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.

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

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.

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

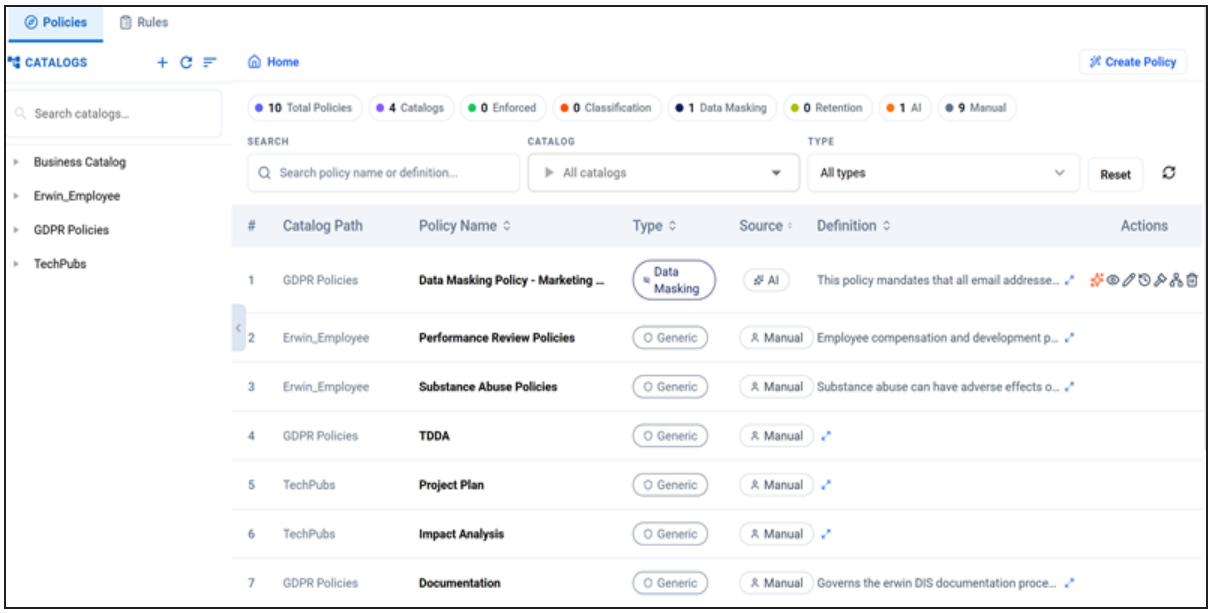
Supported Environments

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.



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
Policies	Use this section to create and manage policies.

Tab	Function
Rules	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

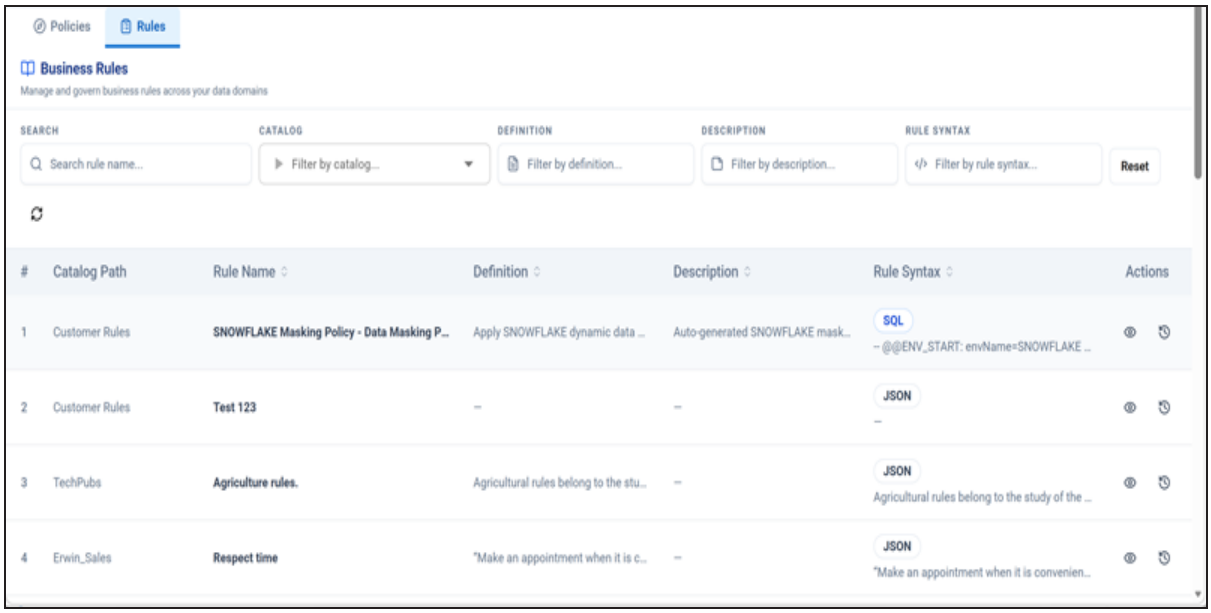
Each policy row in the list includes an Actions column. The following functions are available for each policy:

- - 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.



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

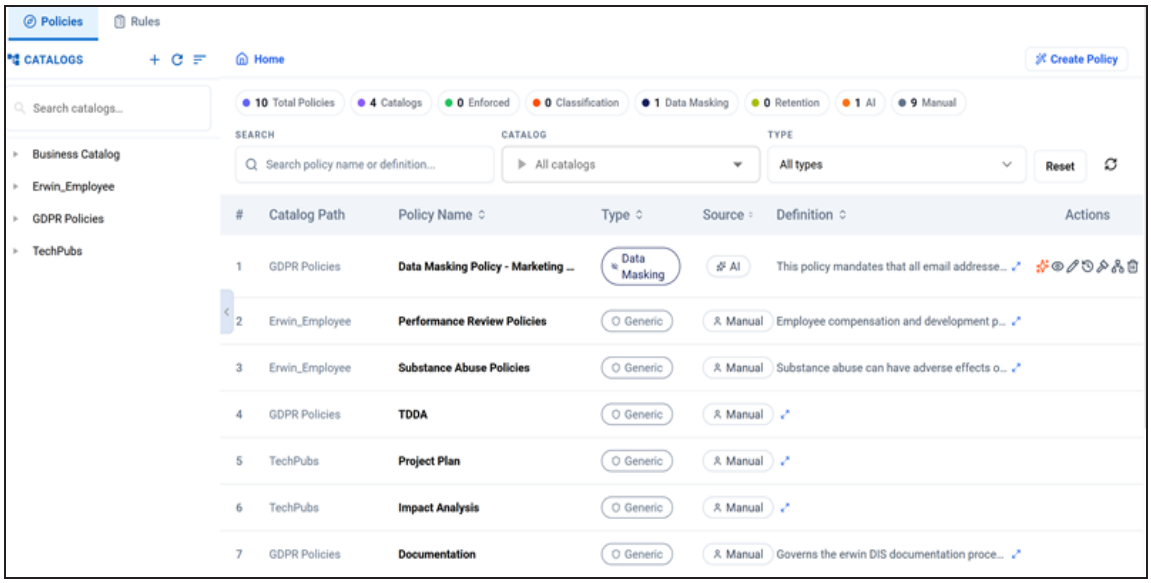
- Ensure you have the required permission to access Policy Manager.
- Understand the policy type you need (Classification, Masking, Retention)
- Have a clear intent for the policy (what data it governs, why, and how)

