

GUIDE

---

# Quest Data Intelligence

Policy Manager Guide 16.0



## Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the Documentation), is for your informational purposes only and is subject to change or withdrawal by Quest Software, Inc and/or its affiliates at any time. This Documentation is proprietary information of Quest Software, Inc and/or its affiliates and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Quest Software, Inc and/or its affiliates

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Quest Software, Inc and/or its affiliates copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Quest Software, Inc and/or its affiliates that all copies and partial copies of the Documentation have been returned to Quest Software, Inc and/or its affiliates or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, QUEST SOFTWARE, INC. PROVIDES THIS DOCUMENTATION AS IS WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL QUEST SOFTWARE, INC. BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF QUEST SOFTWARE, INC. IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Quest Software, Inc and/or its affiliates Provided with Restricted Rights. Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © Quest Software, Inc. and/or its affiliates All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# Contact Quest

## Understanding your Support

Review [support maintenance programs and offerings](#).

## Registering for Support

Access the [Quest support](#) site and click Sign in to register for product support.

## Accessing Technical Support

For your convenience, Quest provides easy access to "One Stop" support for [Quest Data Intelligence \(Quest DI\)](#), and includes the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- Quest Support policies and guidelines
- Other helpful resources appropriate for your product

For information about other Quest products, visit [Quest Products Overview](#).

## Provide Feedback

If you have comments or questions, or feedback about Quest product documentation, you can send a message to the [documentation team](#).

## News and Events

Visit [News and Events](#) to get up-to-date news, announcements, and events. View video demos and read up on customer success stories and articles by industry experts.

## Contents

---

Policy Manager .....	6
Supported Policy Types .....	6
Supported Environments .....	7
Creating Policies .....	10
Managing Policies .....	20
Using AI Explain .....	20
Viewing Policy Details .....	22
Editing Policies .....	23
Viewing Activity Log .....	24
Enforcing Policies .....	27
Using Mind Maps .....	30
Deleting Policies .....	31

# Policy Manager

Policy Manager is an AI-powered module within Data Governance that enables business stewards and data stewards to create and enforce policies with minimal manual effort. It automates policy draft creation, business rule generation, and enforcement activities.

Policy Manager addresses following key challenges:

- **Speed:** AI-assisted policy creation reduces time from weeks to hours
- **Consistency:** Automated rule generation ensures policies are enforced uniformly
- **Accessibility:** Non-technical users can create and manage policies
- **Compliance:** Enforcement tracking provides audit trails for compliance
- **Scalability:** Apply policies across multiple databases and environments

## Supported Policy Types

- **Data Classification**  
Classifies data assets by sensitivity level such as Public, Internal, Confidential, and Restricted. For example, "Mark all customer PII as Confidential."
- **Data Masking**  
Hides sensitive data in environments. For example, "Mask credit card numbers in DEV databases."
- **Data Retention**  
Defines data lifecycle and deletion schedules. For example, "Delete transactional logs older than 90 days."
- **Manual Policies**  
Business policies from Business Glossary Manager listed for reference. Not directly enforced through Policy Manager.



## Policy Manager



Ensure that your administrator has enabled the Policy Manager permissions for you.

## Supported Environments

Policy Manager supports the following databases for policy enforcement:

- Snowflake
- Databricks

To access Policy Manager, go to **Application Menu > Data Governance > Policy Manager**.

The Policy Manager page appears, with the Policies tab open by default.

#	Catalog Path	Policy Name	Type	Source	Definition	Actions
1	GDPR Policies	Data Masking Policy - Marketing	Data Masking	AI	This policy mandates that all email addresses...	
2	Erwin_Employee	Performance Review Policies	Generic	Manual	Employee compensation and development p...	
3	Erwin_Employee	Substance Abuse Policies	Generic	Manual	Substance abuse can have adverse effects o...	
4	GDPR Policies	TDDA	Generic	Manual		
5	TechPubs	Project Plan	Generic	Manual		
6	TechPubs	Impact Analysis	Generic	Manual		
7	GDPR Policies	Documentation	Generic	Manual	Governs the erwin DIS documentation proce...	

The Policy Manager page provides a centralized workspace for data governance teams to create, organize, and maintain business policies across all catalogs.

Two tabs allow you to switch between governance objects:

Tab	Function
<a href="#">Policies</a>	Use this section to create and manage policies.

Tab	Function
<a href="#">Rules</a>	Use this section to view rules and the activity log for rules.








## Policies

The Policies tab is the active view that lists all business policies across your catalogs. Use the summary chips to quickly filter the list by policy type, search by policy name or definition, and narrow results further using the Catalog dropdown. From this tab, you can view, manage, and take actions on existing policies, and create a new policy using the **Create Policy** button.

You can also add a new catalog from Policies tab. Click [+](#) at the top of the catalog panel.

### Actions

Each policy row in the list includes an Actions column. The following functions are available for each policy:

-  - AI Explain - Generates a plain - English summary of the policy using AI, based on all policy components including its definition, rules, and metadata.
-  - View Policy - Opens the full policy details in the default display format, showing the policy name, description, definition, draft status, and associated metadata.
-  - Edit Policy - Re-opens the policy creation wizard, allowing users to modify the policy definition, associated assets, linked rules, or any other attributes.
-  - Activity Log - Displays a complete audit trail of all changes made to the policy, including updates to assets, definitions, descriptions, and linked rules.
-  - Enforce Policy - Executes the AI-generated SQL queries on the connected data source through Quest DI to enforce a policy.
-  - Mind Map - Displays all associations and relationships for a policy.
-  - Delete - Removes the policy along with all its associations and rules.

For more information, refer to the [Creating Policies](#) and [Managing Policies](#) topics.



## Rules

The Rules tab lists all business rules across your data domains. Use the available filters to search and narrow the list, and take actions on individual rules directly from the table.

