4	Data Preview ID SQL 90ms itt 2 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07 4 2020-04-15 05:12:2	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION	y is_default N N N	is_current Y N N	is_inherited N N N Y	assigned_to_users 35 1 1 1	granted_to_roles 0 1 0 1	granted_roles 3 0 0 0	owner SBI_TEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN	Open Histor Columns Zonnent Account administrat
Results C Query.1 Filter result Row 1 2 3 4 5	Data Preview ID SQL 90ms itt 90ms 90ms 2 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07 4 2020-04-15 05:12:2 5 2022-06-02 07:05	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE	y is_default N N N N	is_current Y N N N N	is_inherited N N N Y N	assigned_to_users 35 1 1 1 1	granted_to_roles 0 1 0 1 0	granted_roles 3 0 0 0 0	owner SBI_TEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN	Open Histor Columns Zonnent Account administrat
Results C Query J Filter result Row 1 2 3 4 5 6	Data Preview ID SQL 90ms Ittac 90ms 90ms 2 2019-09-17 16:47:2 2 2022-06-22 07:10:4 3 2022-06-02 07:07 4 2020-04-15 05:12:2 5 2022-06-02 07:05 6 2020-05-06 00:56:	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE	y is_default N N N N	Is_current Y N N N N N	is_inherited N N Y N Y	assigned_to_users 35 1 1 1 1 1	granted_to_roles 0 1 0 1 0 2	granted_roles 3 0 0 0 0 0 0	owner SBILTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN	← Open Histor Columns ← ↓ comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7	Data Preview ID SQL 90ms Itt 0 created_on 2 2019-09-17 16:47:2 3 2022-06-22 01:10:4 4 2022-06-02 07:07 5 2022-06-02 07:07 6 2022-06-02 07:05 7 2020-05-06 00:56 7 2022-06-02 01:12:4	37 rows	y is_default N N N N N	Is_current Y N N N N N N	is_inherited N N Y N Y N	assigned_to_users 35 1 1 1 1 1 1 1	granted_to_roles 0 1 0 1 2 0 2	granted_roles 3 0 0 0 0 0 0 1	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN	← Open Histor Columns ▼ ↓ comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8	Data Preview ID SQL 90ms Itta 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07 4 2020-06-02 07:07 5 2022-06-02 07:05 6 2022-06-02 07:05 7 2020-05-06 00:56 7 2022-06-27 01:12:4 3 2022-01-27 13:27.5	37 rows	y is_default N N N N N N	Is_current Y N N N N N N N	is_inherited N N Y N Y N Y	assigned_to_users 35 1 1 1 1 1 1 1 1 3	granted_to_roles 0 1 0 1 0 2 0 1 0 1	granted_roles 3 0 0 0 0 0 0 1 1 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN	← Open Histor Columns ▼ ↓ comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8 9 9	Data Preview JD SQL 90ms Itta 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07 4 2020-06-02 07:07 5 2022-06-02 07:05 6 2022-06-02 07:05 7 2022-06-27 01:12:4 3 2022-01-27 11:12:4 3 2022-01-27 13:27.5 2 2021-01-27 04:39.4.9.4.9.4.9.4.9.4.9.4.9.4.9.4.9.4.9.4	37 rows	y Is_default N N N N N N N N	Is_current Y N N N N N N N N N	is_inherited N N Y N Y N Y N Y	assigned_to_users 35 1 1 1 1 1 1 1 1 3 1 1 2 1	granted_to_roles 0 1 0 1 0 2 0 0 1 1 0 0 1 1 0	granted_roles 3 0 0 0 0 0 0 0 1 1 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN ACCOUNTADMIN ACCOUNTADMIN	← Open Histor Columns ▼ ↓ comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8 9 10 11	Data Preview ID SQL 90ms Itta 2019-09-17 1647.2 2 2022-06-27 0110-4 3 2022-06-02 07.07 4 2020-04-15 05.12.2 5 2022-06-02 07.07 4 2020-06-02 07.05 5 2020-06-27 01.12.4 3 2022-01-27 13.12.4 3 2022-01-27 13.12.4 3 2022-10-92 70.53.61 4 2021-10-22 04.38.4 3 2022-10-27 05.361 4 2022-30.80.09.07. 13.27.5	37 rows	y is_default N N N N N N N N N	Is_current Y N N N N N N N N N N N N	Is_inherited N N N Y N Y N Y N Y N Y N	assigned_to_users 35 1 1 1 1 1 1 1 1 3 1 10 0	granted_to_roles 0 1 0 1 0 2 0 0 1 1 0 1 0 1 0 0	granted_roles 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN ACCOUNTADMIN ACCOUNTADMIN	Open Histor Columns Zonment Account administrat

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 \rightarrow Services Configuration \rightarrow 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 Protectallows 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.

Ingestion to DGC
Image: control of the service in th

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.

Standards	Data protection standards create a layer of protection for similar types of data by masking them wherever they are.
	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 tar- gets all of these columns by choosing the PII data category and masking it.
Rules	After establishing this primary layer (blanket) of protection to your most sensitive data, use data access rules to man- age access and enhance protection for specific usages.
	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.

FAQs

- 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.
- 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

Audit Groups

Tab	Description
Data Protection Standards	Define default data source access to data types based on data categories, data attributes, or classes/classifications through data protection standards
	Note Data access rules for particular groups can override created standards.
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 Col- libra Protect Data Source Policies API.
Groups	Add groups through custom code via the Data Access API link and view existing current data access groups.
	Note You must add at least one group before you can create a standard or a rule.
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.

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

Page Section	Description
Standards summary	Under the heading, there is a summary about data protection standards. Click the Create a Data Protection Standard button to create a standard and get star- ted 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 Col- libra Protect and in the data source.

Synchronization Status	Description
Pending	This standard has been created or edited, and is pending synchronization.
Failed	The synchronization of this standard has failed. Click the 1 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 synchronization. To learn m	with the data source and statuses will be nore, 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.	
HR PII Standard	
Description Mask personal information for HR with hashing	
for the group * Human Resources	
with * (1) Hashing	
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 Clas- sification	A data category or data classification to apply the protection on.
Masking	Masking option for the standard.
	Note Click ^① to learn more about the masking options for standards.

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

- 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 particular groups will override these defaults.	access to types of data based on	n data categories or data classifications. Data Access Rules for
Standard Name*		
Tool tip standard		
Description		
for the group * Human Resources	~ +	-
and the group Marketing	~ +	-
protect* Data Category Data Classification	GDPR data related to criminal	al convictions and offences
with * (1) Default masking	~	
Summary For the Group Human Resources and Marketing protect GDPR data related to criminal convictions and with Default masking	l offences	
		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 $\hat{\bullet}$ 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.

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

Page Section	Description
Rules summary	Under the heading, there is a summary about data access rules. Click the Create a Data Access Rule button to create a standard.
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 Pro- tect 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 ① 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 synchronize be updated along with the synchronization. To	es with the data source and statuses will 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 \lor + -
asset * Geographic Information \lor + -
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 ① Default masking \vee for Data Category Data Classification Genetic data \vee + -
and Select an action \checkmark rows where Unauthorized \checkmark has Select a code set \checkmark Select a code value \checkmark
Summary
Grant access to Marketing
for Geographic Information with Default masking for Genetic data
O 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 pro- tecting. Protect enables you to protect the fol- lowing asset types: Business process, data set, and data cat- egory. Learn more in technical background and prescriptive paths.

Field	Description
Masking (optional) • Data Category / Data Classification	Masking option for the rule. Click the To learn more about masking options. • Select a data category or a data classification to apply masking to.

Field	Description
Action (optional)	Filter the data by
Data Classification	selecting hide or show.
 Code Set 	 Select data
• Code Value	classification that is either hidden or shown
	 Code set to set up row filtering in the tables. A code set must be selected to filter by a code value.
	 Code value of the code set selected.

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_sdfxgxcfhcjhvjbvkjbk,jbjhgxdfzs	Masked	Genetic data	0	
C_NAME	Masked	Genetic data	0	
DS_TBL0001_COL0001	Masked	Genetic data	0	
				Cancel Save Ru

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 *I* 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 \vee + -
asset * Customer Data v + -
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 (1) Hashing \vee for Data Category Data Classification Personal Information \vee + -
and Select an action rows where Unauthorized bas Select a code set Select a code value
Summary Grant access to Marketing for Customer Data with Hashing for Personal Information
O 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 \mathbf{i} icon in the appropriate row
 - » The Delete data access rule dialog box appears.
- 2. Click the red **Delete** button.



Data source policies

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

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

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 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.

Column name		Description	
Tags		For policies that original this column lists the name tag. The convention is the the name of the asset the that standard.	ated in a standard, me of the attached hat each tag has hat is included in
			+ 🕁 Tasks 🗷 🗘 🕐 👥 🏭
Data Source Policies This is a list of policies that are currently active in the source data tables. Data Protection Policy Mans 1 PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3823236b-bb2746/d4-3046-12426b089dL. PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3223b47a 0fda-4309-a00-4212ceb089dL. PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3	Policy Logic create or replace masking policy 'COLLIBMA/MAKING_POLICY/ create or replace masking policy 'COLLIBMA/MAKING_POLICY/	20032360-0017-000-42120000904/JNUTY as (VAL NUMBER(8,0,0)) 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMBER(8,0,0)) 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY(8)8608 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA.	Tags "PROTECT_QA.MASKING.Personally identifiable information" "PROTECT_QA.MASKING.Personally identifiable information"

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 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.