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:

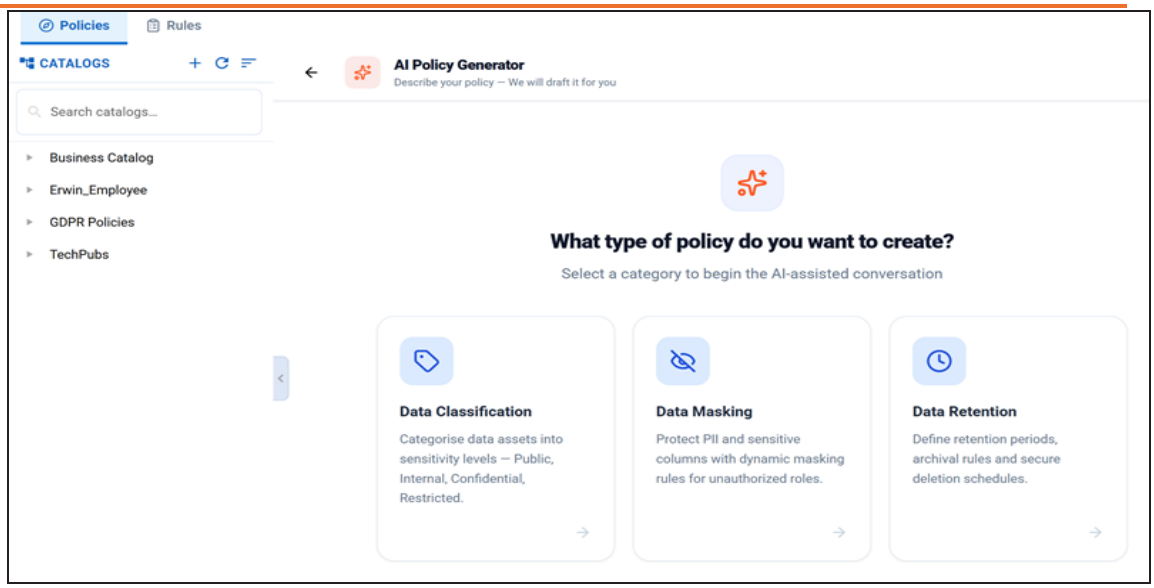
1. Go to **Application Menu** > **Data Governance** > **Policy Manager**.

   The Policy Manager page opens.



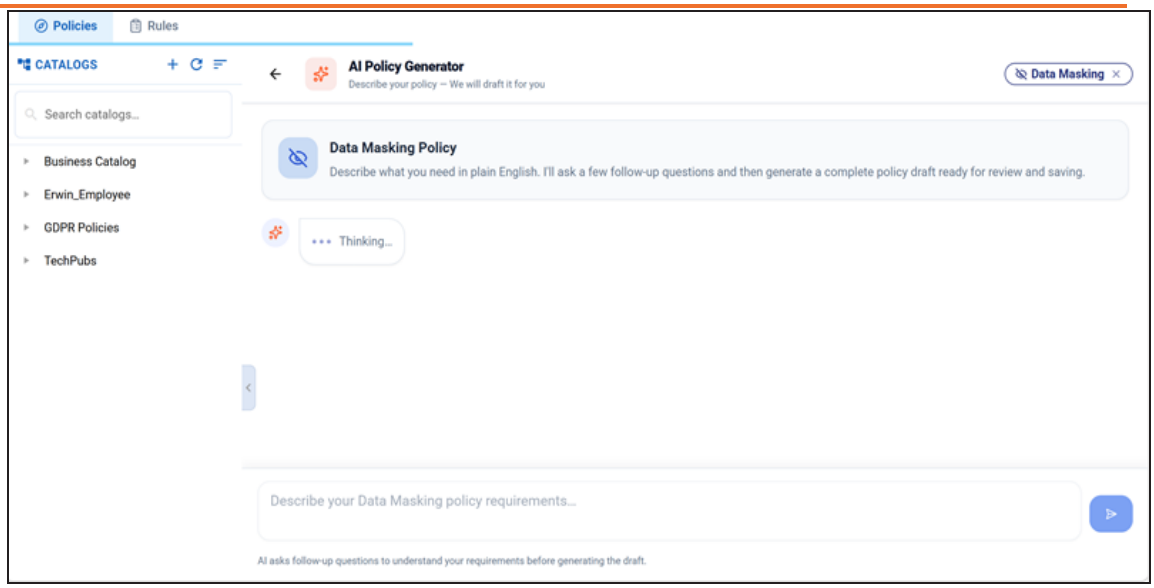
2. On the Policies tab, click **Create Policy**.

   The AI Policy Generator page opens.



3. Select a policy type:
    - Data Classification
    - Data Masking
    - Data Retention

    The AI Policy Generator chat window opens.



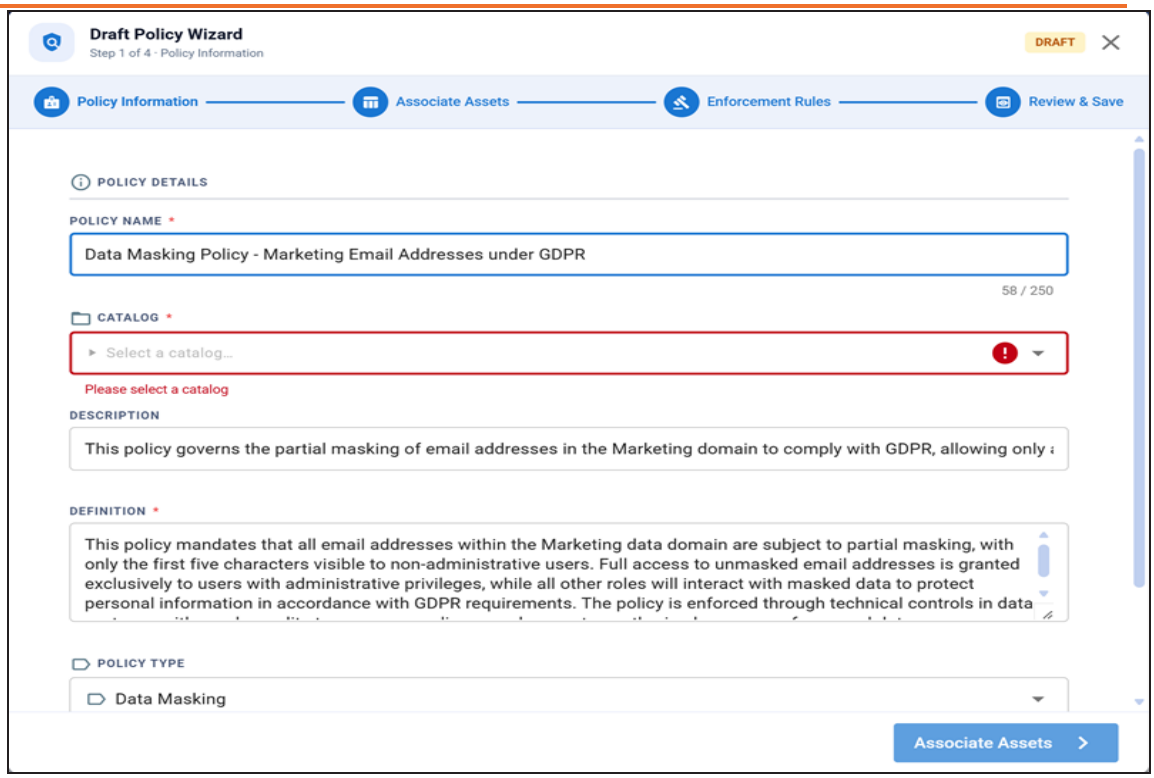
4. Answer the clarification questions prompted by the AI Policy Generator.