#	Catalog Path	Rule Name	Definition	Description	Rule Syntax	Actions
1	Customer Rules	SNOWFLAKE Masking Policy - Data Masking P...	Apply SNOWFLAKE dynamic data ...	Auto-generated SNOWFLAKE mask...	SQL -- @@ENV_START: envName=SNOWFLAKE ...	
2	Customer Rules	Test 123	--	--	JSON --	
3	TechPubs	Agriculture rules.	Agricultural rules belong to the stu...	--	JSON Agricultural rules belong to the study of the ...	
4	Erwin_Sales	Respect time	*Make an appointment when it is c...	--	JSON *Make an appointment when it is convenien...	

## Actions

Each rule row includes the following actions:

- View Rule - Opens the full rule details in the default display format, showing the rule name, catalog path, definition, description, and syntax.
- Activity Log - Displays a complete audit trail of all changes made to the rule over time.

# Creating Policies

This topic walks you through creating a policy with AI assistance. Policies are created in the draft stage and can be refined before generating rules and enforcing them.

### Before You Start

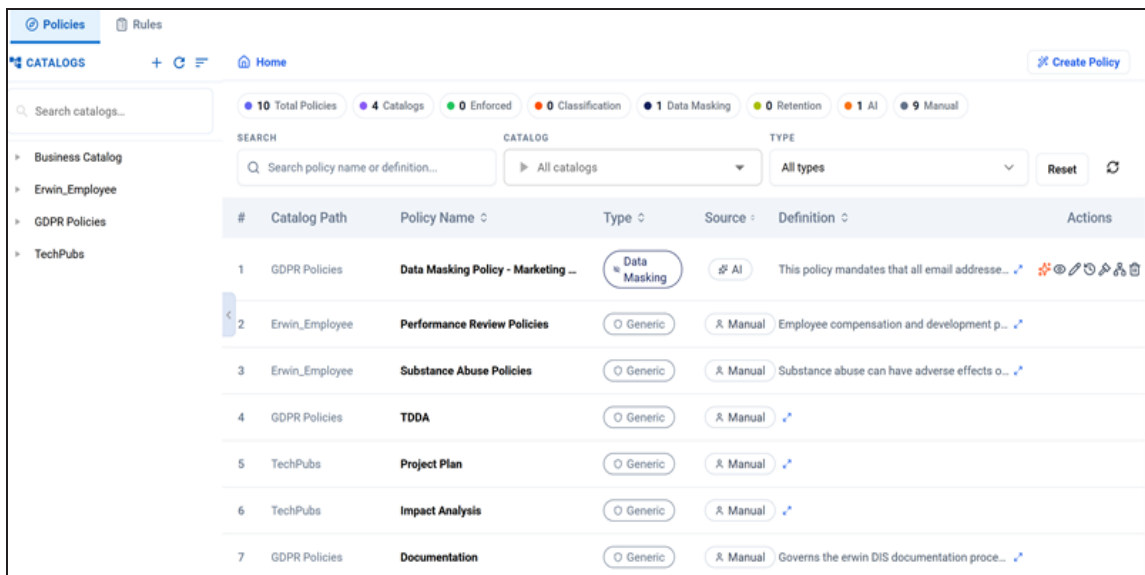
- Ensure you have the required permission to access Policy Manager.
- Understand the policy type you need (Classification, Masking, Retention)
- Have a clear intent for the policy (what data it governs, why, and how)

For example, the following steps display how to create a data masking policy and configure partial masking for email addresses by masking five characters.

To create business policies, follow these steps:

1. Go to **Application Menu > Data Governance > Policy Manager**.

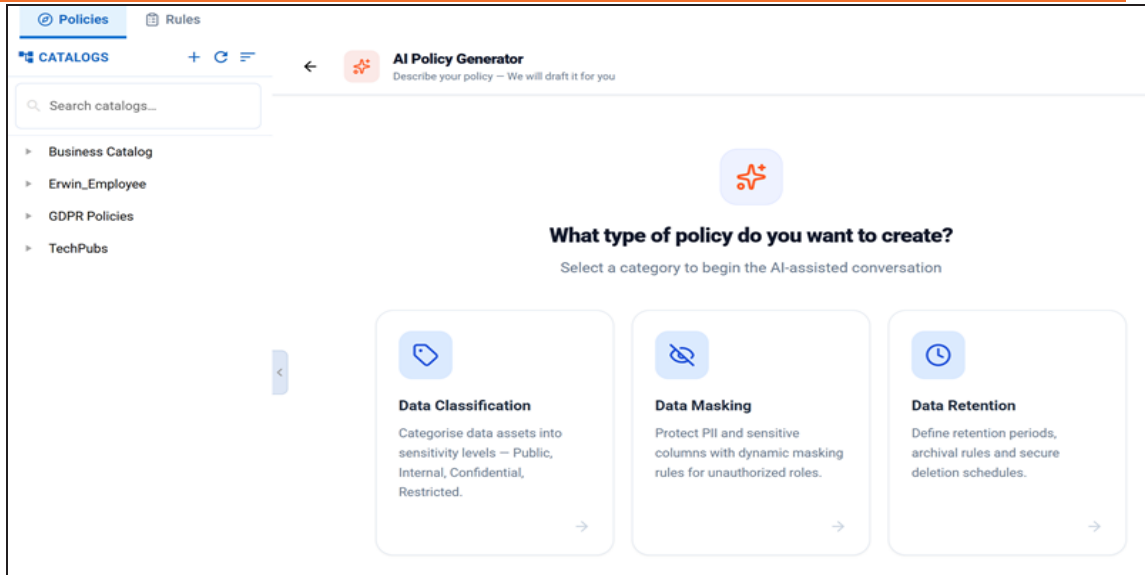
The Policy Manager page opens.



2. On the Policies tab, click **Create Policy**.

The AI Policy Generator page opens.