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

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

Protect				
Data Protection Standards Data Access Rule	s Data Source Policies Groups	Audit		
Groups				
Adding Groups To add a group, you have to use the Collibra P	rotect Group API. Currently, only Snowflake	data sources are supported.		
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 Protect group
System Reference	
Created By	User who created the Protect group

Column name	Description
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

The Audit page allows you to generate an audit log of access records from the data source .



Generate an audit log

Why would I need to generate an audit log?

Note The actions you take in Collibra Protect only appear in an audit log after one hour.

Steps

1. In Collibra Protect, go to the Audit tab.

Click one of the predefined time buttons (Today, Yesterday, A week ago, or 30 days ago) or use the date picker to specify a start date for the audit log.

- 2. Click the green Generate Log button.
 - » The audit log displays the first 1,000 records after the selected start time.

Note Important Generating an audit log can take some time. Do not navigate away from the page or your request is canceled. For full details, contact your data source administrator.

Audit cm Today Yesterday A week ago 30 days ago									
artuar Maryaozz									
Generate Log									
 For audit log generation, data sources may have laten 	cy to summarize access records. Logs generated here for today	r 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-ead6-0001-000306f69dd2	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					
01a74801-0501-ead6-0001-000306f69dda	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES					
01a74801-0501-ec9a-0001-000306f6b1b6	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM					
01a74801-0501-ec9a-0001-000306f6b1ba	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES					
01a74801-0501-ead6-0001-000306f69de2	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM					
01a74801-0501-ec9a-0001-000306f6b1be	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES					
01a74801-0501-ec9a-0001-000306f6b1c2	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM					
01974901.0501.er0s.0001.000206f6h1r6	Can 20 2022 2-01 AM	CEDTIEICATION	COLLIBDA TOCU CEDOL LINEITEM	COLLIBDA TOCH COOL LINEITEM					
4 1-50 51-100 101-150 701-712 ▶									

The audit log table columns include:

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

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

Note In this 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.

Masking within a rule				
Description				
Set rule for				
group* Marketing	~	+	-	
asset * Customer Data	~	+	-	
and the asset Audit & Internal Controls	\sim	+	-	
 Crant access to all data tables linked to these access column 				
By checking this box, access will be given to tables in the data	s. Ibase that are li	inked to	o the se	elected 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 the	se tables canno	ot be re	voked 1	through Collibra Protect. It can only be revoked by direct action on the data source.
with (i) Hashing v for Data Cat	egory Data (Classifi	cation	Personal Information V + -
with (1) Show last V 2 for Data Cat	egory Data (Classifi	cation	Personal and family details \vee + -
and Select an action V rows where Select a data class	ification	\sim	has	Select a code set V Select a code value V
Summary				
Summary Grant access to Marketing for Customer Data and Audit & Internal Controls				

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	e*							
Masking	between rules - 1							
Descriptior	n							
Set rule 1	for							
group *	Marketing	~	/	+	-			
asset *	Customer Data	~	/	+	-			
Gran By c rule	nt access to all data tables linked to the checking this box, access will be given to b granting access is saved and synchroniz	ese asset columns. tables in the database that ed, access to these tables c	are link annot l	ked to be rev	the se voked ti	lected assets. If this box is unchecked, no ac hrough Collibra Protect. It can only be revok	cess ed b	s will be given to the selected tables. Note: Once the yy direct action on the data source.
with (i	Hashing 🗸 🗸	for Data Category D	Data Cla	assific	ation	Personal Information	/	+ -
and set	lect an action	alact a data classification		5.4	hac	Select a code set		Select a code value
and Ser				v	Tids	Select a code set		Select a code value
lule Name	e*							
Masking	; between rules - 2							
Descriptior	n							
Set rule	for							
group *	Marketing	~	·	+	-			
asset *	Audit & Internal Controls	~	/	+	-			
🔽 Grai	int access to all data tables linked to the	ese asset columns.						
By c rule	checking this box, access will be given to e granting access is saved and synchroniz	tables in the database that ed, access to these tables o	are link annot l	ked to be rev	the se voked ti	lected assets. If this box is unchecked, no ac hrough Collibra Protect. It can only be revok	cess ed b	s will be given to the selected tables. Note: Once the by direct action on the data source.
with (i	Show last V	for Data Category D	Data Cla	assific	ation	Personal and family details	~	+ -
and Sel	lect an action v rows where	elect a data classification		\sim	has	Select a code set 🔍		Select a code value
Summa Grant acco	ary ess to Marketing							
for Audit 8 with Show	& Internal Controls w last 2 characters for Personal and famil	y 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.

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

Standard Name *		
Masking between standards - 1		
Description		
for the group * Marketing	~ + -	
protect* Data Category Data Classification	Personal Information	~
with * (i) Hashing	\checkmark	
Summary		
For the Group Marketing		
protect Personal Information with Hashing		

Masking between standards - 2		
Description		
Securitori		
for the group * Human Resources	~ + -	
protect [*] Data Category Data Classification	Name	\sim
with * (i) Show last	2	
Summary		
⁻ or the Group Human Resources		

Conflicting filters affecting 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.

iltering within a rul	e for the same	e data classific	ation								
escription											
t rule for											
oup * Marketing				~	+ -						
	D-t-				1						
set * Customer [Data			~	+ -						
set * Customer I	Data o all data table	es linked to th	nese asset column	s.	+ -						
 Grant access to 	Data o all data table s box, access v	es linked to th vill be given to	nese asset column	s. base that are link	+ –	elected assets. If this box is unche	cked, no acces	s will be given to th	e selected tables. No	te: Once	the
 Grant access to By checking this rule granting accession 	Data o all data table s box, access v ccess is saved a	es linked to th vill be given to and synchron	n ese asset column b tables in the datal ized, access to thes	s. base that are link se tables cannot b	+ – ed to the s	elected assets. If this box is unche through Collibra Protect. It can or	ecked, no acces	s will be given to th by direct action on t	e selected tables. No :he data source.	te: Once	the
 Grant access to By checking this rule granting ac th (1) Select a 	Data o all data table s box, access v ccess is saved a masking optic	es linked to th vill be given to and synchron	hese asset column b tables in the datal ized, access to thes	s. base that are link te tables cannot b	ed to the servoked	elected assets. If this box is unche through Collibra Protect. It can on Select a data category	cked, no acces	s will be given to th by direct action on t	e selected tables. No he data source.	te: Once	the
set * Customer I Grant access to By checking this rule granting ac th (1) Select a	Data o all data table s box, access v ccess is saved a a masking optic	es linked to th will be given to and synchron	nese asset column o tables in the datai ized, access to thes for Data Cate	s. base that are link se tables cannot b egory Data Cla	+ –	elected assets. If this box is unche through Collibra Protect. It can on Select a data category	ecked, no acces aly be revoked	s will be given to th by direct action on 1	e selected tables. No he data source.	te: Once	the
set * Customer I Grant access to By checking this rule granting ac th (1) Select a d Show	Data o all data table s box, access v ccess is saved a a masking optio	es linked to th vill be given to and synchron on	bese asset column o tables in the datal ized, access to thes for Data Cato Country	s. base that are link se tables cannot b egory Data Cla	+ – ed to the e revoked ssification	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces ly be revoked	s will be given to th by direct action on 1 BE	e selected tables. No che data source.	te: Once +	the
set * Customer I G Grant access to By checking this rule granting ac th ① Select a id Show d Hide	Data o all data table s box, access w ccess is saved a a masking option rc	es linked to the vill be given to and synchron on v ows where	hese asset column tables in the datal ized, access to thes for Data Cate Country	s. base that are link ie tables cannot the egory Data Cla	+ – ed to the e e revoked ssification ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	icked, no acces nly be revoked	s will be given to th by direct action on I BE PI	e selected tables. No the data source.	te: Once + +	
Set * Customer I By checking this rule granting ac th (1) Select a and Show ad Hide	Data Data a all data table s box, access v ccess is saved a a masking optic rc rc rc	es linked to th vill be given to and synchron on v ows where [bese asset column tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link te tables cannot t egory Data Cla	+ – ed to the e revoked ssification w ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces	s will be given to th by direct action on I BE PL	e selected tables. No the data source.	te: Once + +	
set * Customer I Grant access to By checking this rule granting ac th ① Select a ind Show ind Hide Jummary	Data Data a all data table s box, access v ccess is saved a a masking optic v rc	es linked to th vill be given to and synchron on v ows where ows where	hese asset column o tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link base that are link to base cannot t egory Data Cla	+ – ed to the e e revoked ssification v ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces	s will be given to th by direct action on 1 BE PL	e selected tables. No he data source.	+ +	
sset * Customer I Grant access to By checking this rule granting ac ith ① Select a nd Show nd Hide JIMMARY ant access to Mark	Data Data table s box, access w ccess is saved a masking optic rc rc rc eting	es linked to th will be given to and synchron on v bows where bows where	hese asset column o tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link base that are link to base cannot t egory Data Cla	+ – ed to the e revoked ssification ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code Country code	ecked, no access	s will be given to th by direct action on 1 BE PL	e selected tables. No he data source.	te: Once + +	

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.