   For example:

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

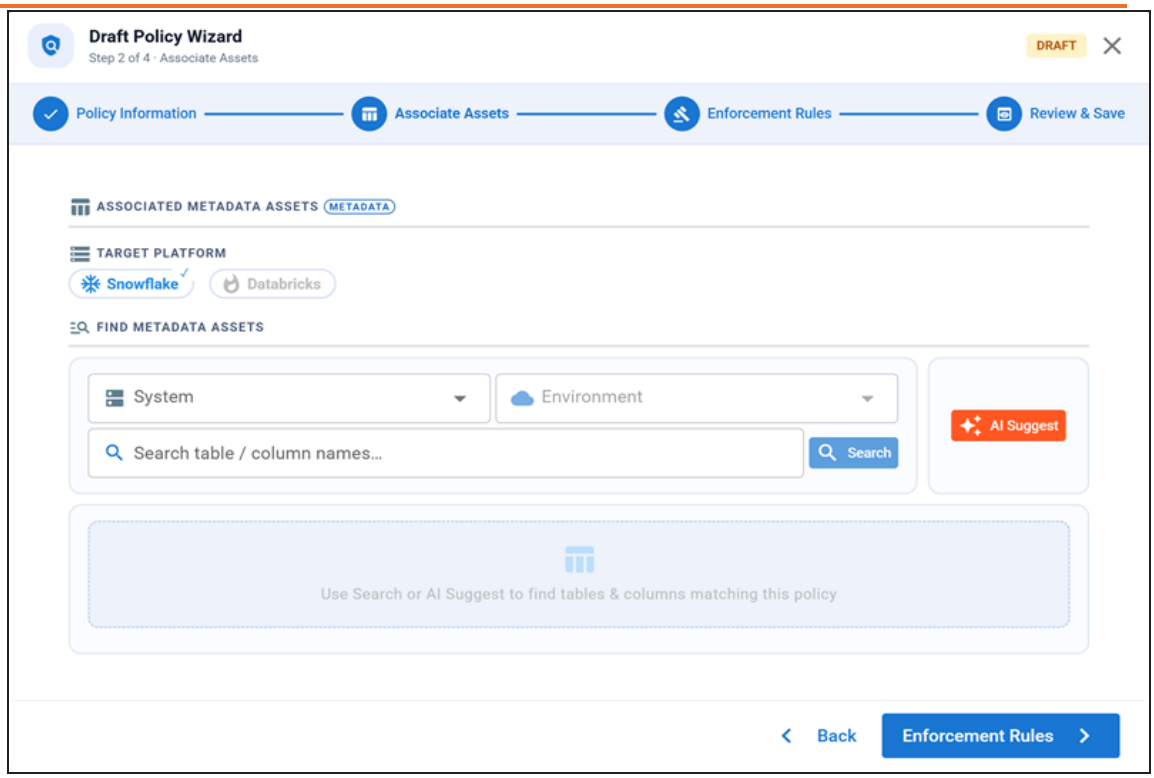
   The AI Policy Generator can ask follow-up questions based on your responses.

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



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.