## Creating Policies

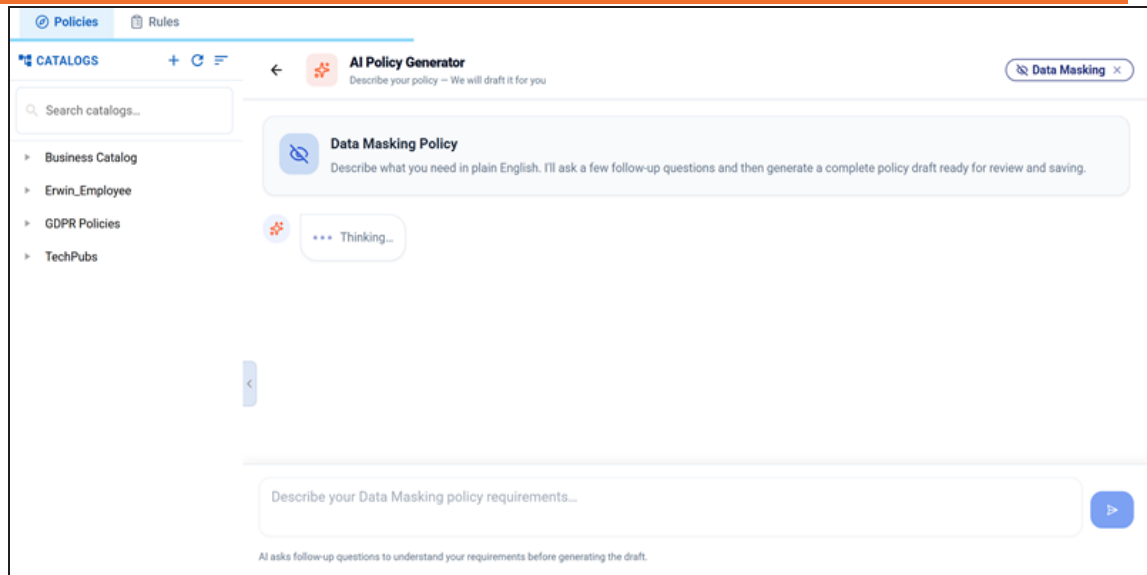


### 3. Select a policy type:

- Data Classification
- Data Masking
- Data Retention

The AI Policy Generator chat window opens.

## Creating Policies



4. Answer the clarification questions prompted by the AI Policy Generator.

For example:

- Which regulation or standard must this policy comply with?
- What is the primary data domain this policy covers?

The AI Policy Generator can ask follow-up questions based on your responses.

## Creating Policies

The screenshot shows the 'AI Policy Generator' interface. On the left, there's a 'CATALOGS' sidebar with a search bar and a list of categories: Business Catalog, Erwin\_Employee, GDPR Policies, and TechPubs. The main area is titled 'AI Policy Generator' with a subtitle 'Describe your policy - We will draft it for you'. It contains two numbered questions: '1. Which regulation or standard (e.g., GDPR, CCPA, HIPAA) does this policy need to comply with?' and '2. What is the primary data domain this policy will cover (e.g., Customer, Employee, Finance, Marketing)?'. Below these questions is a text box with the example: '(e.g. Customer Data, Employee / HR, Finance, Marketing, Product Catalog, Healthcare, Supply Chain, Legal & Compliance, Operations, IT Infrastructure)'. A chat interface on the right shows a user message: 'You - 10:43 am GDPR, Marketing' and an AI response: 'AI Generator - 10:43 am Thank you. To tailor the Data Masking policy further: 1. Which data categories within the Marketing domain should be masked or protected (e.g., email addresses, phone numbers, campaign data)? 2. What type of masking do you require—partial masking (e.g., showing only part of the data) or full masking (completely hiding the data)?'. At the bottom, there's a text input field with the text 'email, partial masking up to 5 characters' and a blue 'Next' button. A small note at the bottom states: 'AI asks follow-up questions to understand your requirements before generating the draft.'

Once all required inputs are provided, the Draft Policy Wizard opens, displaying the first section, Policy Information.

## Creating Policies

**Draft Policy Wizard**  
Step 1 of 4 · Policy Information

**POLICY DETAILS**

**POLICY NAME \***  
Data Masking Policy - Marketing Email Addresses under GDPR  
58 / 250

**CATALOG \***  
Select a catalog...  
Please select a catalog

**DESCRIPTION**  
This policy governs the partial masking of email addresses in the Marketing domain to comply with GDPR, allowing only :

**DEFINITION \***  
This policy mandates that all email addresses within the Marketing data domain are subject to partial masking, with only the first five characters visible to non-administrative users. Full access to unmasked email addresses is granted exclusively to users with administrative privileges, while all other roles will interact with masked data to protect personal information in accordance with GDPR requirements. The policy is enforced through technical controls in data

**POLICY TYPE**  
Data Masking

**Associate Assets**

5. Review or update the Policy Name.
6. In the catalog field, select the catalog where you want to save the policy.
7. Review the policy description, definition, policy type, and tags.
8. Click **Associate Assets**.

The Associate Assets section opens.

## Creating Policies

The screenshot shows the 'Draft Policy Wizard' interface, specifically Step 2 of 4: Associate Assets. The wizard is in 'DRAFT' mode. The progress bar at the top shows four steps: Policy Information (completed), Associate Assets (current step), Enforcement Rules, and Review & Save. The main content area is titled 'ASSOCIATED METADATA ASSETS (METADATA)'. Under 'TARGET PLATFORM', 'Snowflake' is selected with a checkmark, and 'Databricks' is also visible. The 'FIND METADATA ASSETS' section contains two dropdown menus: 'System' (set to 'System') and 'Environment' (set to 'Environment'). Below these is a search box labeled 'Search table / column names...' with a 'Search' button. To the right of the search box is an 'AI Suggest' button. A large light blue box with a dashed border contains the text: 'Use Search or AI Suggest to find tables & columns matching this policy'. At the bottom right, there are 'Back' and 'Enforcement Rules' navigation buttons.

9. Select the system, environment, table, and columns to associate with the policy. You can do one of the following:

- Select assets manually using drop-down lists or the search box, or
- Click **AI Suggest** to view recommended tables and columns.