Filtering wi	ithin a rule for differ	ent data classific	ations								
escription											
et rule fo	or										
*	Jarketing										
group N	viai keung			· +	_						
isset* Ci	ustomer Data			~ +	-						
Grant	access to all data t	ables linked to t	hese asset column	IS.							
Grant By che	ecking this box, acce	ables linked to t	hese asset column o tables in the data	s. base that are linked to	the sel	ected assets. If this box is uncher	cked, no acce	ss will be given to	the selected tables. N	ote: Once	e the
Grant By che rule gr	access to all data t ecking this box, acce ranting access is sav	ables linked to t ss will be given t red and synchror	hese asset column o tables in the data nized, access to the	is. base that are linked to se tables cannot be rev	the sel oked tł	ected assets. If this box is unche nrough Collibra Protect. It can on	cked, no acce ly be revoked	ss will be given to by direct action o	the selected tables. No	ote: Once	e the
Grant By che rule gr vith (1)	ecking this box, accerranting access is sav	ables linked to t ress will be given t red and synchror option	hese asset column o tables in the data nized, access to the for Data Cat	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation	ected assets. If this box is unchen nrough Collibra Protect. It can on Select a data category	cked, no acce ly be revoked	ss will be given to by direct action o	the selected tables. No	ote: Once	the
Grant By che rule gr vith (1)	ecking this box, accerranting access is sav	ables linked to t iss will be given t red and synchron option	hese asset column o tables in the data nized, access to the for Data Cat Country	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has	ected assets. If this box is unchen nrough Collibra Protect. It can on Select a data category Country code	cked, no acce ly be revoked ~	ss will be given to by direct action o BE	the selected tables. No on the data source.	ote: Once +	e the
Grant By che rule gr with Show and Hide	access to all data t ecking this box, acce ranting access is sav Select a masking v ~	ables linked to t ass will be given t red and synchron option v rows where rows where	hese asset column o tables in the data nized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific V	the sel oked th ation has has	ected assets. If this box is unchen rough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	e the
Grant By che rule gr with (1) and Show and Hide	access to all data t ecking this box, acce ranting access is sav Select a masking v v	ables linked to t ass will be given t red and synchror opption v rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific V	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with (1) Show Hide	x access to all data t ecking this box, acce ranting access is sav Select a masking v v v Y	ables linked to t ass will be given t red and synchror option v rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked v	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with Show Hide Gummar Grant access or Customer	Select a masking of the second	ables linked to t ss will be given t red and synchror option rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked v	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with Show and Show Hide Summar Gummar Gummar or Customend Show ro Customend Show ro Show ro S	Access to all data t ecking this box, acce ranting access is sav Select a masking v v v v v v v v v v v v v v v v v v v	ables linked to t ss will be given t red and synchron option rows where rows where has Country code	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	

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	l classifications - 1						
escription							
Set rule for							
group * Marketing		\sim	+	-			
asset * Customer Data		\sim	+	-			
Grant access to all data tables linked to the	ese asset columns.						
 By checking this box, access will be given to rule granting access is saved and synchroniz 	tables in the database tl ed, access to these tabl	hat are li les cannc	inked to ot be re	o the se voked t	lected assets. If this box is unchecked, no acce hrough Collibra Protect. It can only be revoked	ess will be given to the selected t d by direct action on the data so	ables. Note: Once the irce.
with (1) Select a masking option	for Data Category	Data (Classifi	cation	Select a data category		
and Show \checkmark rows where \bigcirc	Country		\sim	has	Country code 🗸 🗸	BE	~ + -
Rule Name *	classifications - 2						
Description							
Set rule for							
group * Marketing		\sim	+	-			
asset * Personal Information		~	+	-			
		-					
Grant access to all data tables linked to the	ese asset columns.						
By checking this box, access will be given to rule granting access is saved and synchroniz	ables in the database the	hat are li les canno	inked to	the sel	lected assets. If this box is unchecked, no acce brough Collibra Protect. It can only be revoked	ss will be given to the selected to	ables. Note: Once the Irce.
Tare Stanting access is survey and synchroniz		co conno		. oncorti	and a substant of the terror of terr		
with (i) Select a masking option \checkmark	for Data Category	Data (Classifi	cation	Select a data category 🗸 🗸		
and Hide \checkmark rows where \bigcirc	Country		\sim	has	Country code 🗸 🗸	PL	~ + -
C							
Summary							
for Personal Information							
and Hide rows where Country has Country code: F	Ψ.						

Reference documentation

As described in the DB synchronization section, Collibra Protect periodically does an aggregation of all data protection standards and data access rules available. These standards and rules prepare a representation containing all databases, schemas, tables, and columns involved as well as their protections and accesses. The synchronization process then triggers Edge capabilities, like Collibra Protect for Snowflake, that 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.

Collibra Protect for Snowflake

Data protection standards rely on tag-based masking policies available in Snowflake. The name of the data category or data classification specified in the standard becomes a tag, which is applied to all affected columns to enforce data protection. For example, let's say a standard is created on the Personally Identifiable Information data category to restrict access for different groups with the organization.

for the group *	Everyone	~	+	-
and the group	Human Resources	\sim	+	-
and the group	Marketing	\sim	+	-
and the group	Sales	\sim	+	-
protect * Data	Category Data Classification	Personally Identifiab	ile Infor	mation
with * (1) Del	ault masking	· · · · · · · · · · · · · · · · · · ·	/	

When synchronized and active, the standard resolves to 14 masking policies, which is one for each Snowflake data type. The masking policies are created at the schema level and use the following naming convention: COLLIBRA/MASKING_POLICY/<asset ID>/<snowflake type>.

Results Da	ata Preview					
✓ Query I	0 <u>SQL</u> 84ms	18 rows				
Filter result		Сору				
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

The example below shows a masking policy created for the type STRING.

Note The data the consumers see depends on the masking option selected. Go to the Masking and Data Types page to learn more.

1	CASE			
2		WHEN	CURRENT_ROLE() = 'PUBLIC' THEN '*'	
3		WHEN	CURRENT_ROLE() = 'HR' THEN '*'	
4			CURRENT_ROLE() = 'MARKETING' THEN '*'	
6		FLSE	val	
7	END	LLOL	* 10 44	

All masking policies are then associated with the Personally Identifyable Information tab, which is created at the schema level and assigned to all columns where the protection needs to be applied. At runtime, Snowflake fetches the right masking policy based on column data type.

35 5404	TAGS:								
Results Da	Results Data Preview								
✓ Query ID	✓ <u>Query D</u> <u>92</u> , 48m 2 mm 2 mm								
		🛓 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			

Data Access Rules are translated as a combination of grant instructions, dynamic masking, and row access policies when specified in the rule. For example, a data set named Employee Data has sensitive columns categorized as Personally Identifiable Information.

යි Business Analysts Community 🕨 🗇 New Data Sets										
Employee Data Zata Set Candidate ☆☆☆☆☆ (0) 回 0 で 0 555										
Add characteristic	Remove									
💼 Summary	🗌 # t Name	is part of								
Details	1 EMPLOYEE_NAME	EMPLOYEES								
Data Elements	2 EMP_ID	EMPLOYEES								
	7 DEPT_ID	EMPLOYEES								
🚻 Sample data	10 SALARY	EMPLOYEES								

In Collibra Protect, a rule is created to grant access of that data set to Human Resources. Since the Grant Access chechbox is enabled, each database, schema, and table in that data set received a grant for the Snowflake role specified and each column that has protection received a column masking policy.

Set rule for	
group * Human Resources	· + -
asset* Employee Data	✓ + -
Grant access to all data tables linked to these asset column By checking this box, access will be given to the tables in the results.	k. atabase with columns linked to the selected assets. If this box is unchecked, no access will be given to these columns.
with (1) No masking v for Data Cat	Eeory Data Classification Personally Identifiable Information V + =

Let's look closer at one of the columns, such as EMPLOYEE_NAME. It belongs to the EMPLOYEES table within the DEMO schema within the PROTECT_QA database.

Business Analysts Community EMPLOYEE_N Column Candida	a Schemas → □ Protect QA 2 Connection > PROTECT_QA > DEMO AME te <□ 0
Add characteristic	SYS Snowflake ▶ ■PROTECT_QA ▶ \$\$DEMO ▶ ■EMPLOYEES ▶ \$EMPLOYEE_NAME
💼 Summary	Description from source system
Details	Empty value
Bo Data Profiling	
୍ୟଟି Diagram	

In Snowflake, each column has a masking policy assigned to it. The masking policies created at the schema level follow the naming convention: COLLIBRA/MASKING_POLICY/<asset ID>.