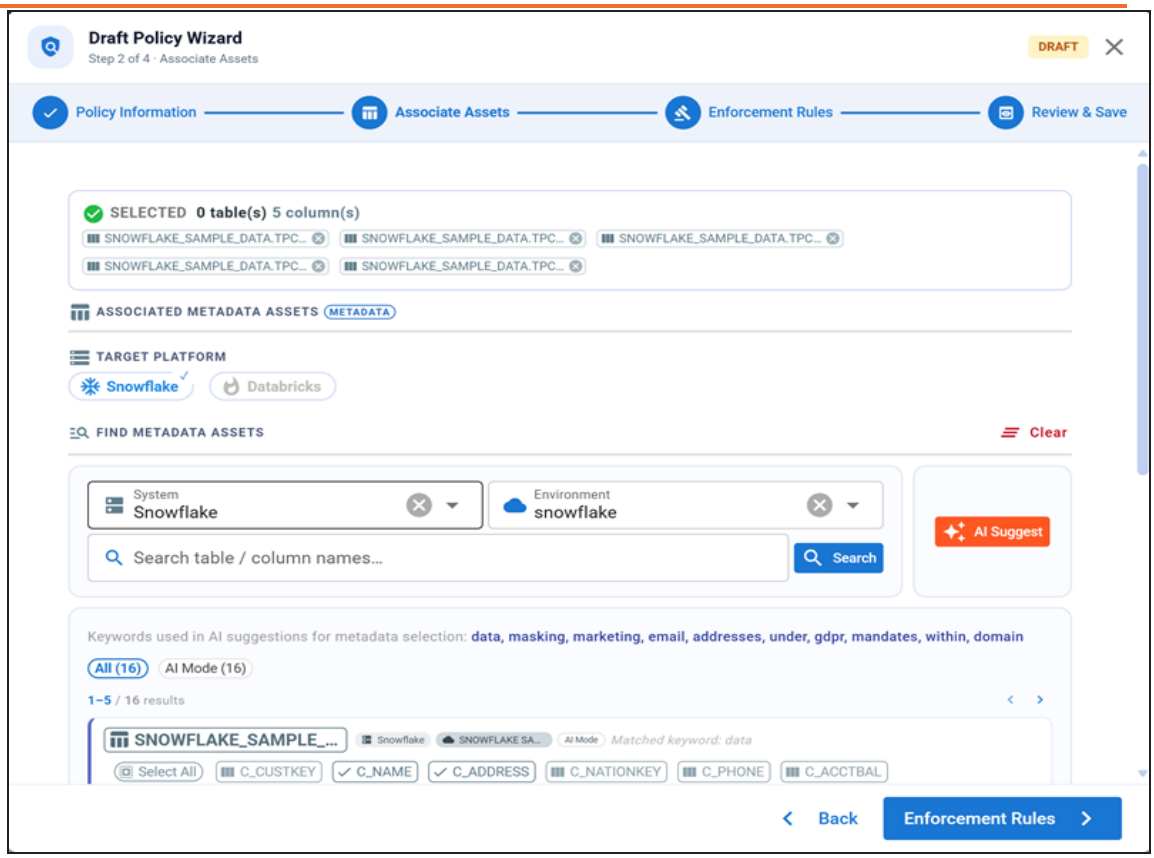


9. Select the system, environment, table, and columns to associate with the policy. You can do one of the following:

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

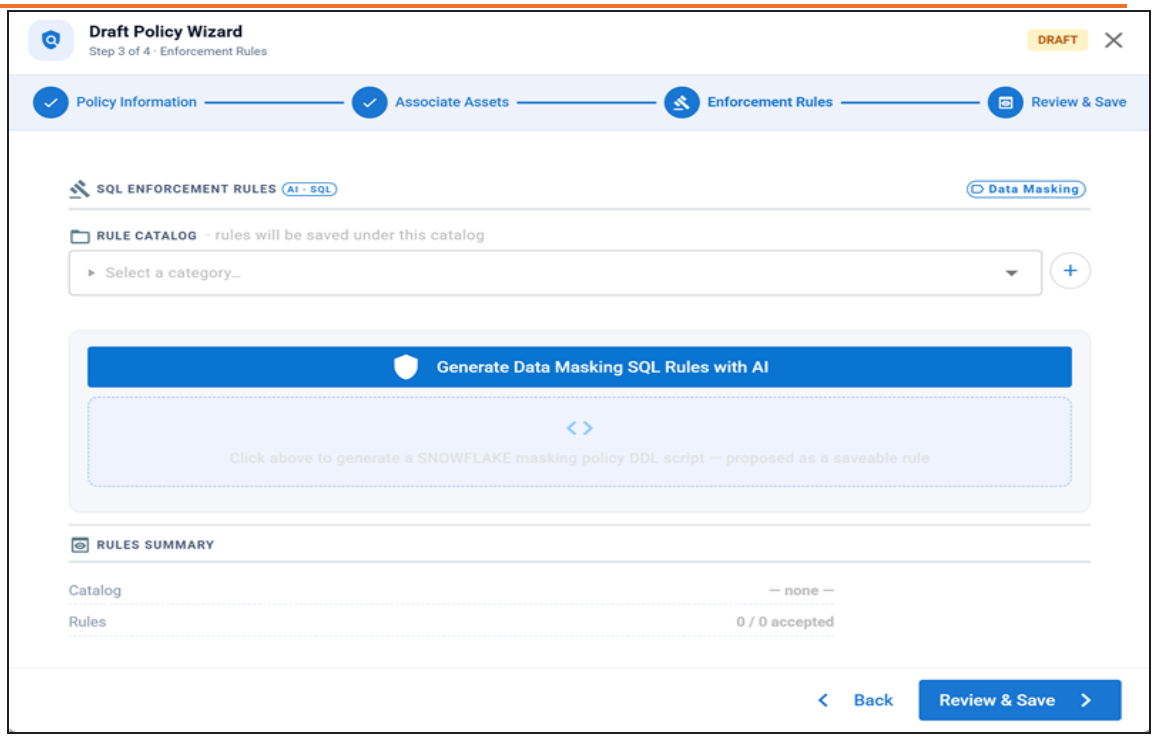
     You can review and accept AI-suggested tables and columns.

   Selected assets appear in the Selected field at the top.



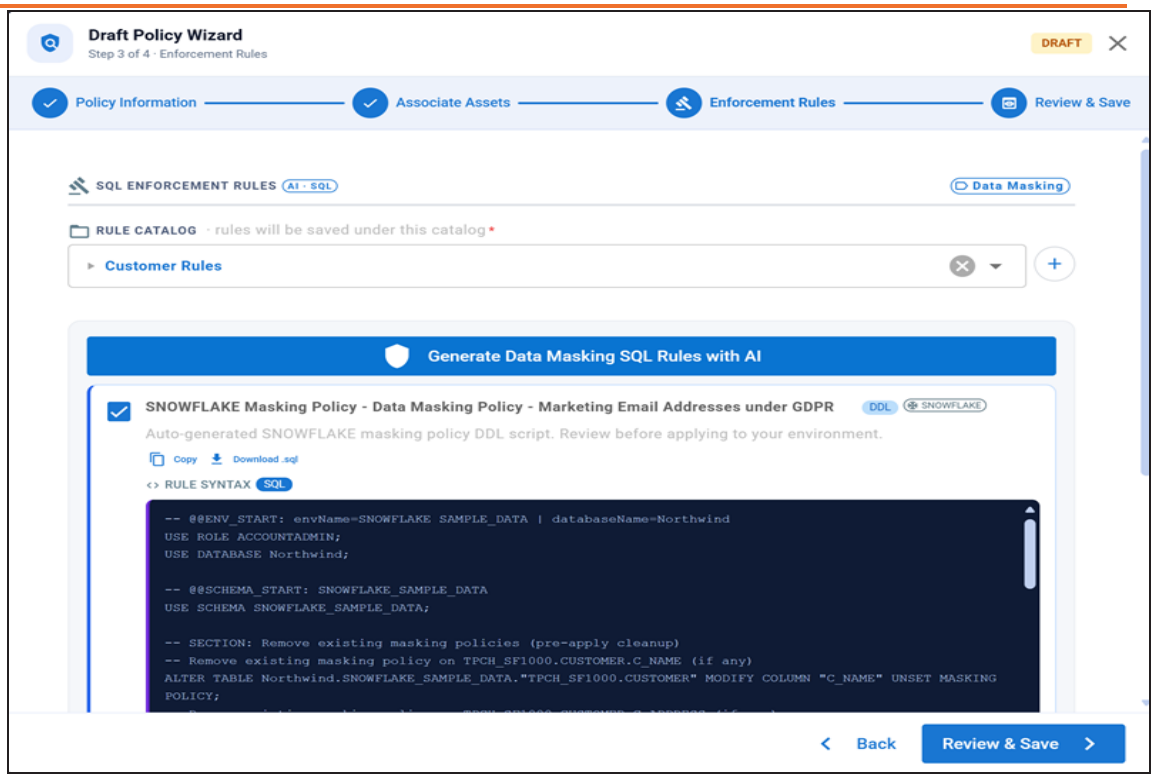
10. Click **Enforcement Rules**.

    The Enforcement Rules section appears.



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.

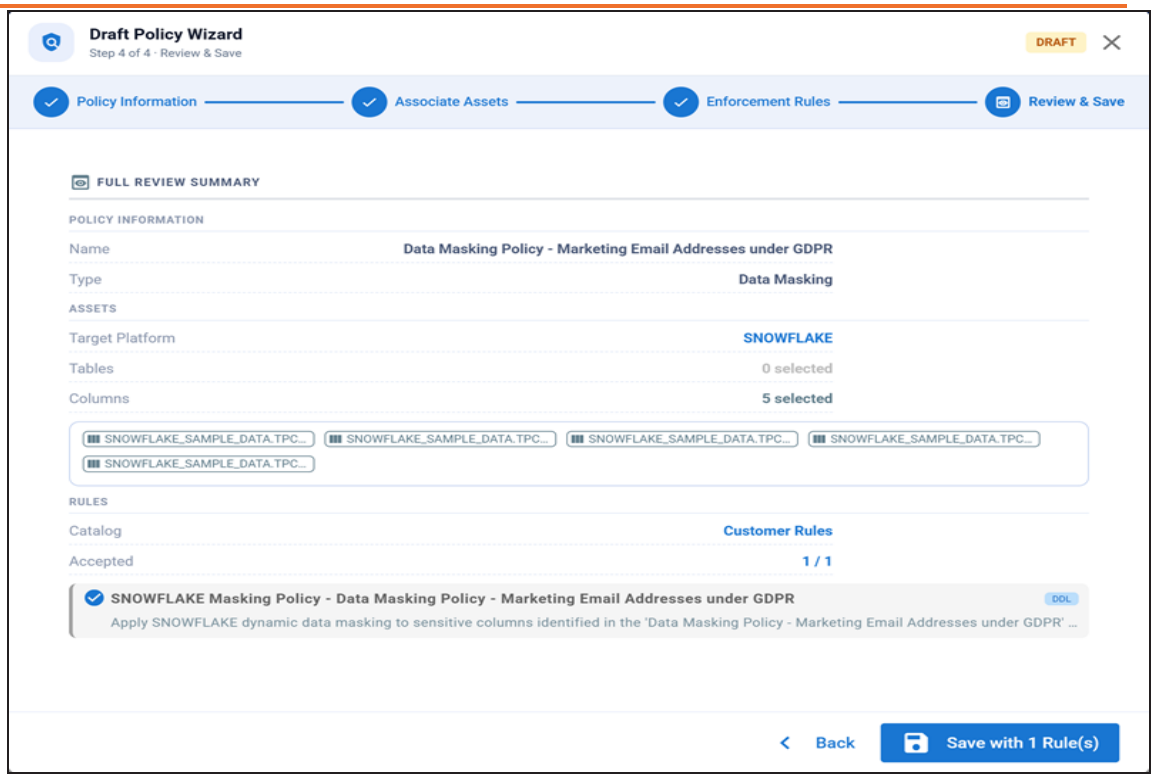


13. (Optional) If you do not want to enforce the policy immediately and want to assess it outside the Quest DI system, click one of the following:

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

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

    The Review & Save page displays the policy summary.



