



Informatica® Metadata Command Center  
November 2025

# Administration

© Copyright Informatica LLC 2021, 2025

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, Informatica Cloud, Informatica Intelligent Cloud Services, PowerCenter, PowerExchange, and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

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

Publication Date: 2025-12-19

# Table of Contents

Preface. . . . .	8
<b>Chapter 1: Metadata access control. . . . .</b>	<b>9</b>
Stakeholders and roles. . . . .	9
Manage stakeholder roles. . . . .	10
Creating a stakeholder role. . . . .	11
Editing a stakeholder role. . . . .	11
Disabling a stakeholder role. . . . .	11
Attribute groups. . . . .	12
Asset groups. . . . .	12
Manage asset groups. . . . .	13
Creating and publishing an asset group. . . . .	13
Editing an asset group. . . . .	14
Access policies. . . . .	14
Manage access policies. . . . .	16
Creating and publishing an access policy. . . . .	17
Editing an access policy. . . . .	19
Disabling a metadata access policy. . . . .	19
Cloning an access policy. . . . .	20
<b>Chapter 2: Data profiling. . . . .</b>	<b>21</b>
Data profiling configuration options. . . . .	21
Monitor data profiling tasks. . . . .	25
Troubleshooting data profiling tasks. . . . .	26
<b>Chapter 3: Data quality. . . . .</b>	<b>30</b>
Data quality configuration options. . . . .	30
Monitor data quality tasks. . . . .	34
<b>Chapter 4: Data observability. . . . .</b>	<b>36</b>
Guidelines for configuring data observability. . . . .	36
Configuring data observability events. . . . .	37
<b>Chapter 5: Data classification. . . . .</b>	<b>39</b>
Types of data classification. . . . .	39
Creating a data element classification. . . . .	40
Data element classification inclusion rule. . . . .	43
Defining a constant for a data element classification rule. . . . .	44
Using reference data to define a data element classification. . . . .	46
Example: Classify a column in a table as CUSIP numbers. . . . .	47

Example: Frequent values in data classification . . . . .	47
Creating a data entity classification. . . . .	48
Updating a data classification. . . . .	49
Updating sensitivity level of multiple data element classifications. . . . .	50
Adding classification categories to multiple data classifications. . . . .	51
Cloning a data classification. . . . .	52
Deleting a data classification. . . . .	52
<b>Chapter 6: Relationship discovery.....</b>	<b>54</b>
Relationship inference model. . . . .	54
Import a relationship inference model . . . . .	55
<b>Chapter 7: Glossary association.....</b>	<b>56</b>
Configuration settings. . . . .	57
<b>Chapter 8: Lineage discovery.....</b>	<b>59</b>
Prerequisites to view CLAIRE recommendations . . . . .	59
Curate CLAIRE recommendations. . . . .	60
Accept or reject CLAIRE recommendations. . . . .	60
Resolve conflicts. . . . .	61
<b>Chapter 9: Lookup tables.....</b>	<b>63</b>
Importing and publishing a lookup table. . . . .	64
Example: Use a lookup table in a data classification expression. . . . .	66
Example: Use the data in a lookup table for glossary association. . . . .	66
Editing a lookup table. . . . .	67
Exporting a lookup table. . . . .	68
<b>Chapter 10: Connections.....</b>	<b>69</b>
Connection assignment overview. . . . .	69
Assigning connections. . . . .	70
Unassigning connections. . . . .	72
Modifying assigned connections. . . . .	72
Export lists of matched and unmatched objects. . . . .	73
Rerunning connections. . . . .	73
Types of connection scans. . . . .	74
<b>Chapter 11: Link catalog sources to generate lineage.....</b>	<b>76</b>
Prerequisites to link catalog sources. . . . .	77
Linking catalog sources. . . . .	77
Step 1. Register general information. . . . .	77
Step 2. Configure source and target catalog sources. . . . .	78
Step 3. Perform rule-based or automated linking, save, and run the configuration. . . . .	81



Manage configurations. . . . .	84
Delete or purge a configuration. . . . .	84
Clone a configuration. . . . .	85
Monitor lineage generation jobs. . . . .	85
<b>Chapter 12: Asset customization. . . . .</b>	<b>87</b>
Manage attributes. . . . .	87
Creating attributes. . . . .	88
Modifying attributes. . . . .	90
Configuring dropdown values. . . . .	91
View asset types for attributes. . . . .	93
Configuring asset types for attributes. . . . .	93
Deleting attributes. . . . .	95
Customize relationship types. . . . .	96
Modifying relationship types. . . . .	96
Define evaluation metrics. . . . .	98
Creating evaluation metrics. . . . .	98
Modifying evaluation metrics. . . . .	100
Deleting evaluation metrics. . . . .	101
<b>Chapter 13: Custom layouts. . . . .</b>	<b>102</b>
Custom layout for asset pages. . . . .	102
Creating a custom layout for an asset page. . . . .	103
Modifying, cloning and deleting a custom layout for an asset page. . . . .	108
Custom layout for preview panes. . . . .	109
Creating a custom layout for a preview pane. . . . .	110
Modifying, cloning and deleting a custom layout for a preview pane. . . . .	114
Custom layouts for the Browse page . . . . .	115
Creating a custom layout for the Browse page. . . . .	115
Modifying, cloning and deleting a custom layout for the Browse page. . . . .	116
Setting the default layout for an asset type. . . . .	117
<b>Chapter 14: Prefix values for asset reference IDs. . . . .</b>	<b>119</b>
Configuring a prefix value. . . . .	119
Rules for creating prefixes. . . . .	119
<b>Chapter 15: Workflows. . . . .</b>	<b>121</b>
Privileges for workflows. . . . .	122
Minimum privileges to design workflows in Metadata Command Center. . . . .	122
Minimum privileges to manage workflows and event configurations in Metadata Command Center. . . . .	123
Minimum privileges to select and view workflows in Metadata Command Center. . . . .	123
Minimum privileges to create workflow tickets in Data Governance and Catalog. . . . .	123

Minimum privileges to work with workflow tickets in Data Governance and Catalog. . . . .	124
Minimum privileges to view all tasks in Data Governance and Catalog. . . . .	124
Minimum privileges to assign or reassign a task in Data Governance and Catalog. . . . .	124
Minimum privileges to cancel open workflow tickets in Data Governance and Catalog. . . . .	125
Predefined workflows. . . . .	125
Workflow components. . . . .	125
Configuring a workflow. . . . .	126
Configuring workflow details. . . . .	126
Designing a workflow. . . . .	127
Validating and publishing a workflow. . . . .	130
Configuring a workflow event. . . . .	131
Configuring event properties. . . . .	131
Choosing a published workflow. . . . .	133
Configuring workflow components. . . . .	133
Saving and enabling a workflow event. . . . .	138
Manage workflows. . . . .	138
Editing a workflow. . . . .	139
Cloning a workflow. . . . .	139
Viewing dependent events of a workflow. . . . .	140
Changing a workflow lifecycle to obsolete. . . . .	140
Manage workflow events. . . . .	140
Editing a workflow event. . . . .	141
Enabling or disabling a workflow event. . . . .	141
Deleting a workflow event. . . . .	141
<b>Chapter 16: IDMC metadata. . . . .</b>	<b>143</b>
Synchronized metadata. . . . .	144
Prerequisites. . . . .	144
Configuring IDMC metadata. . . . .	146
Configure run-time metadata synchronization intervals. . . . .	147
Disabling IDMC metadata. . . . .	148
Monitor IDMC metadata jobs. . . . .	149
Connect to reference source systems. . . . .	150
Updating synchronized metadata in the catalog. . . . .	153
Viewing assets. . . . .	154
View lineage for mappings. . . . .	154
<b>Chapter 17: Notifications. . . . .</b>	<b>156</b>
Configuring data quality notifications. . . . .	156
<b>Chapter 18: Usage analytics. . . . .</b>	<b>158</b>
Configuring usage analytics. . . . .	158
Privileges for usage analytics dashboards. . . . .	159

Usage analytics dashboards. . . . .	159
<b>Chapter 19: Jobs.....</b>	<b>161</b>
Monitor jobs for technical assets. . . . .	162
Monitor the bulk import of business assets. . . . .	166
Monitor data access jobs. . . . .	168
<b>Chapter 20: Upgrade an organization to the latest version.....</b>	<b>172</b>
<b>Chapter 21: Informatica Resources.....</b>	<b>173</b>
Informatica Intelligent Cloud Services web site. . . . .	173
Informatica Intelligent Cloud Services Communities. . . . .	173
Informatica Intelligent Cloud Services Trust Center. . . . .	173
Informatica Product Availability Matrices. . . . .	174
Informatica Documentation. . . . .	174
Informatica Knowledge Base. . . . .	174
Informatica Global Customer Support. . . . .	174

# Preface

Read *Administration* to learn about the various capabilities such as data profiling, data quality, data classification, relationship discovery, and glossary association that you can perform on the extracted metadata in Metadata Command Center. You can also learn how to create and manage custom attributes for assets, configure workflows to create and modify assets, assign and unassign connections to catalog sources, monitor jobs, and configure notifications.

# CHAPTER 1

## Metadata access control

Metadata access control allows you to manage how users interact with assets. Metadata access control uses access policies to control the level of access that users have on assets. You can restrict access and selectively assign access on specific assets to users through access policies.

Create and publish access policies to control the visibility of assets or specific attributes on an asset and define permissions that a user can have on assets and features.

Before you create an access policy, you need to create users and assign them to user roles and user groups. Also, create asset groups and stakeholder roles.

To create access policies and to understand how to implement access control, you need to understand how to work with roles and the various objects that you create and use in an access policy.

Metadata access control includes the following concepts:

- [“Stakeholders and roles” on page 9](#)
- [“Attribute groups” on page 12](#)
- [“Asset groups” on page 12](#)
- [“Access policies” on page 14](#)

## Stakeholders and roles

Stakeholders are users or user groups that have access to assets in an organization. A role is a set of privileges that you can assign to users and user groups. When the organization administrator creates roles and sets the correct permissions and privileges, the roles define the boundaries within which the users can act. Roles are categorized into user roles and stakeholder roles.