You can review and accept AI-suggested tables and columns.

Selected assets appear in the Selected field at the top.



## Creating Policies

**Draft Policy Wizard**  
Step 2 of 4 · Associate Assets

**Policy Information** **Associate Assets** **Enforcement Rules** **Review & Save**

✓ **SELECTED 0 table(s) 5 column(s)**

SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC...  
SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC...

**ASSOCIATED METADATA ASSETS** **METADATA**

**TARGET PLATFORM**

**Snowflake** **Databricks**

**FIND METADATA ASSETS** **Clear**

System: Snowflake Environment: snowflake

Search table / column names... **Search** **AI Suggest**

Keywords used in AI suggestions for metadata selection: data, masking, marketing, email, addresses, under, gdpr, mandates, within, domain

**All (16)** **AI Mode (16)**

1-5 / 16 results

**SNOWFLAKE\_SAMPLE...** **Snowflake** **SNOWFLAKE SA...** **AI Mode** **Matched keyword: data**

**Select All** **C\_CUSTKEY** **C\_NAME** **C\_ADDRESS** **C\_NATIONKEY** **C\_PHONE** **C\_ACCTBAL**

**Back** **Enforcement Rules**

10. Click **Enforcement Rules**.

The Enforcement Rules section appears.

## Creating Policies

**Draft Policy Wizard**  
Step 3 of 4 · Enforcement Rules

**Policy Information** **Associate Assets** **Enforcement Rules** **Review & Save**

**SQL ENFORCEMENT RULES** **AI - SQL** **Data Masking**

**RULE CATALOG** - rules will be saved under this catalog

Select a category...

**Generate Data Masking SQL Rules with AI**

Click above to generate a SNOWFLAKE masking policy DDL script - proposed as a saveable rule

**RULES SUMMARY**

Catalog — none —

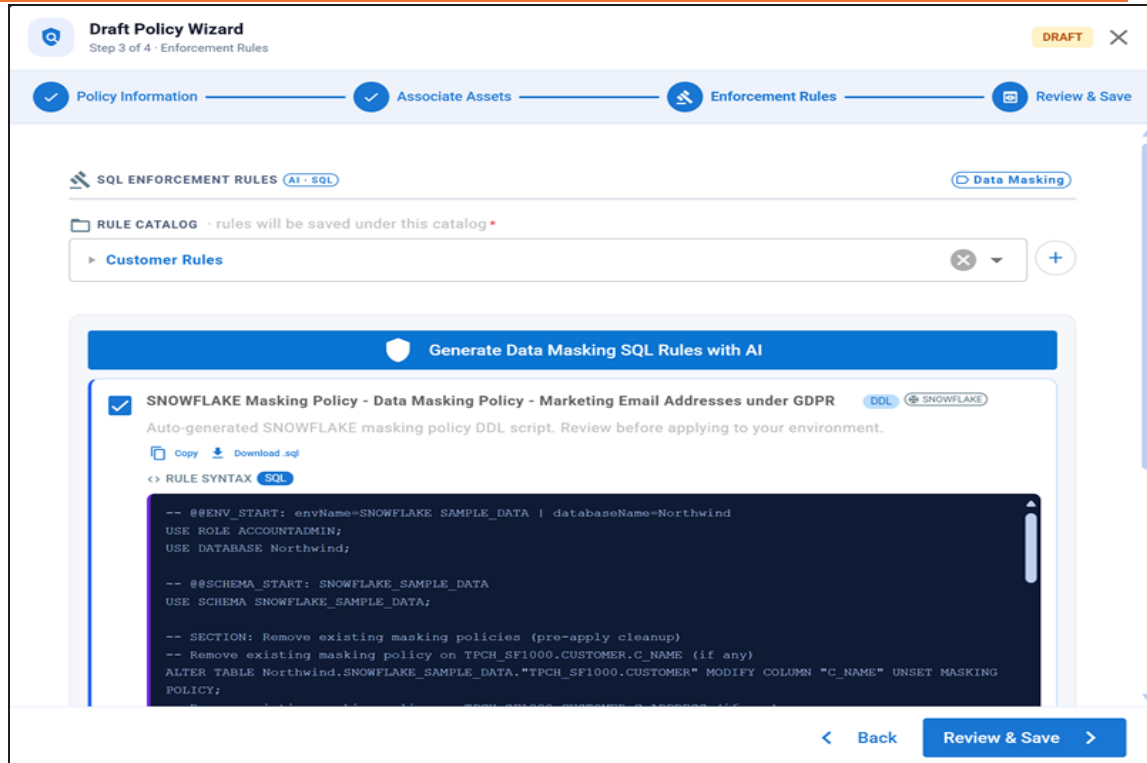
Rules 0 / 0 accepted

[Back](#) [Review & Save](#)

11. In the Rule Catalog field, select a rule catalog from the drop-down list. For example, Customer Rules.
12. Click **Generate Data Masking SQL Rules with AI**.

These are SQL rules used to enforce the policy. The system generates the SQL rules automatically. No manual input is required.

## Creating Policies



13. (Optional) If you do not want to enforce the policy immediately and want to assess it outside the Quest DI system, click one of the following:

- **Copy**
- **Download**

14. After verification, click **Review & Save**.

The Review & Save page displays the policy summary.

## Creating Policies

**Draft Policy Wizard**  
Step 4 of 4 · Review & Save

**Policy Information** **Associate Assets** **Enforcement Rules** **Review & Save**

**FULL REVIEW SUMMARY**

**POLICY INFORMATION**

Name: Data Masking Policy - Marketing Email Addresses under GDPR

Type: Data Masking

**ASSETS**

Target Platform: SNOWFLAKE

Tables: 0 selected

Columns: 5 selected

Columns selected: SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC... SNOWFLAKE\_SAMPLE\_DATA.TPC...