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

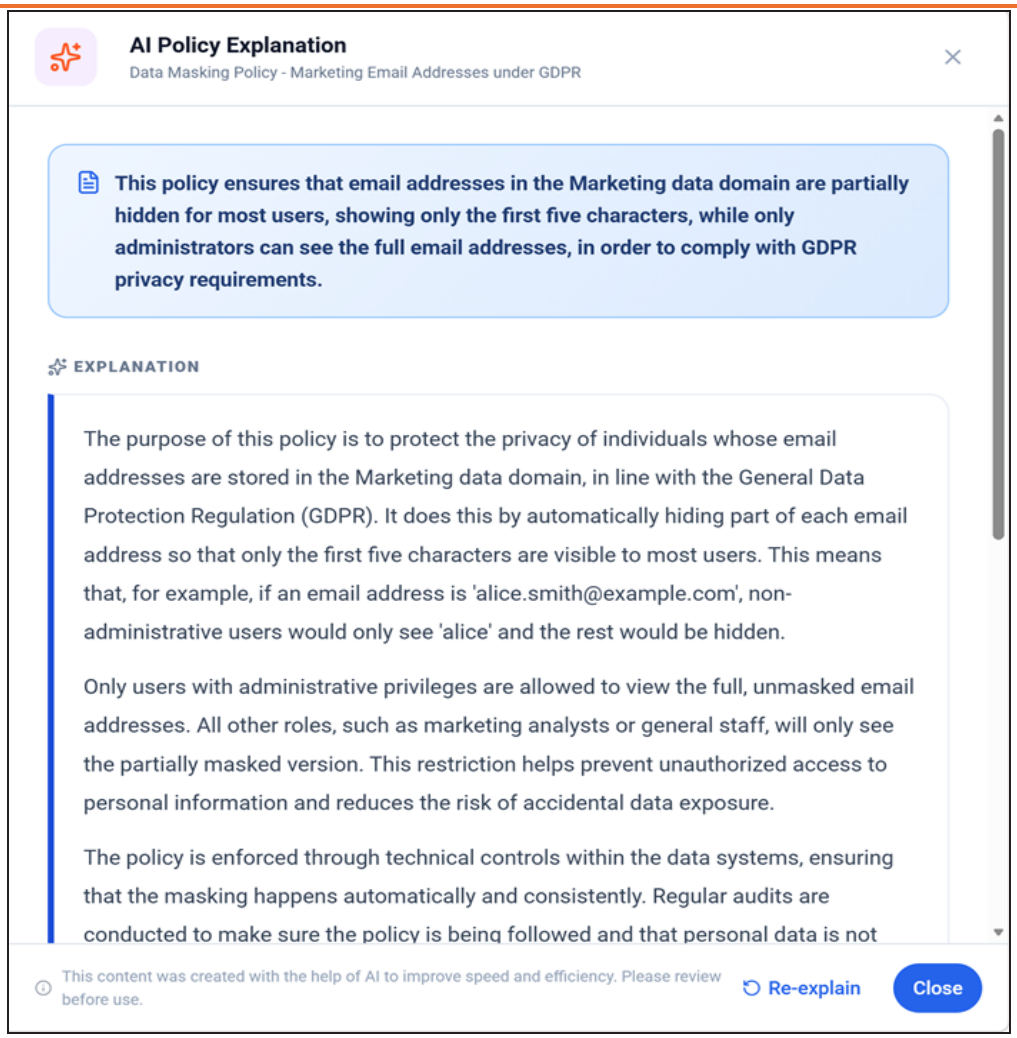
The AI Explain feature generates a simplified summary of your policy. This is particularly useful for stakeholders who need to understand the policy's purpose without reviewing the complete technical details.

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

To generate AI explanation :

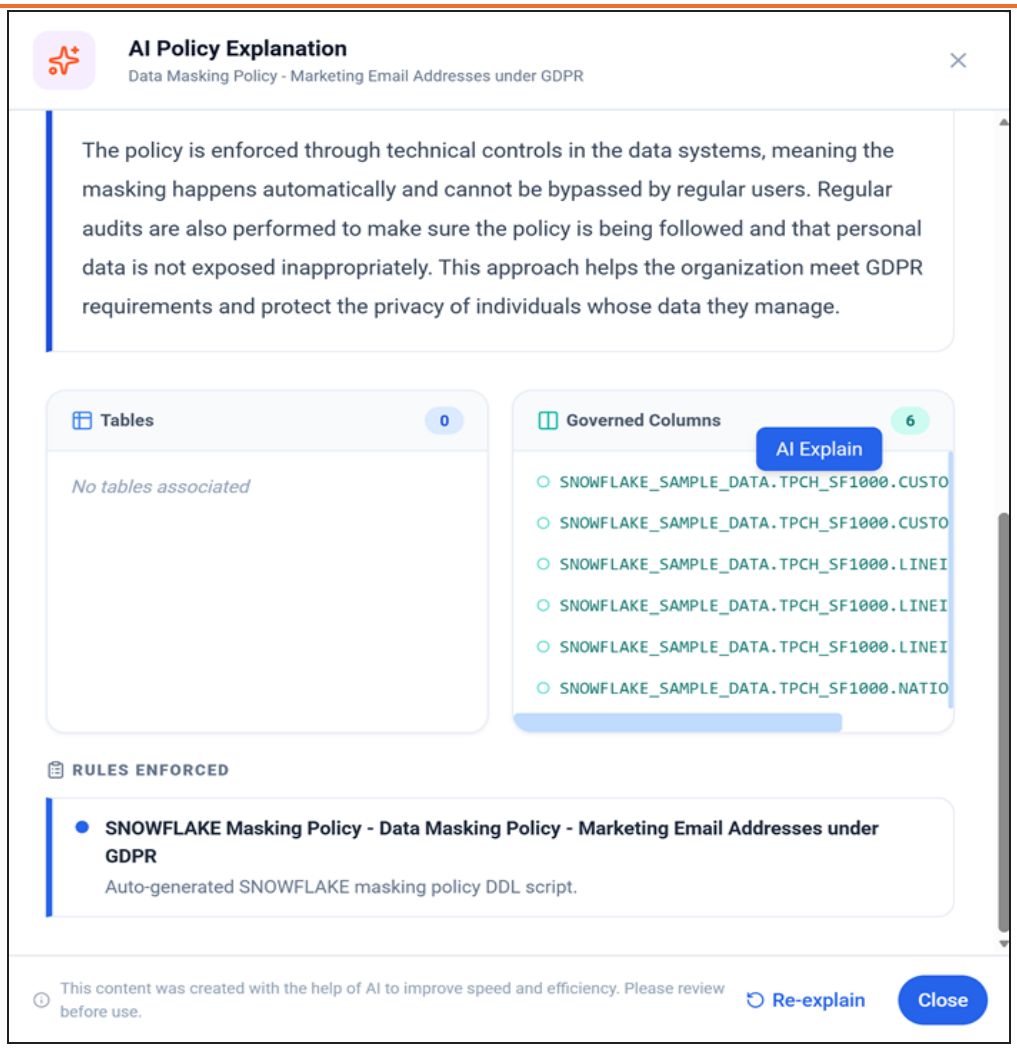
1. On the Policies tab, locate the policy to be explained.
2. In the Actions column, click  .