### Stakeholders

You associate assets with stakeholders in Data Governance and Catalog. The associated users and user groups appear in the list of stakeholders on the **Stakeholders** tab. If a user or user group associated with an asset is deleted, the page indicates that the user or user group is deleted. You can view the assets associated with a user or user group on the **Users** tab on the **Access Control** page. To view the list of associated access policies or assets, select a user or user group and click **Show Policies** or **Show Assets** from the Actions menu.

### User roles

A user role defines the permissions and privileges for different types of assets and features. Organization administrators can create and assign user roles for the organization in Administrator. You can assign a user role to the users or user groups in your organization.

You can view access policies associated with user roles on the **Users** tab on the **Access Control** page. To view the list of associated access policies, select the user role and click **Show Policies** from the Actions menu.

For more information about creating user roles and assigning them to users and user groups, see *User Administration* in Administrator.

### Stakeholder roles

A stakeholder role is a defined organizational responsibility that you declare on assets in Metadata Command Center. You create stakeholder roles from user roles. A user with a stakeholder role can have granular access to assets based on the access policies that you configure.

Stakeholder roles allow you to control how authorized users interact with the assets for which they are responsible. A stakeholder role reflects a user's responsibilities as a stakeholder of an asset and allows them to perform governance activities with only the permissions and privileges necessary to perform their tasks.

You can view the access policies or assets associated with a stakeholder role on the **Users** tab on the **Access Control** page. To view the list of associated access policies or assets, select the stakeholder role and click **Show Policies** or **Show Assets** from the Actions menu.

The following image shows the **Stakeholder Roles** tab with a list of stakeholder roles:

Name	Asset Types	Description	Last Updated
temp_role	Technical Asset, Business Asset	Role for managing assets in Dat...	Nov 19, 2024, 6:38 PM
Data Marketplace Data Collectio...	Marketplace Asset	The Data Owner of a data collec...	Nov 19, 2024, 12:35 AM
Governance Owner	Business Asset, Technical Asset	Role for managing assets in Dat...	Nov 19, 2024, 12:35 AM
Data Marketplace Delivery Tem...	Marketplace Asset	The Delivery Owner of a delivery...	Nov 19, 2024, 12:35 AM
Data Marketplace Data Collectio...	Marketplace Asset	The Technical Owner of a data c...	Nov 19, 2024, 12:35 AM
Governance Administrator	Business Asset, Technical Asset	Governance Administrator role f...	Nov 19, 2024, 12:35 AM
Data Marketplace Category Ow...	Marketplace Asset	The Category Owner of a catego...	Nov 19, 2024, 12:35 AM
ST_Engg	Technical Asset	Governance User role for Data G...	Nov 14, 2024, 5:27 AM
Staf_test	Technical Asset, Marketplace A...	Governance Administrator role f...	Nov 14, 2024, 5:25 AM
ZZ Business Asset Manager	Business Asset		Oct 24, 2024, 12:30 AM
Customer 360 Manager	Marketplace Asset, Technical A...	MDM Customer 360 Manager	Oct 23, 2024, 7:02 AM

## Manage stakeholder roles

You can create, modify, or disable stakeholder roles on the **Stakeholder Roles** tab.

You can associate stakeholder roles with asset types and a user role and view access policies and assets associated with a stakeholder role on the **Stakeholder Roles** tab. You cannot delete a stakeholder role that you create.

You can select users assigned the stakeholder role when you assign stakeholders to assets. The stakeholder role replaces the stakeholdership privilege in Data Governance and Catalog.

If the user role corresponding to the stakeholder role is deleted in Administrator, a warning icon appears, and you need to disable the stakeholder role.

## Creating a stakeholder role

Create a stakeholder role to grant granular access to stakeholders who are responsible for certain assets.

You can't delete a stakeholder role that you create.

1. On the **Access Control** page, select the **Users** tab.
2. Click the **Stakeholder Roles** tab, and then click **Add**.  
The **New Stakeholder Role** dialog appears.
3. Select the user role from which you want to create the stakeholder role.
4. Select the asset types to associate with the stakeholder role.
5. Click **Create**.

The stakeholder role is created and enabled.

## Editing a stakeholder role

You can modify the asset types that you add to a stakeholder role that you create.

1. On the **Access Control** page, click **Users**.
2. Click the **Stakeholder Roles** tab and select the stakeholder role that you want to modify.
3. From the Actions menu, click **Edit**.
4. Select the asset types that you want to add or remove.
5. Click **Update**.

## Disabling a stakeholder role

Disable a stakeholder role if the user role associated with the stakeholder role is deleted. You can also disable a stakeholder role to prevent users from assigning it to assets and access policies.

1. On the **Access Control** page, click **Users**.
2. Click the **Stakeholder Roles** tab.
3. Select the stakeholder role that you want to disable.
4. From the Actions menu, click **Disable**.

To associate the role with access policies again, you can enable the disabled role. To enable a stakeholder role that you disabled, click **Enable**.

## Attribute groups

Use attribute groups to control access to asset attributes when you define access policies.

The following table describes the attribute groups that you can use:

Attribute Group	Description
Profiling	Attributes related to basic data profiling results.
Data	Attributes related to advanced data profiling results such as value frequency and min - max values.
Code	Attributes related to the programmatic definition of an asset that you can view on the <b>Code</b> tab for technical assets.
Unpublished changes	Attributes related to assets that are not published during an approval workflow process.

## Asset groups

You can use asset groups to control access to a set of assets. By grouping assets, you can use user group policies to grant or restrict access to multiple assets at a time.

For the access policies associated with asset groups to take effect, assign the asset groups to specific assets in Data Governance and Catalog or associate asset groups with assets when you run a catalog source job in Metadata Command Center. After you publish a user group policy that includes asset groups, you can use the access policy to control the access level on assets that are associated with the asset group.

When you create an asset group, you can create a hierarchy of up to four levels by selecting a parent asset group.



The following image shows the **Asset Groups** tab on the **Customize** page with a list of hierarchical asset groups in Metadata Command Center:

The screenshot shows the 'Customize' page with the 'Asset Groups' tab selected. The table lists 25 asset groups, including Finance, Global, Americas, and Asia, with columns for Name, Description, Updated On, Updated By, and Lifecycle.

<input type="checkbox"/>	Name	Description	Updated On	Updated By	Lifecycle
<input type="checkbox"/>	▼ Finance		Oct 21, 2024, 8:33 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	Finance France		Oct 21, 2024, 9:32 AM	ADELE ADMIN	PUBLISHED ⓘ
<input type="checkbox"/>	Finance UK		Oct 21, 2024, 9:32 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	Finance US		Oct 21, 2024, 9:32 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	▼ Global		Oct 21, 2024, 9:34 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	▼ Americas		Oct 21, 2024, 9:36 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	Brazil		Oct 21, 2024, 9:40 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	Canada		Oct 21, 2024, 9:40 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	USA		Oct 21, 2024, 9:40 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	▼ Asia		Oct 21, 2024, 9:36 AM	ADELE ADMIN	PUBLISHED
<input type="checkbox"/>	India		Oct 21, 2024, 9:40 AM	ADELE ADMIN	PUBLISHED

## Manage asset groups

You can create, modify, publish, and delete asset groups.

You can manage asset groups on the **Asset Groups** tab on the **Customize** page. After you publish an asset group, you can associate access policies and assets with the asset group.

You can't delete parent asset groups that are associated with child asset groups. Also, you can't delete asset groups that are associated with assets or access policies. Remove the associated child asset groups, access policies, or assets before you delete the asset group.

### Required privileges for the user role

To view asset groups, the administrator needs to enable the View Asset Groups feature privilege for Metadata Command Center. Additionally, to view, create, update, and delete asset groups, you need the Manage Asset Groups feature privilege.

## Creating and publishing an asset group

Create asset groups to group related assets and control access to multiple assets as a group.

1. On the **Customize** page, select the **Asset Groups** tab.
2. Click **Add**.

Alternatively, on the navigation panel, click **New > Customization > Asset Group > Create**.

3. Configure the following properties:

Property	Description
Name	A name to identify the asset group.
Description	Optional. A description of the asset group.
Parent	Optional. The parent asset group with which you want to associate the asset group. The parent asset group can be a part of a hierarchy. Select an asset group from the list.

4. Click **Save**.
5. To publish the asset group, click **Publish** or to discard the draft, click **Discard**.

## Editing an asset group

You can update the name and description of an asset group.

1. On the **Customize** page, select the **Asset Groups** tab.
2. Select the asset group that you want to modify.
3. From the Actions menu, click **Edit**.
4. Update the name and description of the asset group as needed.

**Note:** You can't update the parent asset group.

5. Click **Save**.
6. To publish the asset group, click **Publish**.

## Access policies

Access policies are sets of rules that you use to define permissions and control the level of access to organizational assets.

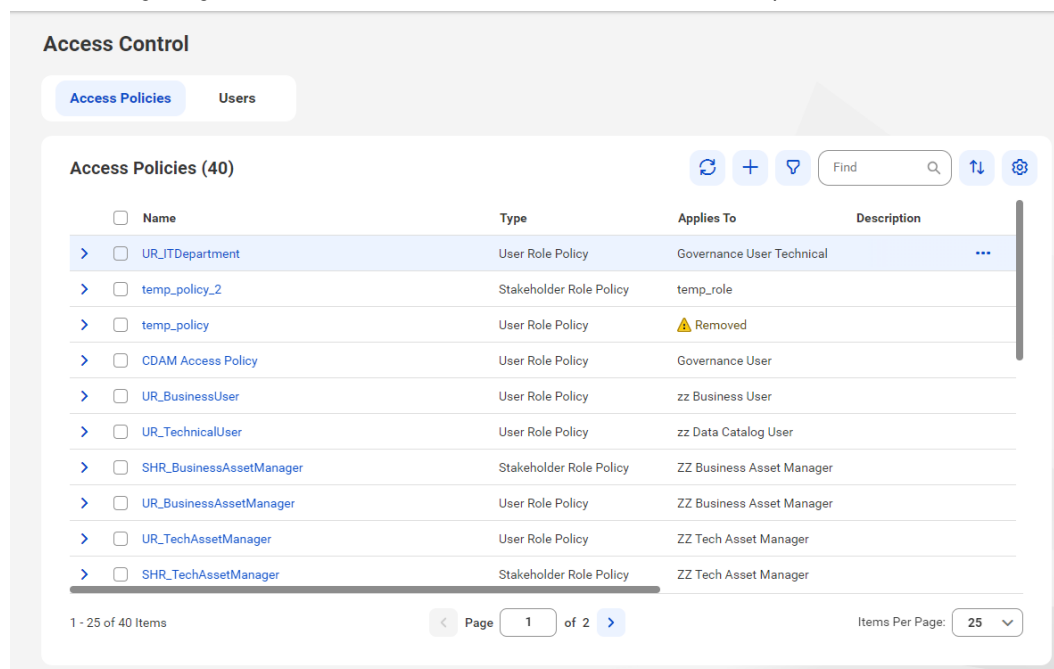
To implement access control, you can use predefined access policies or define access policies in Metadata Command Center. Predefined access policies are associated with predefined user roles defined in Administrator. For information about predefined access policies, see *Introduction and Getting Started*.