**RULES**

Catalog: Customer Rules

Accepted: 1 / 1

**SNOWFLAKE Masking Policy - Data Masking Policy - Marketing Email Addresses under GDPR** (DDL)

Apply SNOWFLAKE dynamic data masking to sensitive columns identified in the 'Data Masking Policy - Marketing Email Addresses under GDPR' ...

[< Back](#) [Save with 1 Rule\(s\)](#)

15. Click **Save with n rule(s)**.

The rules are saved in the Quest DI database, and you return to the Policies tab.

For further workflow, refer to the [Managing Policies](#) topic.

# Managing Policies

After you create and associate policies with your data assets, you can perform several actions to maintain and enforce your data governance rules. The policies tab provides comprehensive tools to monitor, modify, and apply your policies across your data infrastructure.

Managing policies involves:


- Using AI Explain to understand policies
- Viewing policy details
- Editing policies
- Reviewing policy activity history
- Enforcing policies on environment
- Viewing policy relationships in Mind Map
- Deleting policies

## Using AI Explain


The AI Explain feature generates a simplified summary of your policy. This is particularly useful for stakeholders who need to understand the policy's purpose without reviewing the complete technical details.


To understand the complete configuration of a policy, you can view its detailed information.


To generate AI explanation :

1. On the Policies tab, locate the policy to be explained.
2. In the Actions column, click .

The AI Policy Explanation pane opens.

**AI Policy Explanation**✕  
Data Masking Policy - Marketing Email Addresses under GDPR


 **This policy ensures that email addresses in the Marketing data domain are partially hidden for most users, showing only the first five characters, while only administrators can see the full email addresses, in order to comply with GDPR privacy requirements.**

 **EXPLANATION**

The purpose of this policy is to protect the privacy of individuals whose email addresses are stored in the Marketing data domain, in line with the General Data Protection Regulation (GDPR). It does this by automatically hiding part of each email address so that only the first five characters are visible to most users. This means that, for example, if an email address is 'alice.smith@example.com', non-administrative users would only see 'alice' and the rest would be hidden.

Only users with administrative privileges are allowed to view the full, unmasked email addresses. All other roles, such as marketing analysts or general staff, will only see the partially masked version. This restriction helps prevent unauthorized access to personal information and reduces the risk of accidental data exposure.


The policy is enforced through technical controls within the data systems, ensuring that the masking happens automatically and consistently. Regular audits are conducted to make sure the policy is being followed and that personal data is not

 This content was created with the help of AI to improve speed and efficiency. Please review before use.↻ [Re-explain](#)Close


You can use the **Re-explain** button to explore the explanation further.

This pane also displays associated Tables, Governed Columns, and Enforced Rules. Scroll down to view them.


## Managing Policies




**AI Policy Explanation**  
Data Masking Policy - Marketing Email Addresses under GDPR










The policy is enforced through technical controls in the data systems, meaning the masking happens automatically and cannot be bypassed by regular users. Regular audits are also performed to make sure the policy is being followed and that personal data is not exposed inappropriately. This approach helps the organization meet GDPR requirements and protect the privacy of individuals whose data they manage.


 **Tables** 0


*No tables associated*


 **Governed Columns** 6





-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.CUSTO
-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.CUSTO
-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.LINEI
-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.LINEI
-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.LINEI
-  SNOWFLAKE\_SAMPLE\_DATA.TPCH\_SF1000.NATIO

 **RULES ENFORCED**

-  **SNOWFLAKE Masking Policy - Data Masking Policy - Marketing Email Addresses under GDPR**  
Auto-generated SNOWFLAKE masking policy DDL script.

 This content was created with the help of AI to improve speed and efficiency. Please review before use.






## Viewing Policy Details

To understand the complete configuration of a policy, you can view its detailed information.

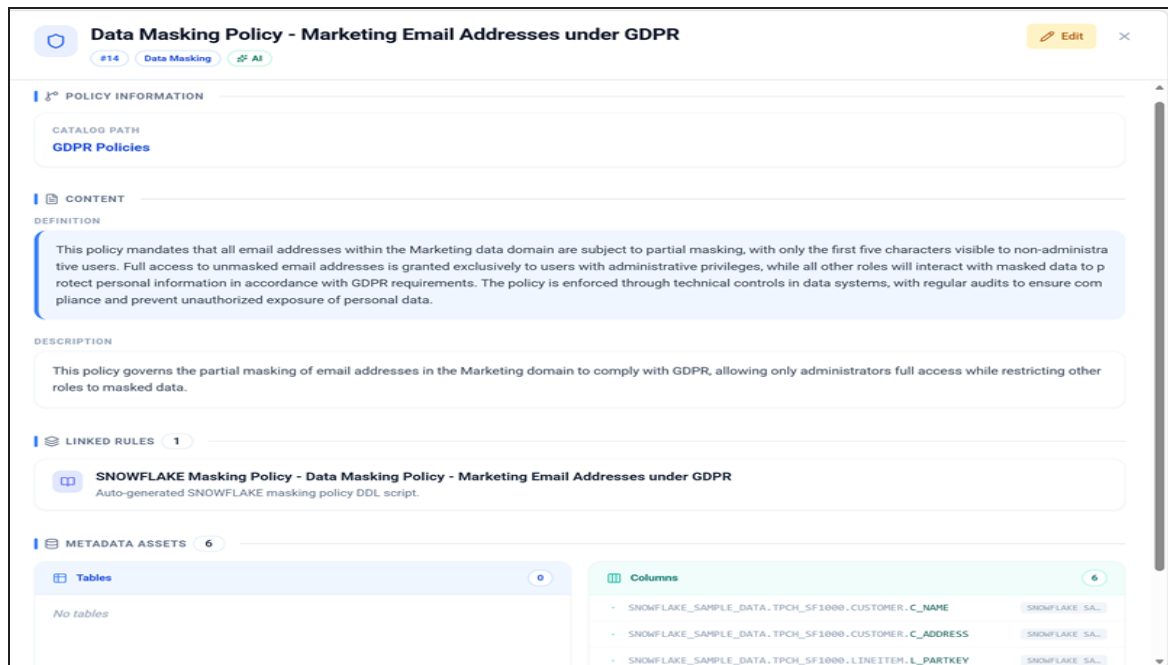
To view policy details:

1. On the Policies tab, locate the policy you want to view.
2. In the Actions column, click  .



## Managing Policies

The Policy pane opens displaying Policy Information.