   The AI Policy Explanation pane opens.



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.



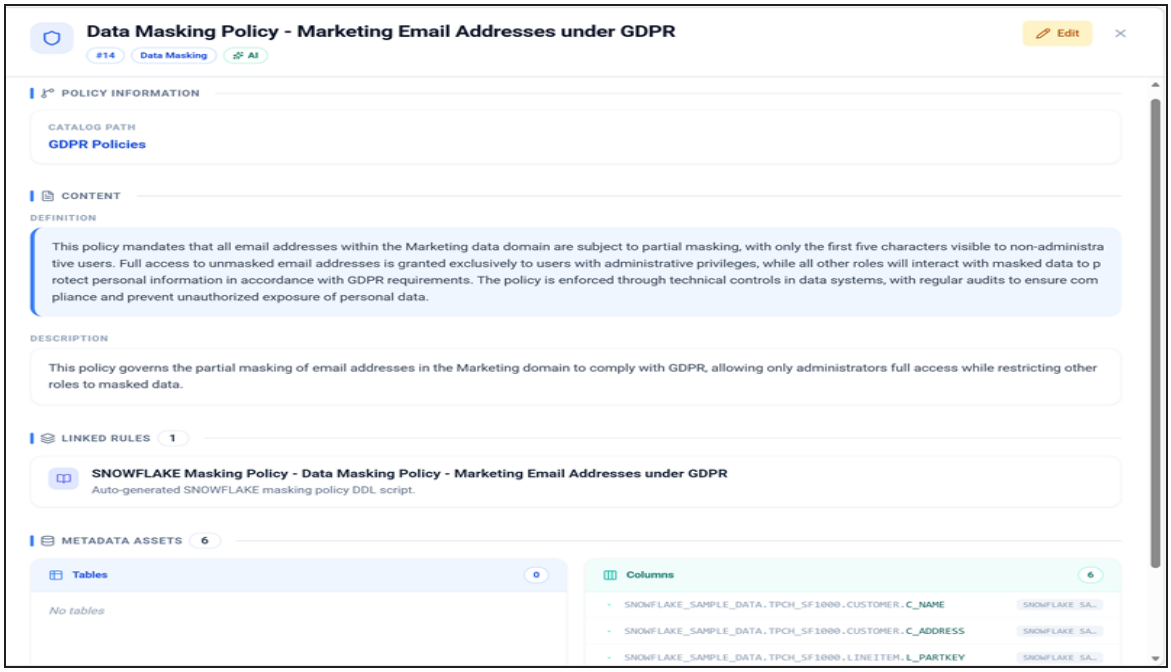
Viewing Policy Details

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  .

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.

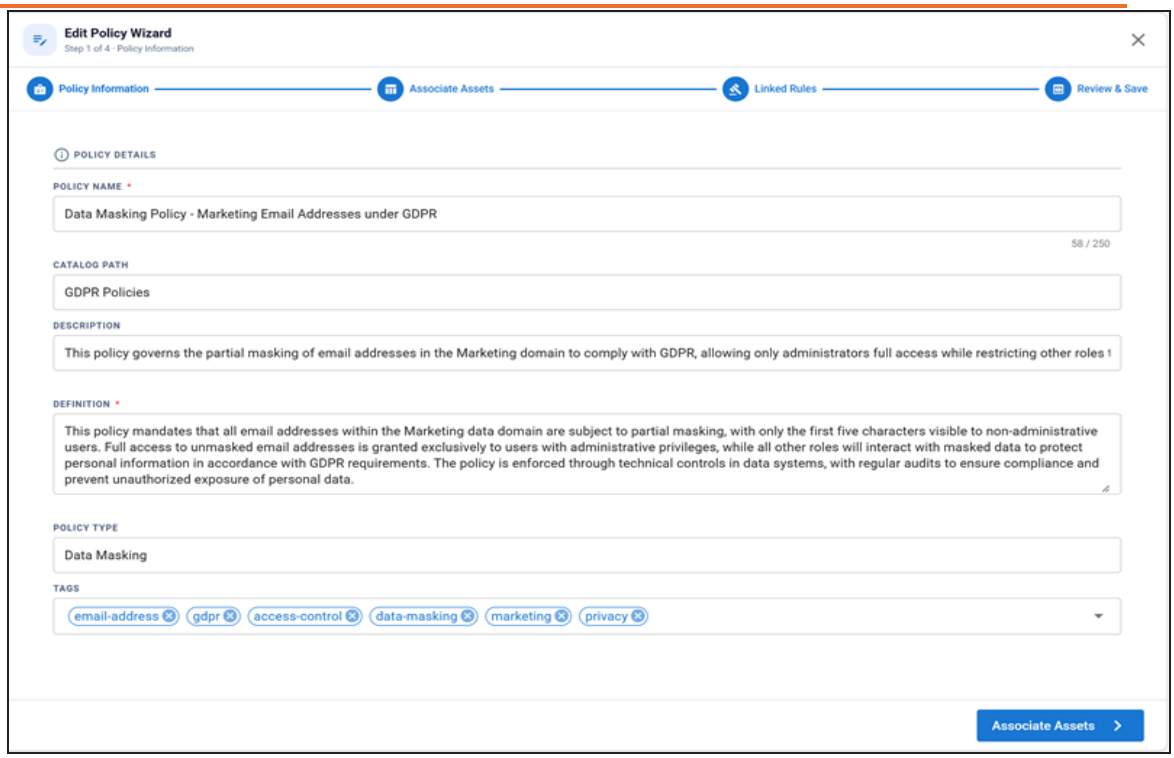
Editing Policies

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.



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.