Results Da	ta Preview									
✓ Query ID	2 <u>Search 20</u> 254. 88ma - 18 rows									
		L Capy								
Row	created_on	name ↓	database_name	schema_name	kind	owner				
18	2022-09-06 03:4610.9	COLLIBRA/MASKINO_POLICY/96e240e8-a05a-41ad-a0e4-cc84c5e876e1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN				
17	2022-09-06 03:46:10.9	COLLIBRA/MASKING_POLICY)ebfv7875-230F-4d8F-8a51-ce6cf5dc2d7F	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN				
16	2022-09-06 03:46:10.9	COLLIBRA/MASKINO_POLICY/83966504-e911-42ea-9472-8ba48695894a	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN				
15	2022-09-06 03:46:10.9	COLLIBRA(MASKING_POLICY)49327b9e-ddc1-4884-b3e4-21988d219cce	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN				
54	2022-09-06 03-46-09.9	COLUBRA/MA5KING_POLICY/284228cc-0a00-4623-0912-98531253881/W/RANT	PROTECT_GA	DEMO	MASKING_POLICY	ACCOUNTADMIN				

The content of the masking policy created for the column EMPLOYEE_NAME is shown below.

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 '*'	
б		ELSE	val	
7	END			

The Human Resources group has access to the plain data without any masking while the other groups have masked access as created in the data protection standard.

Important In this example, the column EMPLOYEE_NAME has the policy tag and a column masking policy assigned to it. In Snowflake, when both are present, the column masking policy takes precedence and the policy tag is not executed. To mitigate this behavior and ensure that the protection defined in the standard is applied, we prepare the column masking policy with the conditions defined in the policy tag.

Masking and data types

Snowflake provides several functions to transform the data. In Collibra Protect, we support four masking options.

 Default Masking is not supported by Snowflake. This implementation was added in our Protect capability, so protection can be applied to a wide range of data types. Each column received a default value according to the column data type. Below is a list of Snowflake data types and their default values.

	Column Data Type	Snowflake Data Type	Default Masking Value
1	NUMBER	NUMBER	0
2	DECIMAL	NUMBER	0
3	NUMERIC	NUMBER	0
4	INT	NUMBER	0
5	INTEGER	NUMBER	0
6	BIGINT	NUMBER	0
7	SMALLINT	NUMBER	0
8	TINYINT	NUMBER	0
9	BYTEINT	FLOAT	0
10	FLOAT	FLOAT	0
11	FLOAT4	FLOAT	0
12	FLOAT8	FLOAT	0

	Column Data Type	Snowflake Data Type	Default Masking Value
13	DOUBLE	FLOAT	0
14	DOUBLE PRECISION	FLOAT	0
15	REAL	FLOAT	0
16	VARCHAR	VARCHAR	*
17	CHAR	VARCHAR	*
18	CHARACTER	VARCHAR	*
19	STRING	VARCHAR	*
20	TEXT	VARCHAR	*
21	BINARY	BINARY	00
22	VARBINARY	BINARY	00
23	BOOLEAN	BOOLEAN	false
24	DATE	DATE	1970-01-01
25	DATETIME	TIMESTAMP_	1970-01-01
		NIZ	00:00:00.000
26	TIME	TIME	00:00:00
27	TIMESTAMP	TIMESTAMP_ NTZ	1970-01-01
			00:00:00.000

	Column Data Type	Snowflake Data Type	Default Masking Value
28	TIMESTAMP_	TIMESTAMP_	1969-12-31
	LTZ	LTZ	16:00:00.000-0800
			Might change based on user TZ
29	TIMESTAMP_	TIMESTAMP_	1970-01-01
	NTZ	NTZ	00:00:00.000
30	TIMESTAMP_	TIMESTAMP_	1969-12-31
	TZ	TZ	16:00:00.000-0800
			Might change based on user TZ
31	VARIANT	VARIANT	0
32	OBJECT	OBJECT	8
33	ARRAY	ARRAY	0
34	GEOGRAPHY	GEOGRAPHY	{"coordinates": [0,0],"type": "Point"} (aka point(0, 0) and visualization can change based on user preferences)

In Collibra Protect, we also support the hashing and show last masking options. These can only be applied to Snowflake data types STRING, NUMBER, and FLOAT.

- 2. Hashing allows us to use Snowflake's SHA2 value function for strings, and the HASH value for numbers
- 3. Show Last allows us to use the substr(to_varchar(value), length(value) n, n) expression for strings, and mod(value, power(10,n)) for numbers. Value is the content and n is the number of characters to be shown.
- 4. No Masking is when the raw content is returned.

Note Whenever a masking option cannot be applied, like hashing on the DATE type, default masking is applied, so protection is guaranteed.

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 \rightarrow (Edge) Sites \rightarrow Your site \rightarrow Capability \rightarrow Add capability \rightarrow 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.

Ade	Database Can	didate ⊂ 0 ℃ 0			
1	Overview Tags Comments	Location Empty value			
°	Diagram Pictures	has Schema	Domain	Description	I
АА 90	Responsibilities References	PRESCRIPTIVE_PATH_SCHEMA	Snowflake > PLM_QA > PRESC Snowflake	Description	Ŷ
© &	History Files	is grouped by Technology As	set	Description	
	Configuration	Snowflake	New Applications		÷

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.

$\tfrac{200}{3007}$	 Browse 	Q	Search										+	₩	Tasks 🧵	Ç1	?	•	
¢ s	ettings General		Operating model	Roles and permis	sions V	Vorkflows	Users ar	nd groups	Services Configuration	on	Migration	Logs	Edge						
		<																_	
																	Add	0	
•	Global roles		Name †		Descriptio	n		Required lic	ense	Men	nbers								
曲	Resource roles		Catalog Author					Standard		1 A	dmin Istrator								
	Global Parmissions		Data Dictionary					Read-only		A 8 E	veryone								
~8	Global Permissions		DataSteward		Allows usa;	ge of Data Stev	ward	Read-only		A E	veryone								
â	Resource Permission		DataSteward Auth	nor				Standard											
			Edge integration e	engineer	Allows mar	naging connect	tions	Standard											
			Edge manager		Allows crea	ating and delet	ing E	Standard										Ŷ	
			Edge site		Allows con	nection from E	dge	Standard		1 E	dge privacy-ris	k-qa-25-07							
			Edge site administ	trator	Allows dow	vnloading Edge	e site	Standard										Ť	
			Glossary		Allows usa	ge of Business	Glo	Read-only											
			Helpdesk					Read-only		æ E	veryone								
			Insights					Standard		A E	veryone								
			Policy Manager					Read-only		8 E	veryone								
			Protect Admin		In this role	, you have the	sam	Standard		1 A	dmin Istrator								
			Protect Author		In this role	, you can creat	e rul	Standard		1 A	dmin Istrator	👤 Autho	or User						
			Protect Manager		This is a ro	le for our syste	em u	Read-only		1 B	dge privacy-ris	k-qa-25-07	1 Polic	y Lifecycl	e Managemer	t API Usei	r		
			Protect Reader		In this role	, you can view	Colli	Read-only		1 R	leader User								
			ReferenceData		Allows usa	ge of Referenc	e Da	Read-only		R E	veryone								
			Sysadmin		Allows for	configuring an	d m	Standard		1 A	dmin 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 per- mission, users cannot see 'Protect' as an application in the III menu. They also cannot navigate to protect related URLs or access protect endpoints.
Protect Author	Users in this role can create rules and stand- ards, view imported policies and groups, and generate audits 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 'pro- tect', 'protect_edit', and an extra 'protect_ administration' permission. This role is not assigned to anyone automatically.

Roles	Description
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. 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.

A Databases Share	Marketplace W	Varehouses Workshee	ts History Account	Partner Connect Help Notifications Snowsight ACCOUNTADMIN
Account				Last refreshed 9:39:49 AM
Usage Billing U	sers Roles	Policies Sessions	s Resource Monitors Reader Accounts	
🕂 Create 🗹 Edit 📿	Drop			
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.	
	10/22/2021, 1:30:58	ACCOUNTADMIN	Di M OL UD David Onto Data	
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.