You can also open the Edit Policy Wizard by clicking the **Edit** button in the top-right corner.

## Editing Policies

You can modify an existing policy to update its definition, associated assets, rules, or other configurations.

To edit a policy:

1. On the Policies tab, locate the policy to be explained.
2. In the Actions column, click .

The Edit Policy Wizard opens, displaying the current configuration.

## Managing Policies

The screenshot shows the 'Edit Policy Wizard' interface, specifically 'Step 1 of 4 - Policy Information'. The wizard has four steps: Policy Information, Associate Assets, Linked Rules, and Review & Save. The 'Policy Information' step is active. It contains the following fields:

- POLICY DETAILS**
  - POLICY NAME**: Data Masking Policy - Marketing Email Addresses under GDPR (58 / 250 characters)
  - CATALOG PATH**: GDPR Policies
  - DESCRIPTION**: This policy governs the partial masking of email addresses in the Marketing domain to comply with GDPR, allowing only administrators full access while restricting other roles.
  - DEFINITION**: This policy mandates that all email addresses within the Marketing data domain are subject to partial masking, with only the first five characters visible to non-administrative users. Full access to unmasked email addresses is granted exclusively to users with administrative privileges, while all other roles will interact with masked data to protect personal information in accordance with GDPR requirements. The policy is enforced through technical controls in data systems, with regular audits to ensure compliance and prevent unauthorized exposure of personal data.
  - POLICY TYPE**: Data Masking
  - TAGS**: email-address, gdpr, access-control, data-masking, marketing, privacy

An 'Associate Assets' button is located at the bottom right of the form.

3. Make any necessary changes, such as:

- Removing existing assets (tables, columns, or data elements)
- Adding new assets to the policy scope
- Modifying the policy definition or description
- Updating associated rules and conditions

The Edit Policy Wizard takes you through the same policy creation workflow, allowing you to make changes at any stage. For more information, refer to the [Creating Policies](#) topic.

## Viewing Activity Log

The Activity Log section maintains a comprehensive record of all changes made to a policy. This audit trail enables you to track modifications and understand the policy's evolution over time.

What the Activity Log records:


## Managing Policies


---

- Adding or removing tables and columns
- Changes to the policy definition or description
- Modifications to policy rules and conditions
- All updates and revisions made during policy lifecycle


The Activity Log provides full traceability of your policy management activities, which is essential for compliance and audit purposes.


To view the Activity Log:


1. On the Policies tab, locate the policy for which you want to view the Activity Log.
2. In the Actions column, click . The Activity Log opens.


 **Activity Log**

Data Masking Policy - Marketing Email Addresses under GDPR





 Expand all

 Collapse all

 **Assign Record**

4 records







Columns assigned

ADMINISTRATOR

May 28, 2026, 07:15:34 AM


 Hide details




Columns assigned

ADMINISTRATOR

May 26, 2026, 05:22:22 AM


 View details




Rules assigned

ADMINISTRATOR

May 26, 2026, 05:22:22 AM


 View details




Tags assigned


ADMINISTRATOR


May 26, 2026, 05:22:21 AM

 View details

 **Add Record**

1 record






Policy Created

ADMINISTRATOR

May 26, 2026, 05:22:21 AM

 View details


### Enforcing Policies



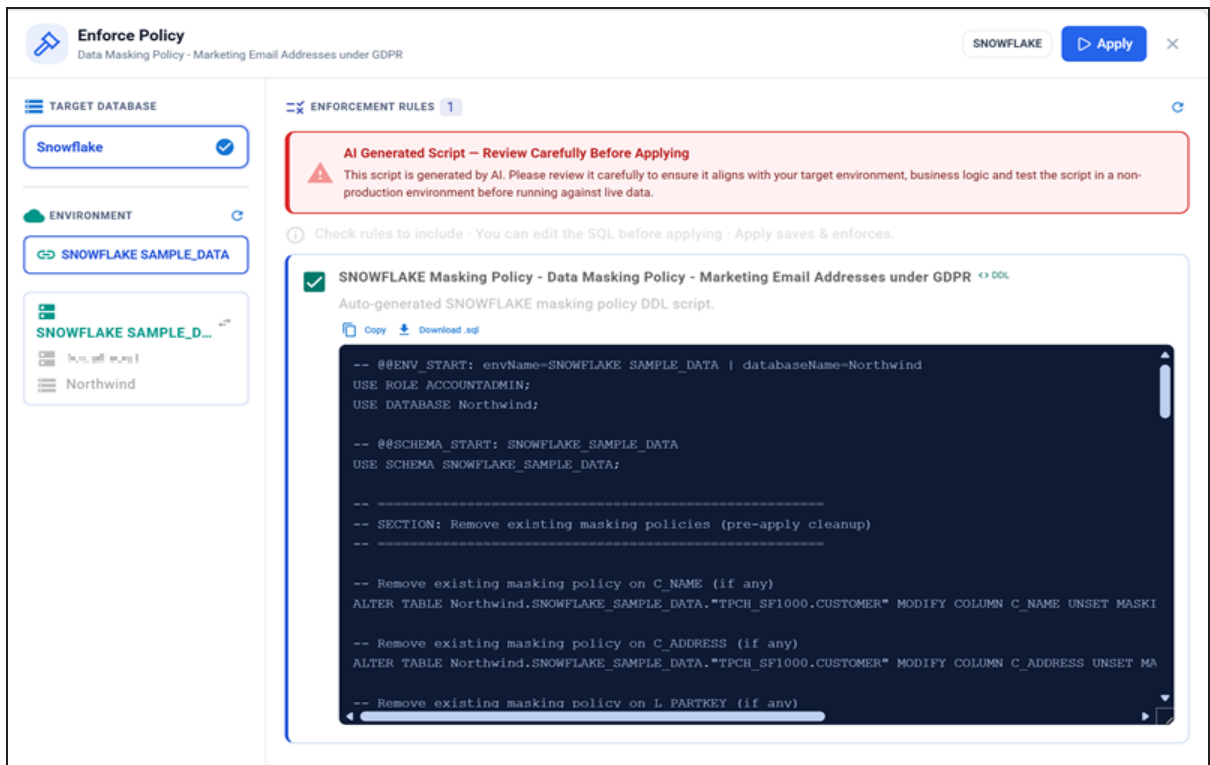
The SQL script generated by AI should be reviewed and tested in a non-production environment before enforcement on production. Ensure you have the required permissions before applying policies to production systems.