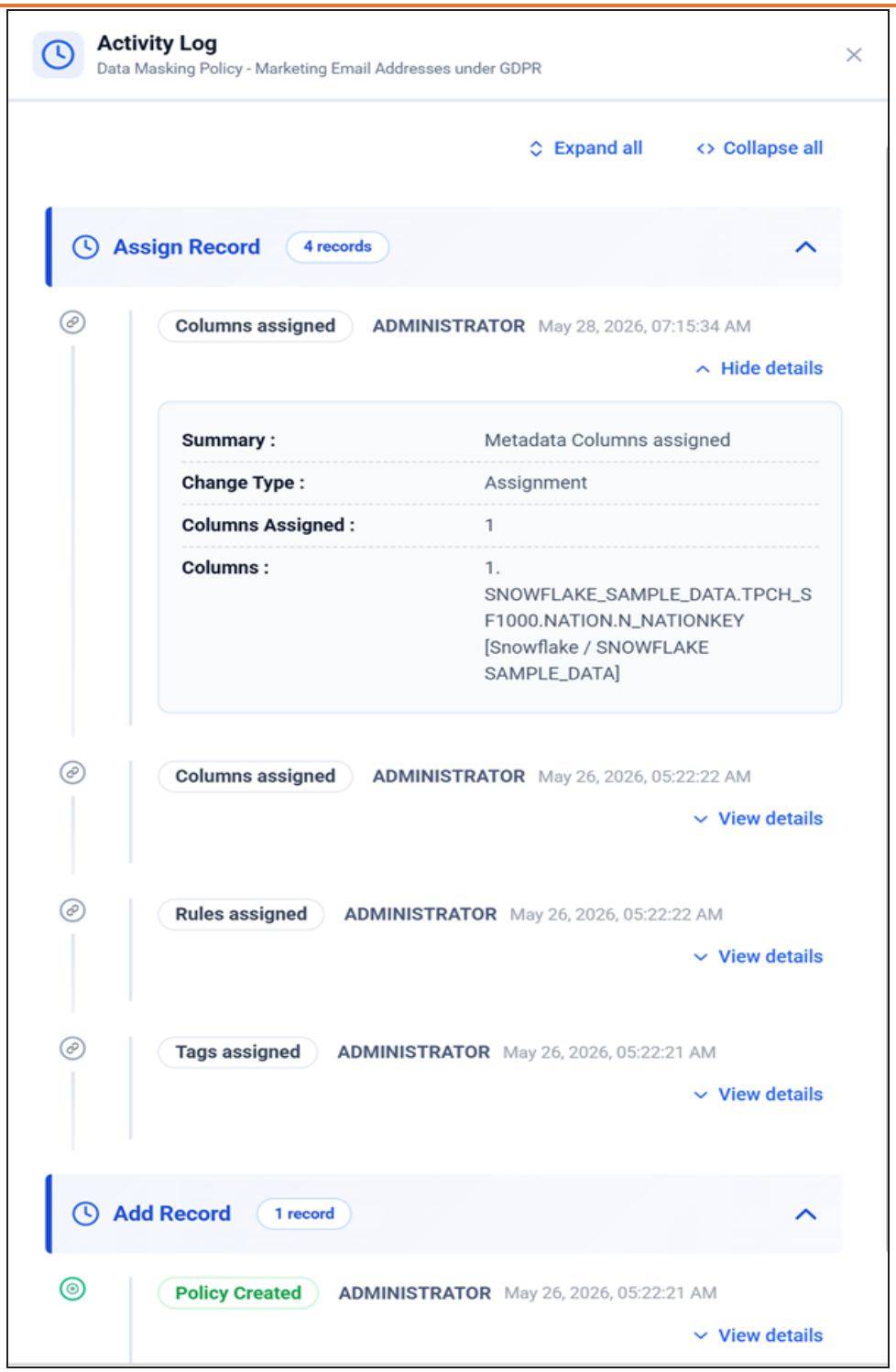
What the Activity Log records:

- 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
Summary :
Metadata Columns assigned
Change Type :
Assignment
Columns Assigned :
1
Columns :
1. SNOWFLAKE_SAMPLE_DATA.TPCH_SF1000.NATION.N_NATIONKEY [Snowflake / SNOWFLAKE SAMPLE_DATA]
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

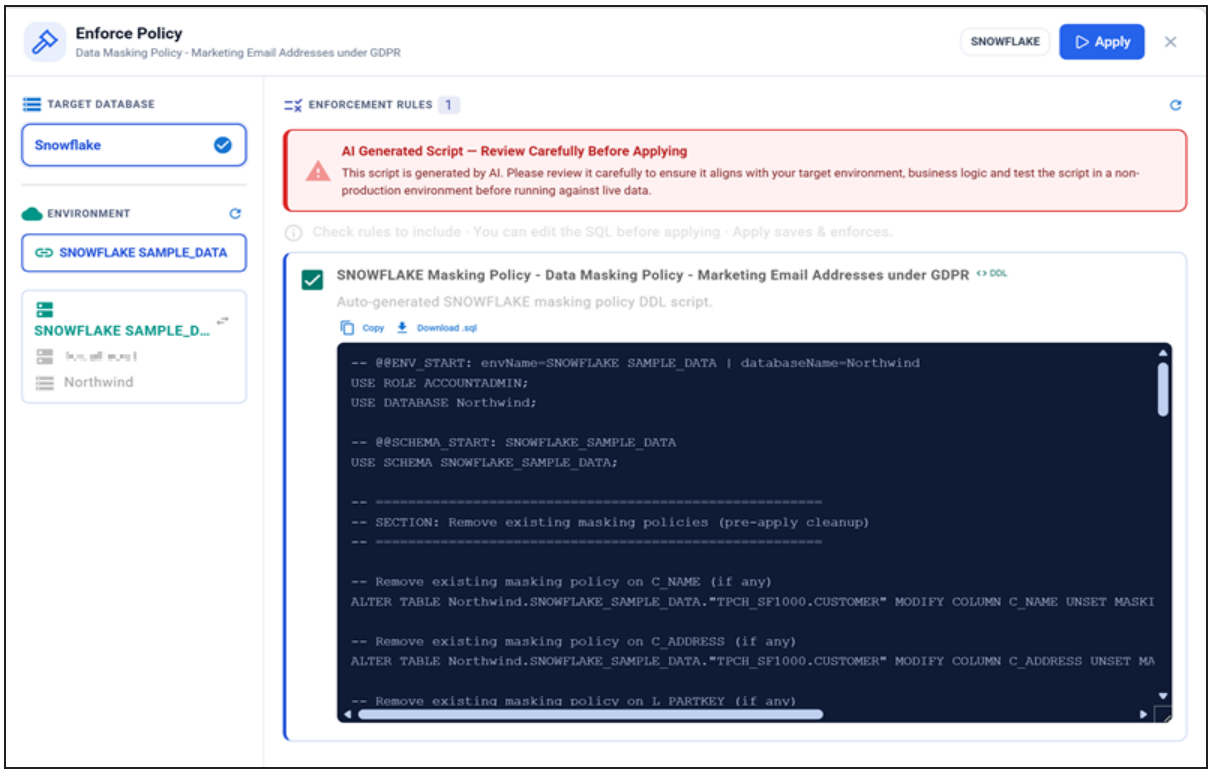
The SQL script generated by AI should be reviewed and tested in a non-production environment before enforcement on production. Ensure you have the required permissions before applying policies to production systems.

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:

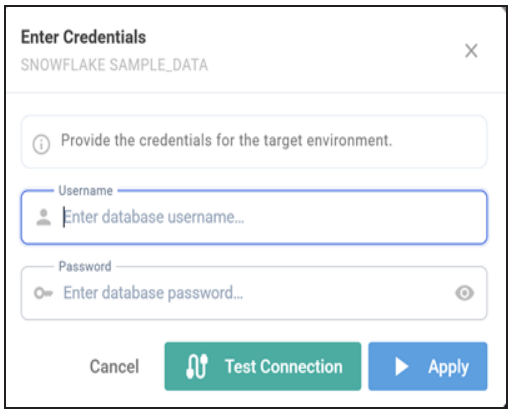
1. On the Policies tab, locate the policy to be enforced.
2. In the Actions column, click .

   The Enforce Policy pane opens.



3. Select the target environment. For example, Snowflake Sample_Data.
4. Click **Apply**.

   The Enter Credentials dialog appears.