To define access policies, you create rules that provide specific permissions and privileges to users or user groups on asset types or attribute groups. The access policies control the level of access that users have based on the assigned user role, stakeholder role, or the user group.

The following table describes the access policies that you can create in Metadata Command Center:

Access policy	Description
User role policy	Defines the access level of users who are assigned a user role in Administrator.
Stakeholder role policy	Defines the access level of users who are assigned a stakeholder role on assets. For information about how to create a stakeholder role, see <a href="#">"Creating a stakeholder role" on page 11</a> .
User group policy	Defines the access level of users who are added to a user group in Administrator. You can also use this access policy to control the access level of all users in the organization.

The following image shows the **Access Policies** tab with a list of access policies:



## Effective permissions granted by access policies

Users inherit the intersection of the permissions granted by all access policies assigned to them.

For example, if a user is assigned the following access policies, then only the intersection of those permissions are granted to the user on the asset:

- User role policy for the Governance Owner
- Stakeholder role policy for the Governance Owner
- User group policy for the Finance user group

When you create a user role or stakeholder role policy and override other access policy types, then this access policy provides access regardless of other access policies that might apply.

You can use user role policies or user group policies to control permissions based on asset groups. The access to asset groups is enforced when at least one access policy grants permission on an asset group.

## Permissions to work with catalog sources

To work with catalog sources, the administrator needs to configure asset privileges for the user role in Administrator. Before you create, update, delete, purge, and run a catalog source, verify that the administrator

granted the required permissions for your user role in the Catalog Source Configuration asset privilege for Metadata Command Center.

The administrator also needs to configure an access policy with the required permissions in Metadata Command Center.

The following table describes the permissions required to create, view, update, purge, copy, and run a catalog source:

Action	User role permissions	Access policy permissions
Create a catalog source	Create, Read, Update	Create, Read Grant the Read permissions to the user role on the connections. This applies to all types of connections, such as staging, flat file, and source connections.
View the catalog source configuration	Read	Read
Update a catalog source	Read, Update	Update
Purge and delete a catalog source	Read, Delete	Delete
Copy a catalog source	Create, Read, Update	Create, Read
Run a catalog source	-	For a catalog source that does not have connection assignments, grant the Read permission to the user role policy.  For a catalog source that has connection assignments, grant the Read and Update permissions to the user role and stakeholder role policies on the reference and endpoint datasources.

## Manage access policies

You can create, modify, clone, disable, or delete access policies.

When you disable or delete an access policy, the rules defined in the access policy do not apply. You cannot delete predefined access policies, but you can disable or clone them.

You can manage access policies on the **Access Policies** tab on the **Access Control** page.

To search for access policies, you can use filters. To show or hide the **Category** and **Updated By** columns on the **Access Policies** tab, right-click any column header and select the column name.

### Required privileges for the user role

To view access policies, the administrator needs to enable the View Access Control feature privilege for Metadata Command Center. Additionally, to create, view, update, and delete access policies, you need the Manage Access Control feature privilege.

## Creating and publishing an access policy

To create an access policy, specify the name and description and associate the access policy with a stakeholder role, user group, or user role. Define one or more rules for the access policy that determine the level of access to assets, and then publish the access policy.

1. Go to **Access Control** and click **Access Policies**.
2. Click **Add**, and then select the type of access policy that you want to create.

Alternatively, on the navigation panel, click **New > Access Control**, select the type of access policy, and then click **Create**.

The **New Access Policy** page opens on the **Overview** tab. The properties that appear depend on the type of access policy you select.

3. Enter the general information applicable to your access policy type.

User role policy

Property	Description
Name	A name to identify the access policy.
Description	Optional. A description of the access policy.
User Role	Select the user role that you want the access policy to apply to.
Override other policy types	Optional. From <b>Advanced Settings</b> , choose to override other access policy types if multiple access policies are enabled.

Stakeholder role policy

Property	Description
Name	A name to identify the access policy.
Description	Optional. A description of the access policy.
Selected Role	<p>Specify if you want the stakeholder role policy to apply to users with specific stakeholder roles or to users who are non-stakeholders.</p> <p>Choose from the following options:</p> <ul style="list-style-type: none"><li>- Stakeholder. Select Stakeholder to specify a stakeholder role.</li><li>- Non-Stakeholder. Select Non-Stakeholder to specify if you want the access policy to apply to both non-stakeholders and users with stakeholder roles.</li></ul>
Stakeholder Role	Required if you choose Stakeholder as the selected role. Select the stakeholder role that you want the access policy to apply to.
Override other policy types	Optional. From <b>Advanced Settings</b> , choose to override other access policy types if multiple access policies are enabled.

## User group policy

Property	Description
Name	A name to identify the access policy.
Description	Optional. A description of the access policy.
Selected Group	Specify if you want the user group policy to apply to a specific user group or to all users. Choose from the following options: <ul style="list-style-type: none"><li>- Single User Group. Select Single User Group to specify a user group</li><li>- All Users. Select All Users if you want the access policy to apply to all users.</li></ul>
User Group	Required if you choose Single User Group. Select the user group that you want the access policy to apply to.

4. Click **Next**.
5. Add one or more rules to define the access policy.  
You can create rules based on asset types or attribute groups.
  - Create a rule based on asset types. For information about how to create rules based on asset types, see [“Creating rules based on asset types” on page 18](#).
  - Create a rule based on attribute groups. For information about how to create rules based on attribute groups, see [“Creating rules based on attribute groups” on page 19](#).
6. Click **Save**.
7. To publish the policy, click **Publish** to start the publishing job.  
To discard the policy, click **Discard**.

## Creating rules based on asset types

You can create rules to define an access policy based on asset types.

1. On the **Rules** tab, click **Add**.  
The **Condition** page appears.
2. Click **Add**.
3. Select **Asset Type**.
4. For user role and stakeholder role policies, perform the following steps:
  - a. Click **Add New** to select one or more asset types from the hierarchy and click **OK**.
  - b. Optional. Add one or more predicates to the condition.
5. For a user group policy, add one of the following conditions based on your requirements:
  - To apply the condition to specific asset groups, choose **Is Any Of > Add New**. In the **Select Asset Groups** window, select one or more asset groups from the hierarchy and click **OK**.
  - To apply the condition to assets that are not associated with asset groups, choose **Is Null**.
6. Click **Add Permission** to grant permissions to users governed by the access policy.  
**Note:** The list of available permissions is based on the asset type and the predicate that you selected.
7. Click **Save**.
8. To create another rule, click **Add** or to edit an existing rule, click **Edit**.

## Creating rules based on attribute groups

You can create rules to define an access policy based on attribute groups.

1. On the **Rules** tab, click **Add**.  
The **Condition** page appears.
2. Click **Add**.
3. Select **Attribute Groups**.
4. For user role and stakeholder role policies, perform the following steps:
  - a. Click **Add New** and choose an attribute group.
  - b. Add one of the following conditions based on your requirements:
    - To add a condition that applies to any asset type, choose **Is Any**.
    - To add a condition that applies to specific asset types, choose **Is Any Of > Add New**. In the **Select Asset Type** window, select one or more asset types from the hierarchy and click **OK**.
  - c. Optional. Add one or more predicates to the condition.
  - d. Select the permissions to grant users governed by the access policy.
5. For a user group policy, perform the following steps:
  - a. Click **Add New** and choose an attribute group.
  - b. Add one of the following conditions based on your requirements:
    - To add a condition that applies to specific asset groups, choose **Is Any Of > Add New**. In the **Select Asset Groups** window, select the asset groups from the hierarchy and click **OK**.
    - To add a condition that applies to assets that are not associated with asset groups, choose **Is Null**.
  - c. Select the permissions to grant users governed by the access policy.
6. Click **Save**.
7. To create another rule, click **Add** or to edit an existing rule, click **Edit**.

## Editing an access policy

You can edit an access policy that you created and change the name, description, and other properties.

1. On the **Access Control** page, click **Access Policies**.
2. Select the access policy that you want to modify.
3. From the Actions menu, click **Edit**.
4. Modify the required properties and click **Save**.  
A draft access policy is created.
5. To publish the updated access policy, click **Publish**.
6. To enable the access policy, click **Enable**.

## Disabling a metadata access policy

Disabling an access policy removes it from all users that are associated with it.

1. On the **Access Control** page, click **Access Policies**.
2. Select the access policy that you want to disable.

3. From the Actions menu, click **Disable**.

A confirmation box appears.

4. Click **Disable**.

You can enable the access policy to associate it with users again. To enable an access policy that you disabled, click **Enable**.

## Cloning an access policy

Clone an access policy to create an access policy that is similar to the existing access policy. You cannot edit a predefined access policy, but you can clone the access policy and update it.

1. On the **Access Control** page, click **Access Policies**.
2. Select the access policy that you want to clone.
3. From the Actions menu, click **Clone**.
4. Modify the name and description and click **Create**.  
**Note:** You cannot change the policy type for a user group policy.
5. Click **Create**.
6. Update the policy as needed and click **Save**.
7. To publish the policy, click **Publish** to start the publishing job.  
To discard the policy, click **Discard**.