Policy enforcement is the final stage in the policy management workflow. During this stage, the SQL queries generated for your policy are applied to your environment through Quest DI.

To enforce a policy:

1. On the Policies tab, locate the policy to be enforced.
2. In the Actions column, click .

The Enforce Policy pane opens.



**Enforce Policy**  
Data Masking Policy - Marketing Email Addresses under GDPR

**TARGET DATABASE**  
Snowflake

**ENVIRONMENT**  
SNOWFLAKE SAMPLE\_DATA

**ENFORCEMENT RULES 1**

**AI Generated Script – Review Carefully Before Applying**  
This script is generated by AI. Please review it carefully to ensure it aligns with your target environment, business logic and test the script in a non-production environment before running against live data.

Check rules to include - You can edit the SQL before applying - Apply saves & enforces.

**SNOWFLAKE Masking Policy - Data Masking Policy - Marketing Email Addresses under GDPR**  
Auto-generated SNOWFLAKE masking policy DDL script.

```
-- @@ENV_START: envName=SNOWFLAKE SAMPLE_DATA | dbName=Northwind
USE ROLE ACCOUNTADMIN;
USE DATABASE Northwind;

-- @@SCHEMA_START: SNOWFLAKE_SAMPLE_DATA
USE SCHEMA SNOWFLAKE_SAMPLE_DATA;

-- SECTION: Remove existing masking policies (pre-apply cleanup)

-- Remove existing masking policy on C_NAME (if any)
ALTER TABLE Northwind.SNOWFLAKE_SAMPLE_DATA."TPCH_SF1000.CUSTOMER" MODIFY COLUMN C_NAME UNSET MASKING POLICY;

-- Remove existing masking policy on C_ADDRESS (if any)
ALTER TABLE Northwind.SNOWFLAKE_SAMPLE_DATA."TPCH_SF1000.CUSTOMER" MODIFY COLUMN C_ADDRESS UNSET MASKING POLICY;

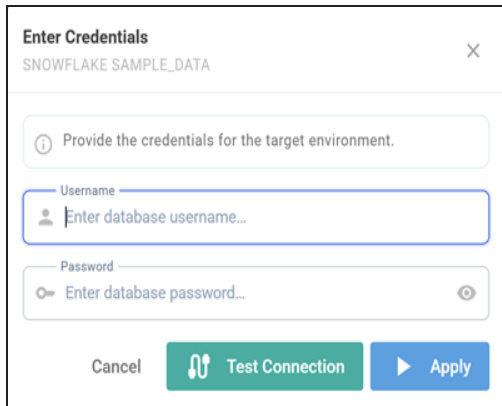
-- Remove existing masking policy on L_PARTKEY (if any)
```

## Managing Policies

---

3. Select the target environment. For example, Snowflake Sample\_Data.
4. Click **Apply**.

The Enter Credentials dialog appears.



The screenshot shows a dialog box titled "Enter Credentials" with a close button (X) in the top right corner. Below the title is the text "SNOWFLAKE SAMPLE\_DATA". A message box with an information icon says "Provide the credentials for the target environment." Below this are two input fields: "Username" with a placeholder "Enter database username..." and "Password" with a placeholder "Enter database password..." and a toggle icon. At the bottom are three buttons: "Cancel", "Test Connection" (with a plug icon), and "Apply" (with a play icon).

5. Confirm you have the necessary permissions and enter your database credentials.

For more information on connections, refer to the [Creating and Managing Environments](#) topic.

6. Click **Test Connection**.
7. After the connection is verified, click **Apply**.

The SQL rules execute on the environment. Data masking takes effect based on the policy rules.

## Managing Policies

**Enforce Policy**  
Data Masking Policy - Marketing Email Addresses under GDPR

SNOWFLAKE **Apply**

**TARGET DATABASE**  
Snowflake

**ENVIRONMENT**  
SNOWFLAKE SAMPLE\_DATA

**ENFORCEMENT RULES 1**

**AI Generated Script — Review Carefully Before Applying**  
This script is generated by AI. Please review it carefully to ensure it aligns with your target environment, business logic and test the script in a non-production environment before running against live data.

Check rules to include · You can edit the SQL before applying · Apply saves & enforces.

**SNOWFLAKE Masking Policy - Data Masking Policy - Marketing Email Addresses under GDPR** [DDL](#)  
Auto-generated SNOWFLAKE masking policy DDL script.