Group	s									
Adding Gro To add a gr	oups roup, you have to use t	he <mark>Collibra Protect Gro</mark>	up API. Currently, or	nly Snowflake data sou	urces are supported.					
Group Nam	ne	System	Reference			Created	Ву		Created Date	
*	Databases Shares	X III Marketplace Warehou	ses (Worksheets)	Q History Account			Partner Connect	P A	Snowsight	ACCOUNTADMIN
Reset		HUMAN RESOURCES	SALES		✓ Roles	New Worksheet	Standard	introspection	BILLING	+ • •
► Run	All Queries Saved	10 seconds ago					<u>1</u> AC	COUNTADMIN 🏭	• DEMO_WH (M) 🛢 PLM	_QA 👫 TPCH_SF1 🔹 🚥
Results D Query.1 Filter result	Data Preview I <u>D SQL</u> 90ms — It	37 rows	v							+ Open Histor
Results C Query I Filter result	Data Preview ID SQL 90ms = It	37 rows	y ie dofault	is surrant	is inherited	assigned to users	granted to roles	granted roles	ownar	← Open Histor Columns ▼ _v
Results C Query J Filter resul Row	Data Preview JD SQL 90ms itt v created_on 1 2019-09-17 16:47.2	37 rows	y is_default N	is_current Y	is_inherited	assigned_to_users	granted_to_roles	granted_roles 3	owner	Open Histor Columns J comment Account administrat
Results C Query J Filter resul Row 1 2	Data Preview JD SQL 90ms itt created_on 1 2019-09-17 16:47:2 2022-06-27 01:10:4	37 rows 2 Cop name ACCOUNTADMIN ANTONIO	y is_default N	is_current Y	is_inherited N N	assigned_to_users 35 1	granted_to_roles 0 1	granted_roles 3 0	owner SBI_TEMPLATE_SN	Open Histor Columns Columns Comment Account administrat
Results C Query I Filter result Row 1 2 3	Data Preview ID SQL 90ms itt created_on 2 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07:	37 rows 2 Cop name ACCOUNTADMIN ANTONIO BILLING	y is_default N N	Is_current Y N	Is_Inherited N N	assigned_to_users 35 1	granted_to_roles 0 1 0	granted_roles 3 0	owner SBI_TEMPLATE_SN ACCOUNTADMIN	← Open Histor Columns ← √ comment Account administrat
Results C Cuery J Filter result Row 1 2 3 4	Data Preview ID SQL 90ms It created_on 2 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07: 4 2020-04-15 05:12:2	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION	y is,default N N N	Is_current Y N N	Is_Inherited N N N	assigned_to_users 35 1 1 1	granted_to_roles 0 1 0 1	granted_roles 3 0 0 0	owner SBI_TEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN	+ Open Histor Columns + comment Account administrat
Results C Query.I Filter result Row 1 2 3 4 5	Data Preview ID SQL 90ms It created_on 2 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07: 4 2020-04-15 05:12:2 5 2022-06-02 07:05:	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE	y Is,defautt N N N N	is_current Y N N N	Is_Inherited N N N Y	assigned_to_users 35 1 1 1 1	granted_to_roles 0 1 0 1 0	granted_roles 3 0 0 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN	+ Open Histor Columns * 2 comment Account administrat
Results C Query J Filter result Row 1 2 3 4 5 6	Data Preview JD SQL 90ms Itta 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07: 4 2020-04-15 05:12:2 5 2022-06-02 07:07: 4 2020-06-02 07:07: 5 2022-06-02 07:05:	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE	y Is_defautt N N N N N	is_current Y N N N N	is_inherited N N Y N Y	assigned_to_users 35 1 1 1 1 1 1	granted_to_roles 0 1 0 1 0 2	granted_roles 3 0 0 0 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN	+ Open Histor Columns - 2 comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7	SQL 90ms LD SQL 90ms ILL 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07: 4 2020-06-15 05:16:2 5 2022-06-02 07:05: 6 2020-06-02 07:05: 7 2020-06-27 01:12:4	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE Direct Marketing	y Is,defautt N N N N N N	is_current Y N N N N N N	is_inherited N N Y N Y N Y	assigned_to_users 35 1 1 1 1 1 1 1 1 1	granted_to_roles 0 1 0 1 0 2 0	granted_roles 3 0 0 0 0 0 1	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN	+ Open Histor Columns * 2 comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8	SQL 90ms LD SQL 90ms ILL 2019-09-17 16:47:2 2 2022-06-27 01:10:4 3 2022-06-02 07:07: 4 2022-06-02 07:05: 5 2022-06-02 07:05: 6 2022-06-02 07:05: 7 2022-06-02 07:05: 8 2022-06-02 07:05: 9 2022-06-27 01:12:4 9 2022-01-27 13:27:5	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE Direct Marketing FIVETRAN_ROLE	y Is,defautt N N N N N N	is_current Y N N N N N N N	is_inherited N N Y N Y N Y	assigned_to_users 35 1 1 1 1 1 1 1 1 1 3	granted_to_roles 0 1 0 1 0 2 0 1 1	granted_roles 3 0 0 0 0 0 1 1	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SEUCRITYADMIN	+ Open Histor Columns * 2 comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8 9 9	SQL 90ms LD SQL 90ms KL - - 2 2019-09-17 16:47:2 - 2 2022-06-27 01:10:4 - 3 2022-06-02 07:07: - 4 2020-06-15 05:12:2 - 5 2020-06-02 07:05: - 6 2020-06-02 07:05: - 7 2020-06-27 01:12:4 - 3 2022-01-27 13:27:5 - 2 2020-10:9-27 05:361 - 2 2020-10:9-27 05:361 -	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE Direct Marketing FIVETRAN_ROLE GLOBAL_PS HP	y Is,defautt N N N N N N N N	is_current Y N N N N N N N N N	is_inherited N N Y N Y N Y N Y	assigned_to_users 35 1 1 1 1 1 1 1 1 3 1 1 2 1 0	granted_to_roles 0 1 0 1 0 2 0 1 0 1 0 1 0 1 0 1 0 1 0 1	granted_roles 3 0 0 0 0 0 1 1 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN ACCOUNTADMIN ACCOUNTADMIN	+ Open Histor Columns * 2 comment Account administrat
Results C Pitter result Row 1 2 3 4 5 6 7 8 9 10	Data Preview ID SQL 90ms 90ms ILL 2 9019-09-17 16:47:2 I 2019-09-17 16:47:2 9022-06-02 07:07 I 2022-06-02 07:07 1 2022-06-02 07:05 I 2022-06-02 07:05 1 2022-06-02 07:05 I 2022-10-92 13:24 1 1 1 1 I 2021-10-92 04:38.4 1 2 1 1 1 1 1 2 100:07 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 </td <td>37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE Direct Marketing FIVETRAN_ROLE GLOBAL_PS HR LAW</td> <td>y Is,defautt N N N N N N N N N</td> <td>Is_current Y N N N N N N N N N N N</td> <td>Is_Inherited N N N N N Y N Y N Y N Y N N N N N N N</td> <td>assigned_to_users 35 1 1 1 1 1 1 1 3 1 1 0 0</td> <td>granted_to_roles 0 1 0 1 0 2 0 1 1 0 1 0 1 0</td> <td>granted_roles 3 0 0 0 0 0 1 1 0 0 0 0</td> <td>owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN ACCOUNTADMIN ACCOUNTADMIN</td> <td>+ Open Histor Columns - comment Account administrat</td>	37 rows Cop name ACCOUNTADMIN ANTONIO BILLING CERTIFICATION CUSTOMER_SERVICE DATALIFT_ROLE Direct Marketing FIVETRAN_ROLE GLOBAL_PS HR LAW	y Is,defautt N N N N N N N N N	Is_current Y N N N N N N N N N N N	Is_Inherited N N N N N Y N Y N Y N Y N N N N N N N	assigned_to_users 35 1 1 1 1 1 1 1 3 1 1 0 0	granted_to_roles 0 1 0 1 0 2 0 1 1 0 1 0 1 0	granted_roles 3 0 0 0 0 0 1 1 0 0 0 0	owner SBLTEMPLATE_SN ACCOUNTADMIN ACCOUNTADMIN ACCOUNTADMIN SBLTEMPLATE_SN SECURITYADMIN ACCOUNTADMIN ACCOUNTADMIN	+ Open Histor Columns - comment Account administrat

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 \rightarrow Services Configuration \rightarrow 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 Protectallows 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.

Ingestion to DGC
Image: control of the service in th

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.

Standards	Data protection standards create a layer of protection for similar types of data by masking them wherever they are.		
	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 tar- gets all of these columns by choosing the PII data category and masking it.		
Rules	After establishing this primary layer (blanket) of protection to your most sensitive data, use data access rules to man- age access and enhance protection for specific usages.		
	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.		

FAQs

- 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.
- 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

Audit Groups

Tab	Description
Data Protection Standards	Define default data source access to data types based on data categories, data attributes, or classes/classifications through data protection standards
	Note Data access rules for particular groups can override created standards.
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 Col- libra Protect Data Source Policies API.
Groups	Add groups through custom code via the Data Access API link and view existing current data access groups.
	Note You must add at least one group before you can create a standard or a rule.
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.

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

Page Section	Description
Standards summary	Under the heading, there is a summary about data protection standards. Click the Create a Data Protection Standard button to create a standard and get star- ted 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 Col- libra Protect and in the data source.

Synchronization Status	Description		
Pending	This standard has been created or edited, and is pending synchronization.		
Failed	The synchronization of this standard has failed. Click the 1 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.	
HR PII Standard	
Description Mask personal information for HR with hashing	
for the group * Human Resources	
with * (1) Hashing	
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 Clas- sification	A data category or data classification to apply the protection on.
Masking	Masking option for the standard.
	Note Click ^① to learn more about the masking options for standards.