## CHAPTER 2

# Data profiling

Enable the data profiling capability to evaluate the quality of the metadata extracted from source systems. The data profiling process assesses the source metadata and views the collected column data statistics to discover content and structure, such as value distribution, patterns, and data types. These statistics can help your organization determine the suitability of the data to solve the business problem.

When you create a catalog source, select the **Data Profiling** option on the **Configuration** wizard to enable data profiling for the catalog source. Set the data profiling configuration options and run the catalog source job to monitor the status of the data profiling task and view the task results on the job overview page. You can view the detailed profiling statistics for the extracted metadata in Data Governance and Catalog when you open the catalog source asset. For more information about viewing profiling statistics extracted from source systems, see the *Asset Details* module in the *Cloud Data Governance and Catalog* help.

## Data profiling configuration options

Based on your requirements, configure the options to determine the type of data that you want the data profiling task to collect, the scope of the profile run, and the sample rows on which you want to run the data profiling task.

After you enable **Data Profiling** on the **Configuration** wizard while creating a catalog source, you can configure the following options on the **Data Profiling** tab:

### Profile filters

You can use filter conditions to reduce the scope of a data profiling task. The profile filters help you create subsets of metadata that you can use to run a data profiling task on a catalog source. For example, you choose to extract metadata from six schemas, but want to run a profiling task on three of the schemas.

You can add multiple filter conditions for each catalog source. Any user with the create, edit, or run catalog source permissions can configure the profile filters. You can apply filters on all relational and file system catalog sources that support profiling capabilities.

The profile filters depend on the filters you apply for metadata extraction. For example, your source includes a schema named `Cust_Emp` with tables such as `Customer1`, `Customer2`, `Employee1`, and `Employee2`. You have applied a metadata extraction filter to include metadata from `Customer1`, `Customer2`, and `Employee1` tables from the schema. Now, when you apply a profile filter, you can only consider `Customer1`, `Customer2`, and `Employee1` tables to run profiles.

The following are types of profile filters:

- **Include Metadata.** Runs a profile on the metadata extracted from the values that you specify in the filter condition.

- **Exclude Metadata.** Does not run a profile on the metadata extracted from the values that you specify in the filter condition.

#### Profile filter examples for relational catalog sources

- The following profile filter runs profiles on the metadata extracted from the `Asia_Pacific` table located in the `Customers` schema of an Oracle source system:

Include Metadata

Schema

Named

Customers.Asia\_Pacific x

Select

- The following profile filter does not run profiles on the metadata extracted from the `Finance` table located in the `EMPLOYEE` schema of an Oracle source system:

Exclude Metadata

Schema

Named

EMPLOYEE.Finance x

Select

- The following profile filter runs profiles on the metadata extracted from the external tables object type using an asterisk wildcard for an Amazon Athena source system:

Include Metadata

External Tables

\*

+

- The following profile filter does not run profiles on the metadata extracted from the external tables object type using an asterisk wildcard for an Amazon Athena source system:

Exclude Metadata

External Tables

\*

+

#### Profile filter examples for file system catalog sources

- The following profile filter runs profiles on the metadata extracted from the `JAN2023` folder:

Include Metadata

Folder

Named

JAN2023 x

Select

- The following profile filter does not run profiles on the metadata extracted from the `CUSTOMER.CSV` file:

Exclude Metadata

File

Named

CUSTOMER.CSV x

Select

## Runtime environment

Select a runtime environment in which you can run data profiling tasks on a Secure Agent. If you don't select a runtime environment, the data profiling task runs in the runtime environment that your organization administrator selected when they created the connection.

**Note:** You can run data profiling and data quality tasks on a Windows Secure Agent configured with NTLMv2 proxy authentication.

## Mode of run

To determine the type of data you want the data profiling task to collect, choose **Keep Signatures Only** or **Keep Signatures and Values**. If you choose **Keep Signatures Only**, the data profiling task collects only aggregate information such as data types, average, standard deviation and patterns. No data values are collected. If you want the data profiling task to collect both signatures and data values, then choose **Keep Signatures and Values**. Data values include minimum value, maximum value, frequent values and more.

## Profile run scope

Determine whether you want to run data profiling only on the changes made to the source system or on the entire source system. Choose one of the following options:

- **Full.** Run data profiling on the entire metadata that is extracted based on the filters applied for extraction.
- **Incremental.** Run the profile only on the changed or updated metadata in the source system.

When you enable incremental profiling for a catalog source and run data profiling for the first time, the data profiling capability profiles the entire metadata based on the filters applied for metadata extraction. Subsequently, incremental profiling discovers any change to the metadata when the metadata extraction capability is enabled and runs profiling only on those changes. For example, if you rename a column after the first run and enable incremental profiling in the subsequent run, only the table containing the renamed column is profiled.

Incremental profiling discovers the following changes to the metadata during the data profiling run:

- Adding a new object
- Renaming a column
- Objects that were not profiled in the previous run because of data profiling task failure or change in the metadata extraction filter.

## Connection

Select the SAP Table connection to run data profiling tasks on SAP ERP objects.

## Sampling type

Determine the sample rows on which you want to run the data profiling task. The sampling options vary based on the catalog source that you create. Choose one of the following options:

- **All Rows.** Runs the profile on all rows in the metadata.
- **Limit N Rows.** Runs the profile on a limited number of rows. You can specify the limited number of rows to run the profile on.
- **Random N Rows.** Runs the profile on the selected number of random rows.
- **Random N Percentage.** Run the profile on select rows based on the percentage of data that you specify in the **Percentage of Data to Sample** field. Google BigQuery tables are organized as data blocks. For example, you can specify 5 percentage of data blocks from a table to run the profile on.
- **Custom Query.** Provide a custom SQL clause to select sample rows to run the data profiling task. In the **Sampling Query** field, enter the custom SQL clause to choose sample rows on which you want to run the data profiling task. Verify that the syntax of the SQL clause matches the syntax of the database that you are connecting to.

Examples:

- If you're using the JDBC catalog source to connect to IBM DB2 and the sampling query is `FETCH FIRST 50 ROWS ONLY`, then the query runs the profile only on the first 50 rows.
- If you enter `employeeName like '%a%'` for a Salesforce catalog source, then the query selects rows that contain 'a' in the column `employeeName`.

**Note:** For the Salesforce catalog source, you cannot use the `LIMIT` clause in a sampling query. For example, you cannot use `Name like '%a%' LIMIT 10`.

## Elastic runtime environment

Select a runtime environment in which you can run data profiling tasks on an advanced cluster. Select an elastic runtime environment for complex file types, including AVRO and Parquet.

**Note:** This option is available when you configure data profiling for Amazon S3, Google Cloud Storage, and Microsoft Azure Data Lake Storage Gen2 catalog sources.

To run a profile on an Avro or Parquet file, connect to the following types of advanced cluster in your organization:

- **Fully-managed cluster.** A multi-node serverless infrastructure that intelligently scales based on your workload and offers the lowest total cost of ownership for your organization. For more information, see [Fully-managed clusters](#).
- **Local cluster.** A single-node cluster that you can start on the Secure Agent machine. You can use a local cluster to quickly onboard projects for advanced use cases. For more information, see [Local clusters](#).

For more information about setting up AWS, Google Cloud, and Microsoft Azure for local and fully-managed clusters, see [Advanced clusters](#) in the Administrator documentation.

### Staging connection

Applicable only for elastic profile executions, that is, for Parquet and Avro sources located in Amazon S3, Microsoft Azure Data Lake Storage Gen2, and Google Cloud Storage source systems.

The staging connection where profiling results are temporarily stored while the job runs.

### Maximum precision of string fields

The maximum precision value for profiles on string data type. Enter a value between 1 and 255. Default value is 50.

### Text qualifier

The character that defines string boundaries. If you select a quote character, the profile ignores delimiters within the quotes. Select a qualifier from the list. Default is Double Quote.

### Code page for delimited files

Select a code page that the Secure Agent can use to read and write data. Use this option to ensure that profile results for assets with non-English characters don't include junk characters. Default value is UTF-8.

Choose one of the following options:

- MS Windows Latin 1. Select for ISO 8859-1 Western European characters.
- UTF-8. Select for Unicode and non-Unicode characters.
- Shift-JIS. Select for double-byte characters.
- ISO 8859-15 Latin 9 (Western European).
- ISO 8859-2 Eastern European.
- ISO 8859-3 Southeast European.
- ISO 8859-5 Cyrillic.
- ISO 8859-9 Latin 5 (Turkish).
- IBM EBCDIC International Latin-1.

**Note:** This option is available when you configure data profiling for the following catalog sources:

- Amazon S3
- Google Cloud Storage
- Microsoft Azure Data Lake Storage Gen2

## Escape character for delimited files

You can specify an escape character if you need to override the default escape character. An escape character ignores a delimiter character in an unquoted string if the delimiter is part of the string value.

If you specify an escape character, the data profiling task overrides the default escape character that the Metadata Extraction job detects and considers the specified escape character. It then reads the delimiter character as a part of the string value. If you don't specify an escape character, the data profiling task considers the default escape character that the Metadata Extraction job detects and reads the delimiter character as a part of the string value.

**Note:** This option is available when you configure data profiling for the following catalog sources:

- Amazon S3
- Google Cloud Storage
- Microsoft Azure Data Lake Storage Gen2

# Monitor data profiling tasks

On the job overview page, monitor the status of data profiling tasks and retry profiling for tasks that complete with errors.

After you run a job that includes data profiling, you can monitor the status of the data profiling task and view the results on the job overview page. The results include statistics such as the number of discovered objects, profiled objects, skipped objects, and failed objects.

Data profiling tasks create the following subtasks:

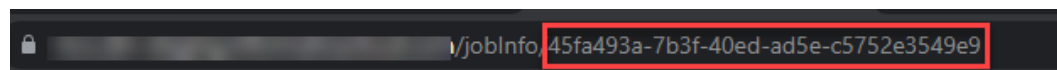
- Bulk ingestion
- Task progress tracker
- Batch profiling

If a subtask completes with errors, retry profiling for the data profiling task. To retry profiling, hover the mouse over the data profiling parent task and click the **Retry Task** icon. When you retry, the job creates a new data profiling task that includes all failed objects from the batch profiling subtasks and runs the profile again with new batch profiling subtasks.