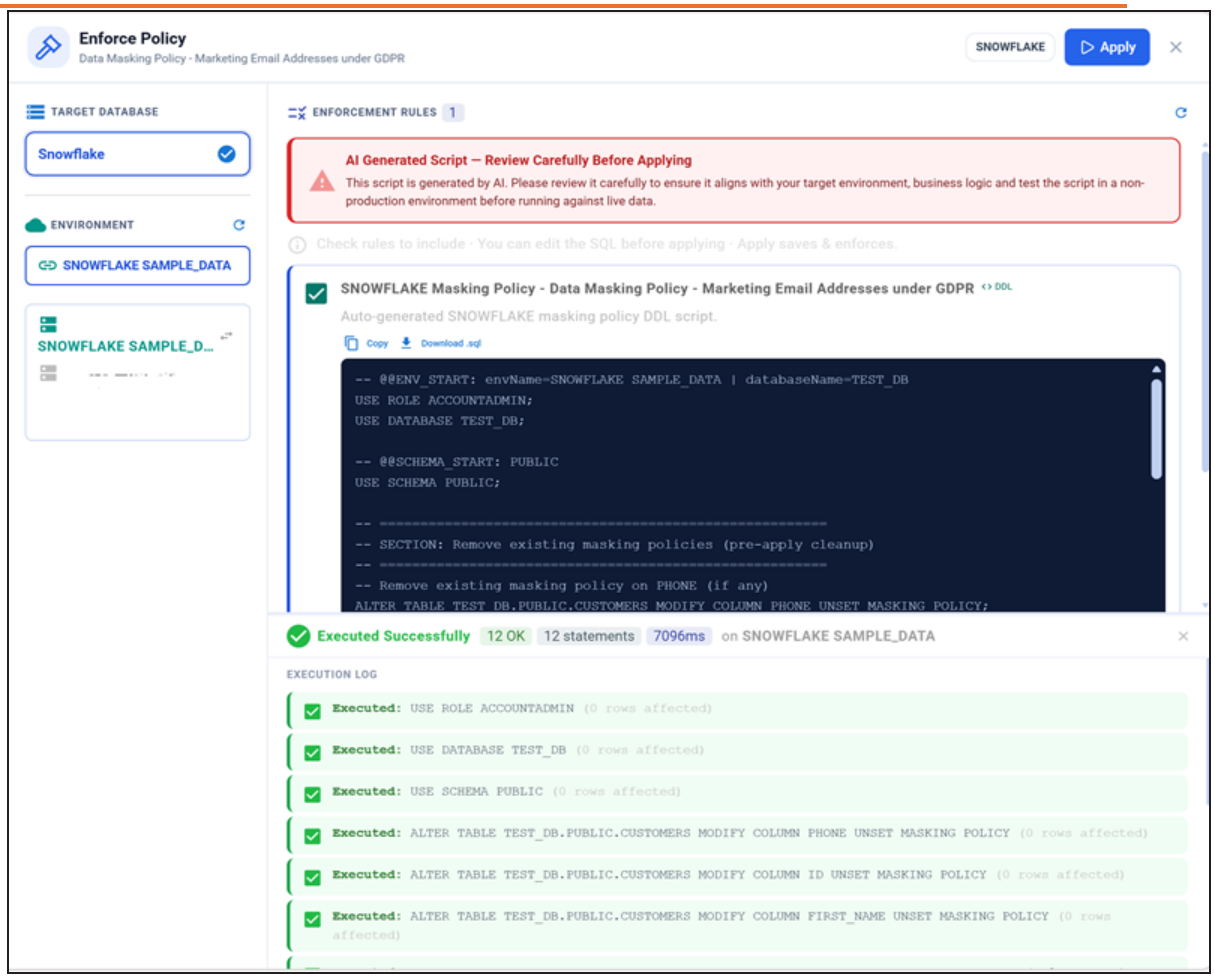


5. Confirm you have the necessary permissions and enter your database credentials.

   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.



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

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.

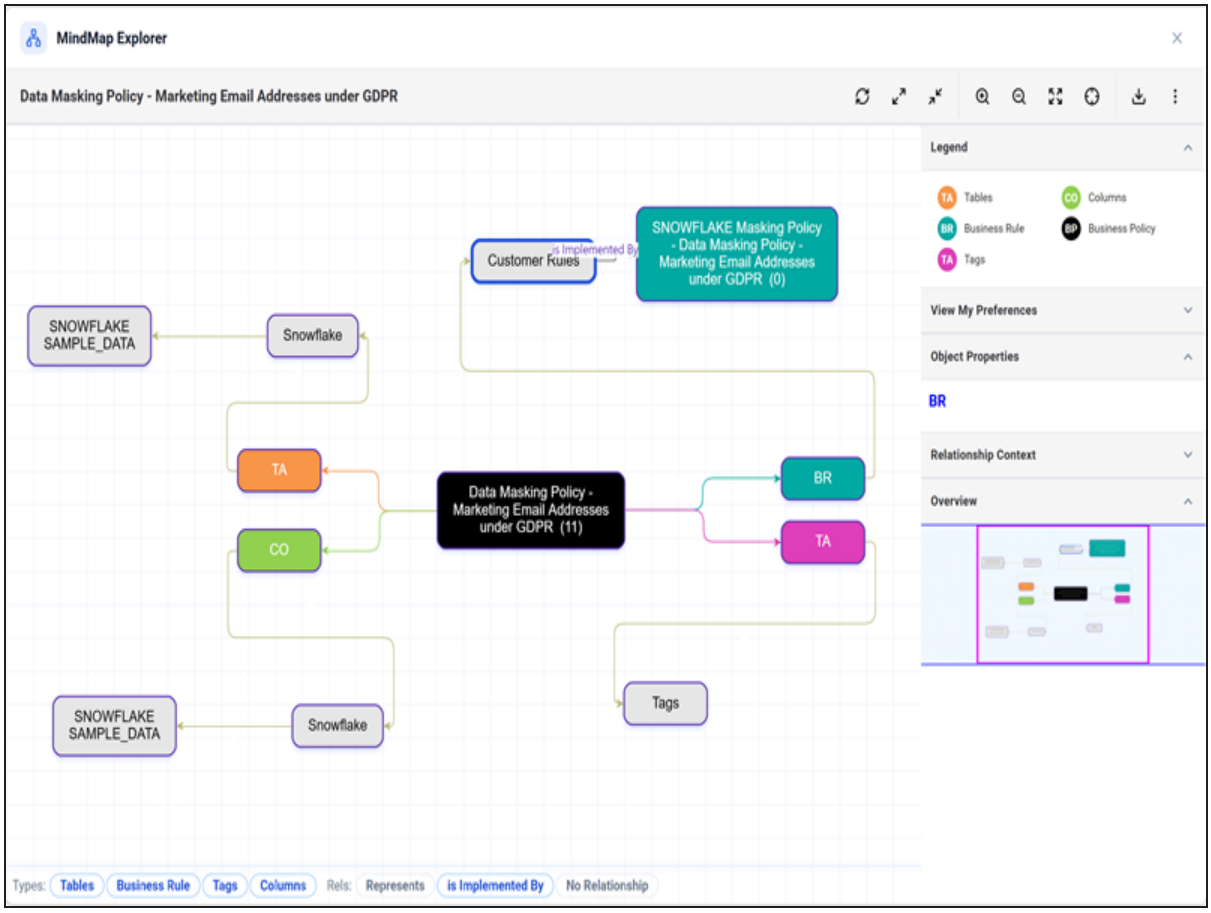
The Mind Map displays:

- 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  .

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:

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.