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

- 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 particular groups will override these defaults.	access to types of data based on	n data categories or data classifications. Data Access Rules for
Standard Name*		
Tool tip standard		
Description		
for the group * Human Resources	~ +	-
and the group Marketing	~ +	-
protect* Data Category Data Classification	GDPR data related to criminal	al convictions and offences V
with * (1) Default masking	~	
Summary For the Group Human Resources and Marketing protect GDPR data related to criminal convictions and with Default masking	l offences	
		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 $\hat{\bullet}$ 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.

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

Page Section	Description
Rules summary	Under the heading, there is a summary about data access rules. Click the Create a Data Access Rule button to create a standard.
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 Pro- tect 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 ① 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 \lor + -
asset * Geographic Information \lor + -
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 ① Default masking \vee for Data Category Data Classification Genetic data \vee + -
and Select an action \checkmark rows where Unauthorized \checkmark has Select a code set \checkmark Select a code value \checkmark
Summary
Grant access to Marketing
for Geographic Information with Default masking for Genetic data
O 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 pro- tecting. Protect enables you to protect the fol- lowing asset types: Business process, data set, and data cat- egory. Learn more in technical background and prescriptive paths.

Field	Description
Masking (optional) • Data Category / Data Classification	Masking option for the rule. Click the To learn more about masking options. • Select a data category or a data classification to apply masking to.

Field	Description
Action (optional)	Filter the data by
Data Classification	selecting hide or show.
 Code Set 	 Select data
• Code Value	classification that is either hidden or shown
	 Code set to set up row filtering in the tables. A code set must be selected to filter by a code value.
	 Code value of the code set selected.

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_sdfxgxcfhcjhvjbvkjbk,jbjhgxdfzs	Masked	Genetic data	0	
C_NAME	Masked	Genetic data	0	
DS_TBL0001_COL0001	Masked	Genetic data	0	
				Cancel Save Ru

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 *I* 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 \vee + -
asset * Customer Data v + -
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 (1) Hashing \vee for Data Category Data Classification Personal Information \vee + -
and Select an action \checkmark rows where Unauthorized \checkmark has Select a code set \checkmark Select a code value \checkmark
Summary Grant access to Marketing for Customer Data with Hashing for Personal Information
O 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 \mathbf{i} icon in the appropriate row
 - » The Delete data access rule dialog box appears.
- 2. Click the red **Delete** button.



Data source policies

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

Protect					
Data Protection Standards	Data Access Rules	Data Source Policies	Groups	Audit	
Data Source Po	licies 🚥				

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 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.

Column name		Description	
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.	
			+ 🕁 Tasks 🗷 🗘 🕐 👥 🏭
Data Source Policies This is a list of policies that are currently active in the source data tables. Data Protection Policy Mans 1 PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3823236b-bb2746/d4-3046-12426b089dL. PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3223b47a 0fda-4309-a00-4212ceb089dL. PROTECT_QA_MASSING_COLLIBRAAMASSING_POLICY/3	Policy Logic create or replace masking policy 'COLLIBMA/MARTINE_POLICY/ create or replace masking policy 'COLLIBMA/MARTINE_POLICY/	20032360-0017-000-42120000904/JNUTY as (VAL NUMBER(8,0,0)) 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMBER(8,0,0)) 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY(8)8608 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA. 230307a-0708-0170-3000-42120000994/JNUTY as (VAL NUMAY) returns DA.	Tags "PROTECT_QA.MASKING.Personally identifiable information" "PROTECT_QA.MASKING.Personally identifiable information"

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 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.

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

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

Protect				
Data Protection Standards Data Access Rule	s Data Source Policies Groups	Audit		
Groups				
Adding Groups To add a group, you have to use the Collibra P	rotect Group API. Currently, only Snowflake	data sources are supported.		
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 Protect group
System Reference	
Created By	User who created the Protect group

Column name	Description
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

The Audit page allows you to generate an audit log of access records from the data source .



Generate an audit log

Why would I need to generate an audit log?

Note The actions you take in Collibra Protect only appear in an audit log after one hour.

Steps

1. In Collibra Protect, go to the Audit tab.

Click one of the predefined time buttons (Today, Yesterday, A week ago, or 30 days ago) or use the date picker to specify a start date for the audit log.

- 2. Click the green Generate Log button.
 - » The audit log displays the first 1,000 records after the selected start time.

Note Important Generating an audit log can take some time. Do not navigate away from the page or your request is canceled. For full details, contact your data source administrator.

Audit 🖘	D days ago			
09/29/2022				
Generate Log				
 For audit log generation, data sources may have laten 	cy to summarize access records. Logs generated here for today	r 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-ead6-0001-000306f69dd2	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
01a74801-0501-ead6-0001-000306f69dda	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES
01a74801-0501-ec9a-0001-000306f6b1b6	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM
01a74801-0501-ec9a-0001-000306f6b1ba	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES
01a74801-0501-ead6-0001-000306f69de2	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM
01a74801-0501-ec9a-0001-000306f6b1be	Sep 29, 2022, 2:01 AM	CERTIFICATION	DQ.PUBLIC.EMPLOYEES	DQ.PUBLIC.EMPLOYEES
01a74801-0501-ec9a-0001-000306f6b1c2	Sep 29, 2022, 2:01 AM	CERTIFICATION	COLLIBRA.TPCH_SF001.LINEITEM	COLLIBRA.TPCH_SF001.LINEITEM
01974901.0501.er0s.0001.000206f6h1r6	Can 20 2022 2-01 AM	CEDTIEICATION	COLLIBDA TOCU CEDOL LINEITEM	COLLIBDA TOCH COOL LINEITEM
4 1-50 51-100 101-150 701-712 ▶				

The audit log table columns include:

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

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

Note In this 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.

Masking within a rule				
Description				
Set rule for				
group* Marketing	~	+	-	
asset * Customer Data	~	+	-	
and the asset Audit & Internal Controls	\sim	+	-	
 Crant access to all data tables linked to these access column 				
By checking this box, access will be given to tables in the data	s. Ibase that are li	inked to	o the se	elected 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 the	se tables canno	ot be re	voked 1	through Collibra Protect. It can only be revoked by direct action on the data source.
with (i) Hashing v for Data Cat	egory Data (Classifi	cation	Personal Information V + -
with (1) Show last V 2 for Data Cat	egory Data (Classifi	cation	Personal and family details \vee + -
and Select an action V rows where Select a data class	ification	\sim	has	Select a code set V Select a code value V
Summary				
Summary Grant access to Marketing for Customer Data and Audit & Internal Controls				

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	e*							
Masking	between rules - 1							
Descriptior	n							
Set rule 1	for							
group *	Marketing	~	/	+	-			
asset *	Customer Data	~	/	+	-			
Gran By c rule	nt access to all data tables linked to the checking this box, access will be given to b granting access is saved and synchroniz	ese asset columns. tables in the database that ed, access to these tables c	are link annot l	ked to be rev	the se voked ti	lected assets. If this box is unchecked, no ac hrough Collibra Protect. It can only be revok	cess ed b	s will be given to the selected tables. Note: Once the yy direct action on the data source.
with (i	Hashing 🗸 🗸	for Data Category D	Data Cla	assific	ation	Personal Information	/	+ -
and set	lect an action	alact a data classification		5.4	hac	Select a code set		Select a code value
and Ser				v	Tids	Select a code set		Select a code value
lule Name	e*							
Masking	; between rules - 2							
Descriptior	n							
Set rule	for							
group *	Marketing	~	·	+	-			
asset *	Audit & Internal Controls	~	/	+	-			
🔽 Grai	int access to all data tables linked to the	ese asset columns.						
By c rule	checking this box, access will be given to e granting access is saved and synchroniz	tables in the database that ed, access to these tables o	are link annot l	ked to be rev	the se voked ti	lected assets. If this box is unchecked, no ac hrough Collibra Protect. It can only be revok	cess ed b	s will be given to the selected tables. Note: Once the by direct action on the data source.
with (i	Show last V	for Data Category D	Data Cla	assific	ation	Personal and family details	~	+ -
and Sel	lect an action v rows where	elect a data classification		\sim	has	Select a code set 🔍		Select a code value
Summa Grant acco	ary ess to Marketing							
for Audit 8 with Show	& Internal Controls w last 2 characters for Personal and famil	y 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.