The number of batch profiling subtasks depends on the number of objects that need to be profiled and the maximum number of objects allowed in a batch profiling subtask. The maximum number of objects in a batch profiling subtask depends on the `mps_maxDeploymentBatchSize` property of the Metadata Platform Service configured for a Secure Agent.

You can view logs for the profiled objects, tasks, and subtasks on the **Logs** tab. After the data profiling task completes, you can view the results on the **Results** tab.

You can download logs to track failed profiling tasks. Click **Failed Session Logs** to download the logs. The ZIP file name represents the catalog source job ID. The catalog source job ID helps you identify the failed profiling task. You can also find the catalog source job ID from the URL of the **Monitor** tab as shown in the following image:



Extract the ZIP file. The extracted ZIP file contains multiple ZIP files based on the number of failed batch profiling tasks. Each ZIP file includes profiling session log files.

The following image shows the job **Overview** page for a data profiling task:

**10table\_10batch\_81C\_Oracle\_sync**

STATUS: **COMPLETED** | COMPLETED TASKS: **8 / 8** | SUBMITTED TIME: Apr 12, 2023, 12:15:47 AM | START TIME: Apr 12, 2023, 12:16:25 AM | END TIME: Apr 12, 2023, 12:20:47 AM | EXECUTION DURATION: 00:04:22

Overview | Logs

Job Details

Tasks (8)

Name	Submitted Time	Start Time	End Time	Execution Duration	Status
Data Profiling	Apr 12, 2023, 12:15:47 AM	Apr 12, 2023, 12:16:25 AM	Apr 12, 2023, 12:20:48 AM	00:04:23	COMPLETED
Data Profiling Task	Apr 12, 2023, 12:16:28 AM	Apr 12, 2023, 12:16:54 AM	Apr 12, 2023, 12:20:47 AM	00:03:53	COMPLETED
Bulk Ingestion	Apr 12, 2023, 12:16:16 AM	Apr 12, 2023, 12:19:32 AM	Apr 12, 2023, 12:20:33 AM	00:01:01	COMPLETED
Task Progress Tracker	Apr 12, 2023, 12:17:01 AM	Apr 12, 2023, 12:17:01 AM	Apr 12, 2023, 12:20:47 AM	00:03:46	COMPLETED
Batch Profiling Task - 1	Apr 12, 2023, 12:17:52 AM	Apr 12, 2023, 12:18:13 AM	Apr 12, 2023, 12:18:41 AM	00:00:28	COMPLETED
Batch Profiling Task - 2	Apr 12, 2023, 12:18:02 AM	Apr 12, 2023, 12:18:12 AM	Apr 12, 2023, 12:18:39 AM	00:00:21	COMPLETED
Batch Profiling Task - 3	Apr 12, 2023, 12:18:06 AM	Apr 12, 2023, 12:18:16 AM	Apr 12, 2023, 12:18:59 AM	00:00:43	COMPLETED
Batch Profiling Task - 4	Apr 12, 2023, 12:18:32 AM	Apr 12, 2023, 12:18:42 AM	Apr 12, 2023, 12:19:02 AM	00:00:20	COMPLETED

Data Profiling Details

Properties | Results

10 TOTAL OBJECTS ASSIGNED | 10 OBJECTS PROFILED SUCCESSFULLY | 0 OBJECTS SKIPPED | 0 OBJECTS FAILED

For more information about the actions that you can perform on the job monitoring pages, see [“Monitor jobs for technical assets” on page 162](#).

## Troubleshooting data profiling tasks

A profile run fails with the following error message for flat files:

```
[INFO] [delimiter: ,][escapeChar: "][qualifier: "]

[WARNING] Malformed CSV row, continuing by ignoring it (multiple rows may have been skipped,
read RFC-4180 for CSV standards.). exception :: IOException reading next record:
java.io.IOException: (startline 2) EOF reached before encapsulated token finished
```

This issue occurs if the file contains double quotes ("), and the catalog source is configured with double quotes as the escape character.

To resolve the issue, configure the **Escape character for delimited files** parameter with a value other than double quotes and rerun the data profiling task.

Data profiling tasks don't include all files if you enable partition detection for Amazon S3, Microsoft Azure Data Lake Storage Gen2, and Google Cloud Storage catalog sources with Parquet files.

This issue occurs if a folder contains partitioned Parquet files with incremental schema.

To resolve the issue, disable partition detection and run the data profiling task.

A profile run fails with the following error message for Microsoft Azure Synapse source objects:

```
Workflow generation failed for object: <DatabaseName/SchemaName/ObjectName> with error:
Invalid datatype: int
This issue occurs when the source object includes data types such as Int, datetimeoffset, or uniqueidentifier.
```

To resolve the issue, rerun the failed task. Click **Retry Task** on the **Job Details** page to rerun the failed data profiling task.

## A profile run fails with the following error message for Amazon S3, Google Cloud Storage, or Azure Data Lake Storage Gen2 source objects:

"Failure w.r.t "java.lang.RuntimeException: No active Metadata\_Platform\_Service found for "Secure Agent ID" for mentioned combinations in description"

This issue occurs when the connection that you use to create a catalog source includes an inactive Secure Agent.

To resolve the issue, use an active Secure Agent when you create the connection or add an active Secure Agent in the elastic runtime environment field when you configure the profiling task.

## A profile run for SAP S/4 HANA source objects fails with the following error message:

"ERROR: "OPTION\_NOT\_VALID: OPTION\_NOT\_VALID Message 000 of class SAIS type E"

This issue occurs when you use an SAP Table connection from one of the following versions:

- S/4 HANA version 2021
- SAP ECC version 6.0 EHP8
- SAP NetWeaver system version 7.40 SP26

To resolve this issue, perform the following steps:

1. In the Informatica Intelligent Cloud Services Administrator, open the **Runtime Environments** page.
2. On the **Runtime Environments** page, select the Secure Agent associated with the SAP Table connection.
3. Click **Edit**.
4. In the **Custom Configuration Details** area, select **Data Integration Server** as the service and **Tomcat** as the type.
5. Enter `SapStrictSql` in the **Name** field and set the value based on the SAP system language as shown in the following image:

Custom Configuration Details

Service	Type	Sub-type	Name	Value
Data Integration Server	Tomcat		SapStrictSql	E

6. In Metadata Command Center, run the catalog source job again.

## Data profiling tasks don't include columns of Date/Time date type in the results.

The Date/Time data type handles years from 1 A.D. to 9999 A.D. in the Gregorian calendar system. Years beyond 9999 A.D. cause an error. The Date/Time data type has a precision of 29 and a scale of 9. To resolve this issue, check the precision value of the column in the source system. If it is greater than 29, reduce the precision value.

## A profile run fails with the error "\*\*\*ERROR: nsort\_release\_recs() returns -10".

To resolve this issue, increase the disk space storage of the hard drive where the Secure Agent is installed.

### Data profiling task for some catalog sources fails with the error "Internal error. The DTM process terminated unexpectedly."

This happens if the length of the column name in a table exceeds the maximum column length allowed for each source system. The following table lists the maximum column length allowed for the source systems that this issue impacts:

Source System	Maximum Column Length
<ul style="list-style-type: none"><li>- Amazon Redshift</li><li>- Amazon S3</li><li>- Google BigQuery</li><li>- Google Cloud Storage</li><li>- JDBC (IBM DB2)</li><li>- Microsoft Azure Data Lake Storage Gen2</li><li>- Microsoft Azure SQL Server</li><li>- Microsoft Azure Synapse</li><li>- Snowflake</li></ul>	73 characters
JDBC (PostgreSQL)	63 characters
JDBC (MySQL)	64 characters

For the profiling task to complete successfully, rename the column so that length has the maximum characters allowed or fewer.

### Data profiling task for some catalog sources fails if the user is assigned only the Governance Administrator role.

This issue impacts the following source systems:

- Amazon S3
- Google BigQuery
- Google Cloud Storage
- Microsoft Azure Data Lake Storage Gen2
- Amazon Redshift
- Snowflake

For the data profiling task to complete successfully, assign the Designer role to the user.

### The data profiling task for a Snowflake catalog source fails with the following exception:

```
"SEVERE: Exception creating result java.lang.ExceptionInInitializerError at  
sun.misc.Unsafe.ensureClassInitialized(Native Method) "
```

To resolve this issue, perform the following steps:

1. In the Informatica Intelligent Cloud Services Administrator, go to **Runtime Environments**.
2. Select the Secure Agent that runs the data profiling task, and click **Edit**.
3. From the Service menu, select **Data Integration Server** and set the following values for these parameters:
  - JVMOption1: "-Xms1024m"
  - JVMOption2: "-Xmx4096m"
4. Click **Save**.
5. Rerun the data profiling for the Snowflake catalog source.



Data profiling task for a catalog source may fail with the error, 'Mapping execution failed for object: <table\_name>: EP\_13236 Could not open the following dll: [./libpmdpaggregate.so]'

This happens if the Data Quality service is not enabled for the Secure Agent on which you are running the data profiling task.

To resolve this issue, perform the following steps:

1. In the Informatica Intelligent Cloud Services Administrator, go to **Runtime Environments**.
2. Click the **Actions** menu for the Secure Agent that runs the data profiling task.
3. From the menu, select **Enable or Disable Services, Connectors**.
4. Select the **Data Quality** service from the list of services, and click **OK**.
5. Rerun data profiling for the catalog source.

### A Rule Occurrence job does not run

A rule occurrence job might not run if the Rule Occurrence isn't created correctly. This happens if a rule occurrence job isn't created as a scorecard. To verify that a Rule Occurrence is created properly, check the following parameters:

- core.location
- core.origin

To check the parameters, perform the following steps:

1. Open a browser network tab.
2. Open the generated Rule Occurrence.
3. Run the following call and check the response: `ccgf-searchv2/api/v1/search`

If there are any discrepancies in the core.location parameter, run the location refresh Rest API.