Copy Download .sql

```
-- @@ENV_START: envName=SNOWFLAKE SAMPLE_DATA | databaseName=TEST_DB
USE ROLE ACCOUNTADMIN;
USE DATABASE TEST_DB;

-- @@SCHEMA_START: PUBLIC
USE SCHEMA PUBLIC;

-- SECTION: Remove existing masking policies (pre-apply cleanup)
-- Remove existing masking policy on PHONE (if any)
ALTER TABLE TEST_DB.PUBLIC.CUSTOMERS MODIFY COLUMN PHONE UNSET MASKING POLICY;
```

**Executed Successfully** 12 OK 12 statements 7096ms on SNOWFLAKE SAMPLE\_DATA

**EXECUTION LOG**

- Executed: USE ROLE ACCOUNTADMIN (0 rows affected)
- Executed: USE DATABASE TEST\_DB (0 rows affected)
- Executed: USE SCHEMA PUBLIC (0 rows affected)
- Executed: ALTER TABLE TEST\_DB.PUBLIC.CUSTOMERS MODIFY COLUMN PHONE UNSET MASKING POLICY (0 rows affected)
- Executed: ALTER TABLE TEST\_DB.PUBLIC.CUSTOMERS MODIFY COLUMN ID UNSET MASKING POLICY (0 rows affected)
- Executed: ALTER TABLE TEST\_DB.PUBLIC.CUSTOMERS MODIFY COLUMN FIRST\_NAME UNSET MASKING POLICY (0 rows affected)

## Reviewing Enforcement Results

After policy enforcement, you can review the execution results to identify which rules were successfully applied and which may require attention.

Result Status	Description	Required Action
Executed	The SQL query executed successfully and the policy rules were applied	No action required
Error	The SQL query failed to execute.	Review the error details and manually



## Managing Policies

Result Status	Description	Required Action
	The rule could not be applied to the specified column or data type	refine the query if needed. Execute the corrected query in a subsequent enforcement step.


## Using Mind Maps

The Mind Map displays all associations and relationships for a policy in a clear, hierarchical view. This helps you understand the complete scope and impact of your policy.

The Mind Map displays:

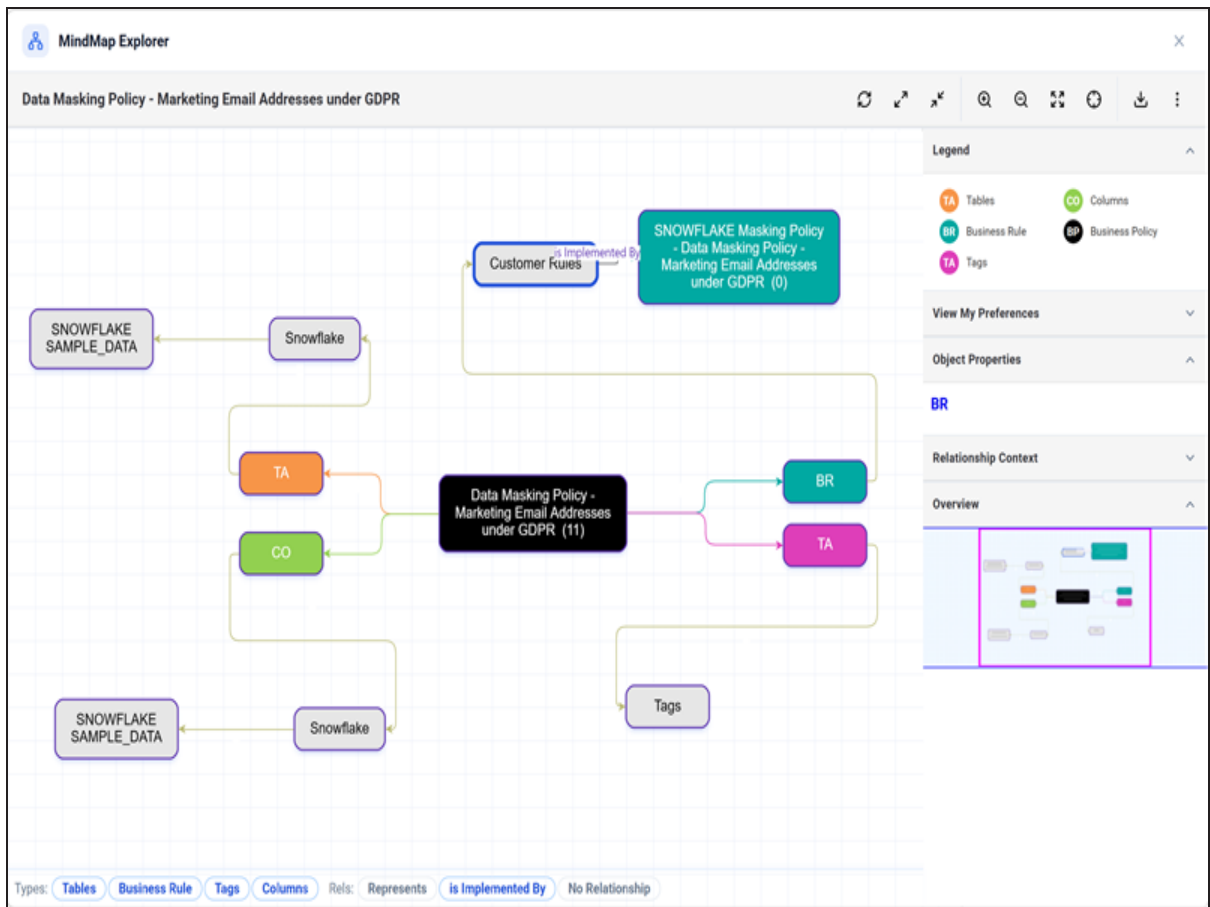
- Which environment, tables, and columns the policy is applied to
- Associated data classifications and tags
- Linked business policies and data quality rules
- Complete asset associations for the policy

To view the mind map:

1. On the Policies tab, locate the policy for which you want to view the mind map.
2. In the Actions column, click .

## Managing Policies

The mind map opens.



## Deleting Policies




Deleting a policy is a permanent action. Ensure you no longer need the policy before proceeding.

When a policy is no longer required, you can delete it from the system. Deletion removes the policy along with all its associations and rules.

To delete a policy:

## Managing Policies

---

1. On the Policies tab, locate the policy to be deleted.
2. In the Actions column, click .

The Confirm Delete dialog appears.

3. Click **Delete**.

The policy, its associations with assets, and all associated rules are removed from the system.