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

Standard Name *		
Masking between standards - 1		
Description		
for the group * Marketing	~ + -	
protect* Data Category Data Classification	Personal Information	~
with * (i) Hashing	\checkmark	
Summary		
For the Group Marketing		
protect Personal Information with Hashing		

Masking between standards - 2		
Description		
Securitori		
for the group * Human Resources	~ + -	
protect [*] Data Category Data Classification	Name	\sim
with * (i) Show last	2	
Summary		
⁻ or the Group Human Resources		

Conflicting filters affecting 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.

iltering within a rul	e for the same	e data classific	ation								
escription											
t rule for											
oup * Marketing				~	+ -						
	D-t-				1						
set * Customer [Data			~	+ -						
set * Customer I	Data o all data table	es linked to th	nese asset column	s.	+ -						
 Grant access to 	Data o all data table s box, access v	es linked to th vill be given to	nese asset column	s. base that are link	+ –	elected assets. If this box is unche	cked, no acces	s will be given to th	e selected tables. No	te: Once	the
 Grant access to By checking this rule granting accession 	Data o all data table s box, access v ccess is saved a	es linked to th vill be given to and synchron	n ese asset column b tables in the datal ized, access to thes	s. base that are link se tables cannot b	+ – ed to the s	elected assets. If this box is unche through Collibra Protect. It can or	ecked, no acces	s will be given to th by direct action on t	e selected tables. No :he data source.	te: Once	the
 Grant access to By checking this rule granting ac th (1) Select a 	Data o all data table s box, access v ccess is saved a masking optic	es linked to th vill be given to and synchron	hese asset column b tables in the datal ized, access to thes	s. base that are link te tables cannot b	ed to the servoked	elected assets. If this box is unche through Collibra Protect. It can on Select a data category	cked, no acces	s will be given to th by direct action on t	e selected tables. No he data source.	te: Once	the
set * Customer I Grant access to By checking this rule granting ac th (1) Select a	Data o all data table s box, access v ccess is saved a a masking optic	es linked to th will be given to and synchron	nese asset column o tables in the datai ized, access to thes for Data Cate	s. base that are link se tables cannot b egory Data Cla	+ –	elected assets. If this box is unche through Collibra Protect. It can on Select a data category	ecked, no acces aly be revoked	s will be given to th by direct action on 1	e selected tables. No he data source.	te: Once	the
set * Customer I Grant access to By checking this rule granting ac th (1) Select a d Show	Data o all data table s box, access v ccess is saved a a masking optio	es linked to th vill be given to and synchron on	bese asset column o tables in the datal ized, access to thes for Data Cato Country	s. base that are link se tables cannot b egory Data Cla	+ – ed to the e revoked ssification	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces ly be revoked	s will be given to th by direct action on 1 BE	e selected tables. No che data source.	te: Once +	the
set * Customer I G Grant access to By checking this rule granting ac th ① Select a id Show d Hide	Data o all data table s box, access w ccess is saved a a masking option rc	es linked to the vill be given to and synchron on v ows where	hese asset column tables in the datal ized, access to thes for Data Cate Country	s. base that are link ie tables cannot the egory Data Cla	+ – ed to the e e revoked ssification ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	icked, no acces nly be revoked	s will be given to th by direct action on I BE PI	e selected tables. No the data source.	te: Once + +	
Set * Customer I By checking this rule granting ac th (1) Select a and Show ad Hide	Data Data a all data table s box, access v ccess is saved a a masking optic rc rc rc	es linked to th vill be given to and synchron on v ows where [bese asset column tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link te tables cannot t egory Data Cla	+ – ed to the e revoked ssification w ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces	s will be given to th by direct action on I BE PL	e selected tables. No the data source.	te: Once + +	
set * Customer I Grant access to By checking this rule granting ac th ① Select a ind Show ind Hide Jummary	Data Data a all data table s box, access v ccess is saved a a masking optic v rc	es linked to th vill be given to and synchron on v ows where ows where	hese asset column o tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link base that are link to base cannot t egory Data Cla	+ – ed to the e e revoked ssification v ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code	ecked, no acces	s will be given to th by direct action on 1 BE PL	e selected tables. No he data source.	+ +	
sset * Customer I Grant access to By checking this rule granting ac ith ① Select a nd Show nd Hide JIMMARY ant access to Mark	Data Data table s box, access w ccess is saved a masking optic rc rc rc eting	es linked to th will be given to and synchron on v bows where bows where	hese asset column o tables in the datal ized, access to thes for Data Cate Country Country	s. base that are link base that are link to base cannot t egory Data Cla	+ – ed to the e revoked ssification ha	elected assets. If this box is unche through Collibra Protect. It can on Select a data category Country code Country code	ecked, no access	s will be given to th by direct action on 1 BE PL	e selected tables. No he data source.	te: Once + +	

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.

Filtering wi	ithin a rule for differ	ent data classific	ations								
escription											
et rule fo	or										
*	Jarketing										
group N	viai keung			· +	_						
isset* Ci	ustomer Data			~ +	-						
Grant	access to all data t	ables linked to t	hese asset column	IS.							
Grant By che	ecking this box, acce	ables linked to t	hese asset column o tables in the data	s. base that are linked to	the sel	ected assets. If this box is uncher	cked, no acce	ss will be given to	the selected tables. N	ote: Once	e the
Grant By che rule gr	access to all data t ecking this box, acce ranting access is sav	ables linked to t ss will be given t red and synchror	hese asset column o tables in the data nized, access to the	is. base that are linked to se tables cannot be rev	the sel oked tł	ected assets. If this box is unche nrough Collibra Protect. It can on	cked, no acce ly be revoked	ss will be given to by direct action o	the selected tables. No	ote: Once	e the
Grant By che rule gr vith	ecking this box, accerranting access is sav	ables linked to t ress will be given t red and synchror option	hese asset column o tables in the data nized, access to the for Data Cat	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation	ected assets. If this box is unchen nrough Collibra Protect. It can on Select a data category	cked, no acce ly be revoked	ss will be given to by direct action o	the selected tables. No	ote: Once	the
Grant By che rule gr vith (1)	ecking this box, accerranting access is sav	ables linked to t iss will be given t red and synchron option	hese asset column o tables in the data nized, access to the for Data Cat Country	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has	ected assets. If this box is unchen nrough Collibra Protect. It can on Select a data category Country code	cked, no acce ly be revoked ~	ss will be given to by direct action o BE	the selected tables. No on the data source.	ote: Once +	e the
Grant By che rule gr with Show and Hide	access to all data t ecking this box, acce ranting access is sav Select a masking v	ables linked to t ass will be given t red and synchron option v rows where rows where	hese asset column o tables in the data nized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific V	the sel oked th ation has has	ected assets. If this box is unchen rough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	e the
Grant By che rule gr with (1) and Show and Hide	access to all data t ecking this box, acce ranting access is sav Select a masking v v	ables linked to t ass will be given t red and synchror opption v rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with (1) Show Hide	access to all data t ecking this box, acce ranting access is sav Select a masking v v	ables linked to t ass will be given t red and synchror option v rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher nrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked v	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with Show Hide Gummar Grant access or Customer	Select a masking of the second	ables linked to t ss will be given t red and synchror option rows where rows where	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked v	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	
Grant By che rule gr with Show and Show Hide Summar Gummar Gummar or Customend Show ro Customend Show ro Show ro S	Access to all data t ecking this box, acce ranting access is sav Select a masking v v v v v v v v v v v v v v v v v v v	ables linked to t ss will be given t red and synchron option rows where rows where has Country code	hese asset column o tables in the data lized, access to the for Data Cat Country State	is. base that are linked to se tables cannot be rev egory Data Classific	the sel oked th ation has has	ected assets. If this box is uncher rrough Collibra Protect. It can on Select a data category Country code Country code	cked, no acce ly be revoked	ss will be given to by direct action o BE PL	the selected tables. Non the data source.	+ +	

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	l classifications - 1						
escription							
Set rule for							
group * Marketing		\sim	+	-			
asset * Customer Data		\sim	+	-			
Grant access to all data tables linked to the	ese asset columns.						
 By checking this box, access will be given to rule granting access is saved and synchroniz 	tables in the database tl ed, access to these tabl	hat are li les cannc	inked to ot be re	o the se voked t	lected assets. If this box is unchecked, no acce hrough Collibra Protect. It can only be revoked	ess will be given to the selected t d by direct action on the data so	ables. Note: Once the irce.
with (1) Select a masking option	for Data Category	Data (Classifi	cation	Select a data category		
and Show \checkmark rows where \bigcirc	Country		\sim	has	Country code 🗸 🗸	BE	~ + -
Rule Name *	classifications - 2						
Description							
Set rule for							
group * Marketing		\sim	+	-			
asset * Personal Information		~	+	-			
		-					
Grant access to all data tables linked to the	ese asset columns.						
By checking this box, access will be given to rule granting access is saved and synchroniz	ables in the database the	hat are li les canno	inked to	the sel	lected assets. If this box is unchecked, no acce brough Collibra Protect. It can only be revoked	ss will be given to the selected to	ables. Note: Once the Irce.
Tare Stanting access is survey and synchroniz		co conno		. oncorti	and a substant of the terror of terr		
with (i) Select a masking option \checkmark	for Data Category	Data (Classifi	cation	Select a data category 🗸 🗸		
and Hide \checkmark rows where \bigcirc	Country		\sim	has	Country code 🗸 🗸	PL	~ + -
C							
Summary							
for Personal Information							
and Hide rows where Country has Country code: F	Ψ.						

Reference documentation

As described in the DB synchronization section, Collibra Protect periodically does an aggregation of all data protection standards and data access rules available. These standards and rules prepare a representation containing all databases, schemas, tables, and columns involved as well as their protections and accesses. The synchronization process then triggers Edge capabilities, like Collibra Protect for Snowflake, that 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.