To Identify if a Rule Occurrence was created from the Cloud Profiling service (via a Scorecard) run the following REST API command: `ccgf-searchv2/api/v1/search`

The REST API response must contain the following attribute values:

- The `com.infa.ccgf.models.governance.profileRef` attribute must contain the Cloud Profile reference ID.
- The value of the `com.infa.ccgf.models.governance.isExternal` attribute must be 'true'.

### Data profiling task for a catalog source with a large number of profiling filters fail with the error `java.lang.OutOfMemoryError`

This happens if you apply filters and run a data profiling task.

To resolve this issue, limit the number of profiling filters to 400 and rerun the data profiling job.

## CHAPTER 3

# Data quality

Enable the data quality capability to generate data quality scores for the extracted metadata from catalog sources. You can then view the data quality scores for assets in Data Governance and Catalog.

When you create a catalog source, select the **Data Quality** option on the **Configuration** wizard to enable data quality for the catalog source. Set the data quality configuration options and run the catalog source job to monitor the status of the data quality task and view the task results on the job overview page.

You can view the detailed information about data quality scores for the extracted metadata in Data Governance and Catalog when you open assets extracted from the source system.

**Note:** You can run data quality tasks only on assets that use rules created with single input and output fields in Data Quality.

For more information about viewing data quality scores of assets extracted from source systems, see the *Asset Details* in the *Data Governance and Catalog* help system.

## Data quality configuration options

Based on your requirements, configure the options to determine the type of data that you want the data quality task to collect, the scope of the data quality run, and the sample rows on which you want to run the data quality task.

After you enable **Data Quality** on the **Configuration** wizard while creating a catalog source, you can configure the following options on the **Data Profiling and Quality** tab:

### Runtime environment

Select a runtime environment in which you can run data quality tasks on a Secure Agent. If you don't select a runtime environment, the data quality task runs in the runtime environment that your organization administrator selected when they created the connection.

**Note:** You can run data profiling and data quality tasks on a Windows Secure Agent configured with NTLMv2 proxy authentication.

### Data Quality Rule Automation

Select to enable data quality automation for assets in the catalog source. When you enable data quality automation and run the catalog source job in Metadata Command Center, a data quality automation job is triggered, and rule occurrences are automatically created and associated with all data elements that are linked to corresponding glossary business assets in Data Governance and Catalog.

Choose one of the following options:

- **Apply on data elements linked with business data set.** Creates rule occurrences for all data elements that are linked with business data sets in the catalog source.
- **Apply on all data elements.** Creates rule occurrences for all data elements in the catalog source.

The following table describes different options that influence the data quality automation process:

isAutomated option on rule templates in Data Governance and Catalog	Data quality option in Metadata Command Center	Data quality automation option in Metadata Command Center	Result
Yes	Yes	Yes	Create rule occurrences for all data elements that are associated with glossary business assets.
Yes	Yes	No	Does not create new rule occurrences for data elements or update an existing rule occurrence on data elements. Does not affect the execution of the existing rule occurrences in Data Governance and Catalog.
Yes	No	Not applicable	Does not create any rule occurrences for data elements. Data quality execution stops for existing rule occurrences that are associated with assets of a particular catalog source.
No	Yes	Yes	Does not create rule occurrences for data elements. Does not affect the execution of the existing rule occurrences in Data Governance and Catalog

For more information about data quality automation, see the *Asset Details* in the *Data Governance and Catalog* help system.

## Data Quality Remediation

Specify a flat file connection to store the list of failed rows so that users can remediate poor data quality scores.

Choose one of the following options:

- **No.** Doesn't enable the **Create Data Quality Failure Ticket** option.
- **Yes.** Shows a list of flat file connections where you write failed rows to customer-managed locations.

## Data Quality Failure Ticket

Specify whether you want to create data quality failure tickets for poor data quality scores based on the threshold defined for the rule occurrence in Data Governance and Catalog.

Choose one of the following options:

- **No.** Doesn't automatically create data quality failure tickets when the data quality scores are poor.
- **Yes.** Automatically creates data quality failure tickets based on the data quality threshold values you define in Data Governance and Catalog, and notifies you when a data quality score is below the threshold.

**Note:** To remediate a poor data quality score, you must configure a workflow event for the data quality failure and enable the event in Metadata Command Center. To enable automatic creation of the data quality failure tickets, ensure that the stakeholders you specified in the **Event Details** tab are added to the data element.

## Cache Result

Specify how you want to preview the rule occurrence results in Data Governance and Catalog.

Choose one of the following options:

- **Agent Cache.** Generates a cache file in the runtime environment. This helps you preview the cached results faster in subsequent data preview runs in Data Governance and Catalog. By default, the results are cached for seven days after you run the data preview task in the runtime environment for the first time. You can also choose to customize the number of days you want to retain the preview results for. To customize the days of preview results, update the `mps_previewFileRetentionInDays` property in the **System Configuration Details** section of the **Metadata Platform Service** in Administrator. For more information about Metadata Platform Service properties, see the *Secure Agent Services* in the Cloud Common Services help system.
- **No Cache.** Does not cache the preview results. You can preview the results live in Data Governance and Catalog.

**Note:** Run the catalog source again whenever you change the **Cache Result** option from Agent Cache to No Cache.

## Connection

Select the SAP Table connection to run data quality tasks on SAP ERP objects.

## Run Rule Occurrence Frequency

Specify whether you want to run data quality rules based on the frequency defined for the rule occurrence in Data Governance and Catalog.

Choose one of the following options:

- **Yes.** Data quality rules run based on the frequency that you configured in Data Governance and Catalog. If you set a data quality schedule for the catalog source, the job doesn't impact the data quality rule occurrence frequency.
- **No.** Disables the data quality rule occurrence frequency that you configured in Data Governance and Catalog. If you don't set a data quality schedule for the catalog source, the data quality rules don't run.

**Note:** Ensure that the data quality schedule has not expired. The data quality rules don't run if the data quality schedule that you configured for the catalog source is expired.

## Sampling type

Determine the sample rows on which you want to run the data quality task. The sampling options vary based on the catalog source that you create.

Choose one of the following options:

- **All Rows.** Runs data quality on all rows in the metadata.
- **Limit N Rows.** Runs data quality on a limited number of rows. You can specify the limited number of rows on which you want to run data quality.
- **Random N Rows.** Runs data quality on the selected number of random rows.
- **Random N Percentage.** Run data quality on select rows based on the percentage of data that you specify in the **Percentage of Data to Sample** field. Google BigQuery tables are organized as data blocks. For example, you can specify 5 percentage of data blocks from a table to run the profile on.
- **Custom Query.** Provide a custom SQL clause to select sample rows to run the data quality task.

In the **Sampling Query** field, enter the custom SQL clause to choose sample rows on which you want to run the data quality task. Verify that the syntax of the SQL clause matches the syntax of the database that you are connecting to.

Examples:

- if you're using the JDBC catalog source to connect to IBM DB2 and the sampling query is `FETCH FIRST 50 ROWS ONLY`, then the query runs data quality only on the first 50 rows.
- if you enter `employeeName like '%a%'` for a Salesforce catalog source, then the query selects rows that contain 'a' in the column `employeeName`.

**Note:** For the Salesforce catalog source, you cannot use the `LIMIT` clause in a sampling query. For example, you cannot use `Name like '%a%' LIMIT 10`.

## Elastic runtime environment

Select a runtime environment in which you can run data quality tasks on an advanced cluster. Select an elastic runtime environment for complex file types, including AVRO and Parquet.

**Note:** This option is available when you configure data quality for Amazon S3, Google Cloud Storage, and Microsoft Azure Data Lake Storage Gen2 catalog sources.

To run data quality on an Avro or Parquet file, connect to the following types of advanced cluster in your organization:

- **Fully-managed cluster.** A multi-node serverless infrastructure that intelligently scales based on your workload and offers the lowest total cost of ownership for your organization. For more information, see [Fully-managed clusters](#).
- **Local cluster.** A single-node cluster that you can start on the Secure Agent machine. You can use a local cluster to quickly onboard projects for advanced use cases. For more information, see [Local clusters](#).

For more information about setting up AWS, Google Cloud, and Microsoft Azure for local and fully-managed clusters, see [Advanced clusters](#).

## Staging connection

Applicable only for elastic data quality executions, that is, for Parquet and Avro sources located in Amazon S3, Microsoft Azure Data Lake Storage Gen2, and Google Cloud Storage source systems.

This is the staging connection where data quality results are stored temporarily during the execution.

## Maximum precision of string fields

The maximum precision value for profiles on string data type. Enter a value between 1 and 255.

## Text qualifier

The character that defines string boundaries. If you select a quote character, the data quality task ignores delimiters within the quotes. Select a qualifier from the list. Default is Double Quote.

## Code page for delimited files

Select a code page that the Secure Agent can use to read and write data. Use this option to ensure that rule results for assets with non-English characters don't include junk characters. Default value is UTF-8.

Choose one of the following options:

- MS Windows Latin 1. Select for ISO 8859-1 Western European characters.
- UTF-8. Select for Unicode and non-Unicode characters.
- Shift-JIS. Select for double-byte characters.
- ISO 8859-15 Latin 9 (Western European).

- ISO 8859-2 Eastern European.
- ISO 8859-3 Southeast European.
- ISO 8859-5 Cyrillic.
- ISO 8859-9 Latin 5 (Turkish).
- IBM EBCDIC International Latin-1.

**Note:** This option is available when you configure data quality for the following catalog sources:

- Amazon S3
- Google Cloud Storage
- Microsoft Azure Data Lake Storage Gen2

### Escape character for delimited files

You can specify an escape character if you need to override the default escape character. An escape character ignores a delimiter character in an unquoted string if the delimiter is part of the string value.

If you specify an escape character, the data quality task overrides the default escape character that the Metadata Extraction job detects and considers the specified escape character. It then reads the delimiter character as a part of the string value. If you don't specify an escape character, the data quality task considers the default escape character that the Metadata Extraction job detects and reads the delimiter character as a part of the string value.

**Note:** This option is available when you configure data quality for the following catalog sources:

- Amazon S3
- Google Cloud Storage
- Microsoft Azure Data Lake Storage Gen2

## Monitor data quality tasks

On the job overview page, monitor the status of data quality tasks and retry tasks that have completed with errors.

After you run the job for a catalog source that has data quality enabled, you can monitor the status of the data quality task and view the results on the **Overview** tab for that job. The data quality result includes statistics such as the discovered objects, profiled objects, skipped objects and failed objects. Data quality tasks create the following subtasks:

- Rule generation
- Rule profiling
- Bulk ingestion
- Task progress tracker
- Batch profiling
- Score propagation

If the data quality task completes with errors, you can retry the task. To retry a task, hover the mouse over the data quality task and click the **Retry Task** icon. When you retry a task, a new rule profiling subtask is created for the data quality task and data quality checks are run on all the objects.

The number of batch profiling subtasks and the maximum number of objects in each batch profiling subtask depend on the `mps_maxDeploymentBatchSize` property of the Metadata Platform Service configured for a Secure Agent.

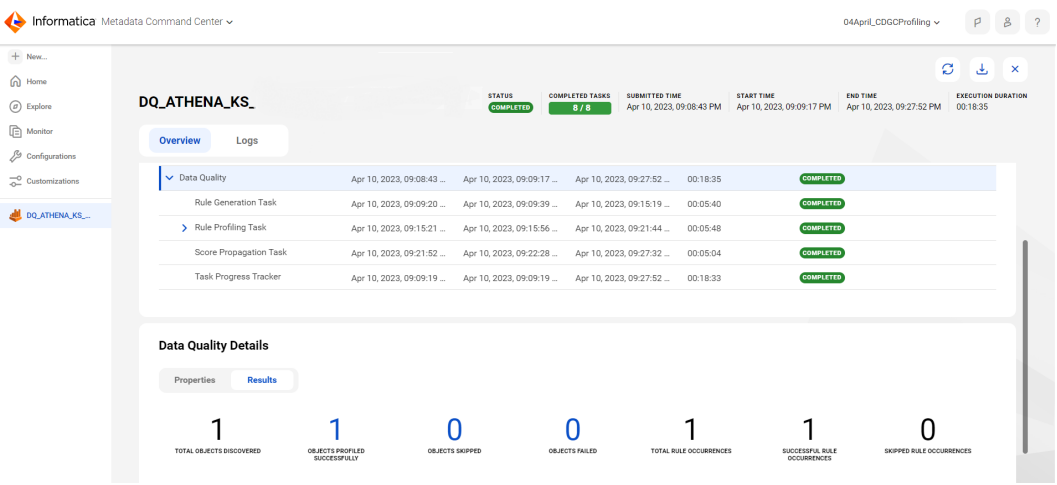
You can view the logs for the objects in the **Logs** tab by sorting the data quality tasks by time. After the data quality task completes, you can view the results in the **Results** tab.

You can download logs to track failed data quality tasks. Click **Failed Session Logs** to download the logs. The ZIP file name represents the catalog source job ID. The catalog source job ID helps you identify the failed data quality task. You can also find the catalog source job ID from the URL of the **Monitor** tab as shown in the following image:



Extract the ZIP file. The extracted ZIP file contains multiple ZIP files based on the number of failed batch profiling tasks. Each ZIP file includes data quality session log files.

The following image shows the job **Overview** page for a data quality task:



For more information about the actions that you can perform on the job monitoring pages, see [“Monitor jobs for technical assets” on page 162](#).

## CHAPTER 4

# Data observability

Data observability analyzes deviations from a usual trend within the data in your source system and generates events for the identified anomalies. You can review and assess the anomalies in Data Governance and Catalog. Enable the data observability capability to identify anomalies in the characteristics of your data and to visualize and evaluate events generated for the anomalies.

When you create a catalog source, enable the **Data Observability** option on the **Data Observability** tab to configure data observability for the catalog source.

For more information about viewing data observability anomalies, see the *Working With Assets* help module for *Data Governance and Catalog*.

## Guidelines for configuring data observability

Consider the following rules and guidelines when you configure data observability:

- Data observability identifies anomalies on the data that you configure and filter for the catalog source. If you apply metadata extraction filters and you further apply profiling filters, data observability identifies anomalies on a subset of the entire data.
- Before you enable data observability for a catalog source, you must either first enable metadata extraction or data profiling based on the catalog source.
- Each time a data observability job runs, Metadata Command Center profiles the data on which metadata is extracted and then detects anomalies on the profiled data .
- To generate accurate data observability results, set the **Profiling Scope** option to **Full** when you configure data profiling.
- Perform a minimum of three profile runs for data observability to detect anomalies in the data.
- However, for the following anomalies, one profiling run is required at minimum:
  - Drop from Maximum anomalies
  - Surge from Minimum anomalies
  - Schema-based anomalies

Data observability detects anomalies from the second profiling run.

- If you modify the profiling filters after data observability has run a few jobs, the resulting profiled data changes. Historic profiled data and historic anomalies are lost. Data observability then runs a job on the new data. To accurately detect anomalies, keep the profiling filters constant over several runs.
- Data observability can observe data that contains up to 50,000 profiled data elements.



# Configuring data observability events

You can apply filters to narrow the data set so that you receive anomaly notifications in Data Governance and Catalog only on relevant and applicable data.

1. Open the catalog source for which you want to configure data observability.
2. In the **Configuration** tab of the wizard, go to the **Data Observability** tab.

The option to enable data observability appears.

The screenshot shows the 'Snowflake Freshness Volume' configuration wizard. The 'Configuration' tab is selected, and the 'Data Observability' sub-tab is highlighted with a red box. Below the sub-tabs, there is a message: 'To get accurate results for data observability, set the Profiling Scope option to Full in the Data Profiling and Quality configuration.' Below this message, the 'Enable Data Observability' toggle is shown, currently turned off.

3. Enable data observability.

The configuration parameters for data observability appear.

The screenshot shows the 'Snowflake Freshness Volume' configuration wizard. The 'Configuration' tab is selected, and the 'Data Observability' sub-tab is highlighted with a red box. Below the sub-tabs, there is a message: 'To get accurate results for data observability, set the Profiling Scope option to Full in the Data Profiling and Quality configuration.' Below this message, the 'Enable Data Observability' toggle is now turned on. Below the toggle, the 'Parameters' section is visible, showing two input fields: 'Minimum Number of Data Points' with a value of 3, and 'Maximum Events to Generate' with a value of 1000.

4. Configure the parameters for data observability.

The following table lists the parameters you can configure:

Option	Description
Minimum Number of Data Points	Specify the minimum number of profiling runs that are required for data observability to start detecting anomalies. For example, if you enter 4 here, anomalies are detected for 4 and subsequent profiling runs. The default value is 3. Enter a number between 3 and 10.
Maximum Events to Generate	Specify the maximum number of anomaly events to generate for each catalog source run. The default value is 1000.
Specify freshness and volume filters	Add filters to observe freshness and volume metrics on the tables that you specify.

Option	Description
Specify data profiling filters	Add filters to objects that you want to profile. You can run data observability on only the profiled objects.
Metric Filters	<p>Select an option to indicate whether you want to further filter the profiled data elements.</p> <ul style="list-style-type: none"> <li>• No filters. Do not filter the profiled data elements. Data observability detects anomalies on the data that you have configured for metadata extraction and profiling.</li> <li>• Filter conditions: Select one or more conditions to filter the profiled data elements. For data observability to detect anomalies, create a further subset of data after metadata extraction and profiling.</li> </ul>
Inclusion or exclusion criteria	<p>Select the filter condition to apply on the profiled data.</p> <ul style="list-style-type: none"> <li>• Include Metric. Specify an inclusion criteria. Data observability detects anomalies on the profiled data that meets the filter criteria.</li> <li>• Exclude Metric. Specify an exclusion criteria. Data observability excludes profiled data that meets the filter criteria.</li> </ul> <p>You can further narrow down the results by clicking <b>Add</b> to add further filter conditions.</p>
Metrics	Select the metric for which data observability notifies users of anomalies.
Sensitivity	<p>Select the sensitivity of the anomaly.</p> <ul style="list-style-type: none"> <li>• Normal. Data observability notifies users of anomalies about normal changes to data.</li> <li>• Sensitive. Data observability notifies users of anomalies about sensitive changes to data.</li> <li>• Severe. Data observability notifies users of anomalies about severe changes to data.</li> </ul>
Detection rules	<p>Select one or more rules to apply on the profiled data to detect anomalies.</p> <ul style="list-style-type: none"> <li>• Static Data. Detect the following anomalies: <ul style="list-style-type: none"> <li>- Percentage variation</li> <li>- Count variation</li> </ul> </li> <li>• 100% or 0% Change Detection. Detect the following types of percentage-based anomalies: <ul style="list-style-type: none"> <li>- Drop from maximum</li> <li>- Surge from minimum</li> </ul> </li> <li>• Standard Deviation. Detect the following anomalies: <ul style="list-style-type: none"> <li>- Drop in transition</li> <li>- Surge in transition</li> <li>- Deviation</li> </ul> </li> <li>• Breaking Trends. Detect the following types of count-based anomalies: <ul style="list-style-type: none"> <li>- Drop</li> <li>- Surge</li> </ul> </li> </ul>

To understand the various types of anomalies and their corresponding metrics in data observability, see the How-to Library article [Understand Data Observability Anomalies in Data Governance and Catalog](#).

## CHAPTER 5

# Data classification

Data classification is the process of identifying and organizing data into relevant categories based on the functional meaning of data. Classifying data can help your organization manage risks, compliance, and data security.

Enable the data classification capability on a catalog source to identify and organize critical source data into logical categories so that you can take measures to work effectively on it. You can either classify data based on AI-defined inclusion rules generated by CLAIRE, or you can curate rule-based data classifications manually in Data Governance and Catalog after the metadata is ingested into the catalog. To create rule-based data classifications, you can either use the predefined classifications, or create custom rules to classify data that is unique to your organization. Metadata Command Center provides more than 200 predefined data classifications by default.

When you configure Data Classification, choose either CLAIRE generated classifications, data classification rules, or both.