Collibra Protect for Snowflake

Data protection standards rely on tag-based masking policies available in Snowflake. The name of the data category or data classification specified in the standard becomes a tag, which is applied to all affected columns to enforce data protection. For example, let's say a standard is created on the Personally Identifiable Information data category to restrict access for different groups with the organization.

for the group *	Everyone	~	+	-
and the group	Human Resources	\sim	+	-
and the group	Marketing	\sim	+	-
and the group	Sales	\sim	+	-
protect * Data	Category Data Classification	Personally Identifiabl	e Infor	mation
with * (1) Del	fault masking	\sim		

When synchronized and active, the standard resolves to 14 masking policies, which is one for each Snowflake data type. The masking policies are created at the schema level and use the following naming convention: COLLIBRA/MASKING_POLICY/<asset ID>/<snowflake type>.

Results Da	ata Preview					
✓ Query I	0 <u>SQL</u> 84ms	18 rows				
Filter result		Сору				
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

The example below shows a masking policy created for the type STRING.

Note The data the consumers see depends on the masking option selected. Go to the Masking and Data Types page to learn more.

1	CASE			
2		WHEN	CURRENT_ROLE() = 'PUBLIC' THEN '*'	
3		WHEN	CURRENT_ROLE() = 'HR' THEN '*'	
4			CURRENT_ROLE() = 'MARKETING' THEN '*'	
6		FLSE	val	
7	END	LLOL	* 10 44	

All masking policies are then associated with the Personally Identifyable Information tab, which is created at the schema level and assigned to all columns where the protection needs to be applied. At runtime, Snowflake fetches the right masking policy based on column data type.

35 5404	TAGS:					
Results Da	ta Preview					
✓ Query ID	201. 48ms	2 rows				
		L 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

Data Access Rules are translated as a combination of grant instructions, dynamic masking, and row access policies when specified in the rule. For example, a data set named Employee Data has sensitive columns categorized as Personally Identifiable Information.

ا Business Analysts Community ► 🗇 New Data Sets					
Employee Data	3 ndidate ☆☆☆☆☆ (0) @ 0 日 段	0 5%			
Add characteristic	Remove				
💼 Summary	🗌 # t Name	is part of			
Details	1 EMPLOYEE_NAME	EMPLOYEES			
Data Elements	2 EMP_ID	EMPLOYEES			
	7 DEPT_ID	EMPLOYEES			
🚻 Sample data	10 SALARY	EMPLOYEES			

In Collibra Protect, a rule is created to grant access of that data set to Human Resources. Since the Grant Access chechbox is enabled, each database, schema, and table in that data set received a grant for the Snowflake role specified and each column that has protection received a column masking policy.

Set rule for	
group * Human Resources	· + -
asset* Employee Data	✓ + -
Grant access to all data tables linked to these asset column By checking this box, access will be given to the tables in the results.	k. atabase with columns linked to the selected assets. If this box is unchecked, no access will be given to these columns.
with (1) No masking v for Data Cat	Eeory Data Classification Personally Identifiable Information V + =

Let's look closer at one of the columns, such as EMPLOYEE_NAME. It belongs to the EMPLOYEES table within the DEMO schema within the PROTECT_QA database.

Business Analysts Community EMPLOYEE_N Column Candida	a Schemas → □ Protect QA 2 Connection > PROTECT_QA > DEMO AME te <□ 0
Add characteristic	SYS Snowflake ▶ ■PROTECT_QA ▶ \$\$DEMO ▶ ■EMPLOYEES ▶ \$EMPLOYEE_NAME
💼 Summary	Description from source system
Details	Empty value
Bo Data Profiling	
୍ୟଟି Diagram	

In Snowflake, each column has a masking policy assigned to it. The masking policies created at the schema level follow the naming convention: COLLIBRA/MASKING_POLICY/<asset ID>.

Results Da	ta Preview					
✓ Query ID	52. 88ms	18 rows				
		L Capy				
Row	created_on	name ↓	database_name	schema_name	kind	owner
18	2022-09-06 03:4610.9	COLLIBRA/MASKINO_POLICY/96e240e8-a05a-41ad-a0e4-cc84c5e876e1	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
17	2022-09-06 03:46:10.9	COLLIBRA/MASKING_POLICY)ebfv7875-230F-4d8F-8a51-ce6cf5dc2d7F	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
16	2022-09-06 03:46:10.9	COLLIBRA/MASKINO_POLICY/83966504-e911-42ea-9472-8ba48695894a	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
15	2022-09-06 03:46:10.9	COLLIBRA(MASKING_POLICY)49327b9e-ddc1-4884-b3e4-21988d219cce	PROTECT_QA	DEMO	MASKING_POLICY	ACCOUNTADMIN
54	2022-09-06 03-46-09.9	COLUBRA/MA5KING_POLICY/284228cc-0a00-4623-b912-9853125b38b1/W/RANT	PROTECT_GA	DEMO	MASKING_POLICY	ACCOUNTADMIN

The content of the masking policy created for the column EMPLOYEE_NAME is shown below.

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	
<pre>3 WHEN CURRENT_ROLE() = 'PUBLIC' THEN '*' 4 WHEN CURRENT_ROLE() = 'MARKETING' THEN '*' 5 WHEN CURRENT_ROLE() = 'SALES' THEN '*' 6 ELSE val 7 END</pre>	
4 WHEN CURRENT_ROLE() = 'MARKETING' THEN '*' 5 WHEN CURRENT_ROLE() = 'SALES' THEN '*' 6 ELSE val 7 END	
5 WHEN CURRENT_ROLE() = 'SALES' THEN '*' 6 ELSE val 7 END	
6 ELSE val 7 END	
7 END	

The Human Resources group has access to the plain data without any masking while the other groups have masked access as created in the data protection standard.

Important In this example, the column EMPLOYEE_NAME has the policy tag and a column masking policy assigned to it. In Snowflake, when both are present, the column masking policy takes precedence and the policy tag is not executed. To mitigate this behavior and ensure that the protection defined in the standard is applied, we prepare the column masking policy with the conditions defined in the policy tag.

Masking and data types

Snowflake provides several functions to transform the data. In Collibra Protect, we support four masking options.

 Default Masking is not supported by Snowflake. This implementation was added in our Protect capability, so protection can be applied to a wide range of data types. Each column received a default value according to the column data type. Below is a list of Snowflake data types and their default values.

	Column Data Type	Snowflake Data Type	Default Masking Value
1	NUMBER	NUMBER	0
2	DECIMAL	NUMBER	0
3	NUMERIC	NUMBER	0
4	INT	NUMBER	0
5	INTEGER	NUMBER	0
6	BIGINT	NUMBER	0
7	SMALLINT	NUMBER	0
8	TINYINT	NUMBER	0
9	BYTEINT	FLOAT	0
10	FLOAT	FLOAT	0
11	FLOAT4	FLOAT	0
12	FLOAT8	FLOAT	0

	Column Data Type	Snowflake Data Type	Default Masking Value
13	DOUBLE	FLOAT	0
14	DOUBLE PRECISION	FLOAT	0
15	REAL	FLOAT	0
16	VARCHAR	VARCHAR	*
17	CHAR	VARCHAR	*
18	CHARACTER	VARCHAR	*
19	STRING	VARCHAR	*
20	TEXT	VARCHAR	*
21	BINARY	BINARY	00
22	VARBINARY	BINARY	00
23	BOOLEAN	BOOLEAN	false
24	DATE	DATE	1970-01-01
25	DATETIME	TIMESTAMP_	1970-01-01
		NIZ	00:00:00.000
26	TIME	TIME	00:00:00
27	TIMESTAMP	TIMESTAMP_	1970-01-01
			00:00:00.000

Chapter 12

	Column Data Type	Snowflake Data Type	Default Masking Value
28	TIMESTAMP_ LTZ	TIMESTAMP_ LTZ	1969-12-31
			16:00:00.000-0800
			Might change based on user TZ
29	TIMESTAMP_ NTZ	TIMESTAMP_ NTZ	1970-01-01
			00:00:00.000
30	TIMESTAMP_ TZ	TIMESTAMP_ TZ	1969-12-31
			16:00:00.000-0800
			Might change based on user TZ
31	VARIANT	VARIANT	0
32	OBJECT	OBJECT	8
33	ARRAY	ARRAY	0
34	GEOGRAPHY	GEOGRAPHY	{"coordinates": [0,0],"type": "Point"} (aka point(0, 0) and visualization can change based on user preferences)

In Collibra Protect, we also support the hashing and show last masking options. These can only be applied to Snowflake data types STRING, NUMBER, and FLOAT.

- 2. Hashing allows us to use Snowflake's SHA2 value function for strings, and the HASH value for numbers
- 3. Show Last allows us to use the substr(to_varchar(value), length(value) n, n) expression for strings, and mod(value, power(10,n)) for numbers. Value is the content and n is the number of characters to be shown.
- 4. No Masking is when the raw content is returned.

Note Whenever a masking option cannot be applied, like hashing on the DATE type, default masking is applied, so protection is guaranteed.