**Note:** To create and manage data classifications, ensure that you define appropriate roles and select the **Manage Data Classifications** feature for that role when configuring privileges for the Metadata Command Center service in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help module.

## Types of data classification

Depending on the type of data that you want to identify and classify in your organization, you can perform data element classification, data entity classification, or use CLAIRE generated data classification.

### Data element classification

This is the smallest unit of data classification. It refers to the classification of columns or fields of tables or files. Data element classification labels and categorizes information contained in data elements based on the metadata extracted from source systems and the facts collected as the result of data profiling. For example, you can use data element classification to find sensitive information in columns, such as, credit card numbers, Social Security Numbers or the driver's license numbers. You can then take actions to secure access to sensitive data and set standards for data privacy in your organization.

### Data entity classification

A data entity is a collection of data elements and is derived based on an inclusion scope. For example, if 'Full Name', 'Gender', 'Date of Birth', 'Email', or 'Phone #' are identified in one or more columns of a table, then that table is classified as a 'person' entity. You can use entity classifications to identify important characteristics of data and group them together as entities. This classification identifies data entities such as purchase order, invoice, customer, location, person, or address contained in a data set.

## CLAIRE-generated data classification

This classification is powered by CLAIRE. When you select it, CLAIRE automatically generates data classifications for the data elements.

When you use rule-based data classifications, you choose from predefined or custom data classifications. When you use CLAIRE-generated data classifications, CLAIRE uses the nomenclature of technical data assets to generate classifications. To generate potential classification labels based on asset names, CLAIRE uses an embedded dictionary.

If you select Generated Data Classification for a catalog source in Metadata Command Center, you can view the automatically generated classifications associated with the data elements on the technical asset page in Data Governance and Catalog.

Generated data classification powered by CLAIRE has the following advantages:

- You can generate data classifications without creating data classification rules. You don't have to know how to create inclusion rules in Metadata Command Center.
- You can generate data classifications even if you don't know which of the existing predefined rule-based data classifications you need to select. CLAIRE automatically generates data classifications for the data elements.
- You can either promote a generated classification to a data element classification, or reject the generated classification.
- Once you promote the generated classification, the system remembers and automatically accepts it in future scans. When you use data classification rules, the rules take precedence.
- If you use generated data classification, you don't have to perform profiling. If you use rule-based classifications with Statistics attributes, you need to run data profiling.

**Note:** Source systems such as SAP Business Warehouse (BW), SAP BW/4HANA, SAP ERP, and Salesforce can contain ambiguous data with technical field names. For such source systems, CLAIRE generates data classifications from the source context. For SAP BW, SAP BW/4HANA, and SAP ERP catalog sources, CLAIRE uses the extracted **Business Name** attribute to generate data classifications. For Salesforce catalog sources, CLAIRE uses the extracted **Label** attribute to generate data classifications.

For more information about working with generated data classifications, see *Asset Management* in the Data Governance and Catalog help.

## Creating a data element classification

Create a data element classification with or without inclusion rules. Rule-based data classifications are used to classify data based on matching patterns or column names. A data classification without rules is used to organize or label data into categories specific to your organization.

To create and manage data classifications, ensure that you define appropriate roles and select the **Manage Data Classifications** feature for that role when configuring privileges for the Metadata Command Center service in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

Create a rule-based data element classification to automate the classification of data. You can use a Spark SQL-based expression language to create inclusion rules in the expression editor in Metadata Command Center. You can also choose from more than 200 predefined rule-based data element classifications that Metadata Command Center provides by default.

If you create a data element classification in Metadata Command Center without any inclusion rules, then you can manually associate the data classification with data elements in Data Governance and Catalog after the metadata is ingested into the catalog. For more information about manually associating data classifications, see *Working With Assets* in the Cloud Data Governance and Catalog help.

To create a data element classification, perform the following steps:

1. In Metadata Command Center, click **New**.
2. In the **New** dialog box, select **Data Classification** from the list of asset types in the left pane.
3. Select **Data Element Classification**, and click **Create**.

The **New Data Element Classification** window appears.

4. On the **General Information** tab, enter a name for the data classification. Optionally, enter a description. To create a rule-based data element classification, proceed to the next step. To create a data classification without inclusion rules, go to step 7.
5. In the **Sensitivity** panel, configure data classification sensitivity levels to specify whether a classification is sensitive or not. You can view the sensitivity level labels associated with data elements in Data Governance and Catalog. You can select the following types of sensitivity levels:
  - **None**. Use this option if data is not sensitive. For example, unrestricted and widely accessible data.
  - **Low**. Use this option if data is public. For example, public website content and company contact information.
  - **Medium**. Use this option if data is internal. For example, emails and documents with no confidential data.
  - **High**. Use this option if data is confidential. For example, financial records, biometric data, medical data, intellectual property, and authentication data.

Default value is **None**.

**Note:** If some of the sensitivity levels that are mentioned in this help differ from what is displayed on the Metadata Command Center interface, contact your administrator to understand the sensitivity levels defined for your organization. For more information, see the Metadata Command Center help.

6. In the **Classification Category** panel, click the **Category** field to open the menu.

**New Data Element Classification**

< Back   Next >   Save   Copy   [Icon]   X

1 General Information   2 Qualifier

Type: Element

**Sensitivity**

Sensitivity Level: \* NONE

**Classification Category**

Category: [Dropdown menu showing PII]

7. From the menu select one or more classification categories you want to add to the data element classification. A classification category is the grouping of data classifications into relevant business domains.

If there are more than 10 classification categories, the **Select Classification Category** dialog box appears. Select one or more classification categories and click **OK**.

The following image shows the **Select Classification Category** dialog box for adding multiple classification categories:

**Select Classification Category**

Select Classification Category (42)   Find   [Icon]   [Icon]

☒ Name ↑

- ☒ Diagnostic Data
- ☐ Operational Data
- ☒ Administrative Data
- ☐ Regulatory Compliance Data
- ☐ Research Data
- ☒ Patient Demographics
- ☐ Laboratory and Diagnostic Data
- ☐ Procedural Data
- ☐ Outcome Measures
- ☐ Public Health Data
- ☐ Patient Documentation
- ☐ Insurance Claim Forms

**Selected Classification Category (3)**

- Diagnostic Data
- Administrative Data
- Patient Demographics

OK   Cancel

8. Click **Next** to open the **Qualifier** tab.
9. In the **Inclusion Rule** section of the **Qualifier** tab, construct a data classification inclusion rule using expressions in the basic or advanced mode.

You can use a combination of **Attributes**, **Operators**, **Built-in Functions**, **Lookup Tables** or **Constants** to define a data classification inclusion rule. In the **Advanced** mode, you can type your expressions directly and see autocomplete suggestions as you type your expression in the classification editor. For more

information about data classification rules and examples of data classification rules, see the following topics:

- [“Data element classification inclusion rule” on page 43](#)
- [“Example: Classify a column in a table as CUSIP numbers” on page 47](#)
- [“Example: Use a lookup table in a data classification expression” on page 66](#)

**Note:** You can specify data classification expression values without exceeding the 5000 character limit.

10. Click **Validate** to validate your expression.

If the validation is successful, a success message appears.

11. Click **Save**.

On the **Explore** page, you can view all the saved data element classifications sorted by their type.

After you create a data classification, you can perform one of the following actions:

- For rule-based data classifications, enable the data classification capability for the catalog source and add the data classification to the catalog source configuration. During the catalog source run, the inclusion rules are used to classify the metadata into meaningful categories based on matching column names and column content patterns. You can view the data classification results in Data Governance and Catalog.
- For both rule-based data classifications or data classifications without rules, manually associate the published data classifications with data elements in Data Governance and Catalog after the metadata is ingested into the catalog. The data elements are manually classified or labeled based on the associated data classification.

## Data element classification inclusion rule

Apply data element classification to a data element by creating inclusion rules. You can create inclusion rules using the metadata that is extracted from the source and the data facts collected due to data profiling. Data element classification is, therefore, independent of the source type. If the data profiling capability is not enabled on the catalog source, then you can create and use metadata-based expressions only.

The data classification expressions are created using a Spark SQL-based language. You can construct a data element classification rule using the following components:

- **Attributes:** Attributes are column values that you obtain from the extracted metadata or from the statistics collected due to data profiling. Metadata-based attributes are column name, column comment, parent name, and parent comment. Statistics-based attributes include, number of profiled values in a column, frequent values in a column, average of values profiled for a column, and other such attributes.
- **Operators:** Operators are used to compare values of columns. For example, you can use an equality operator to check if the names of the two columns are the same.

**Note:** When you use standard comparison operators such as `>`, `>=`, `=`, `<`, or `<=` to compare values of columns that contain NULL or unknown values, the result is NULL if any of the compared values is NULL or unknown.

- **Built-in Functions:** Built-in functions are used to calculate values and manipulate data. For example, a function can be changing a name to all upper case or lower case using the `Lower` or `Upper` functions. Other supported functions include, but are not limited to, `Trim`, `Size`, `Length`, `Substring`, `Forall`.
- **Lookup Tables:** When there is a finite set of values, use lookup tables that you have imported and published to check whether the values in the column appear in the lookup table. You can look up any attribute in the column of the lookup table. For example, the expression `NAME IN LOOKUP_TABLE.REFCOLUMN` looks for the name of the column in the `REF` column of the lookup table. You

can either import and publish a predefined lookup table that Metadata Command Center provides by default or import your own lookup table.

- **Constants:** A constant contains a value that doesn't change during the execution of the expression. Constants are used in data classification rules to store lengthy values to improve the readability of complex classification expressions. To use a constant in a data classification rule, you must define a constant by specifying a name and a value for the constant. The scope of a constant is local, not global. This means that the constant that you create within a data classification rule can be used only within that rule. To define a constant within a classification rule, see [“Defining a constant for a data element classification rule” on page 44](#).
- **Reference Data:** You can use reference data from Reference 360 to specify rules for data classification. When creating data element classifications, you specify values from Reference 360 to check whether these values appear in the data elements from your catalog source. If the selected reference data values match the values in a data element, that data element is classified under the corresponding data element classification.

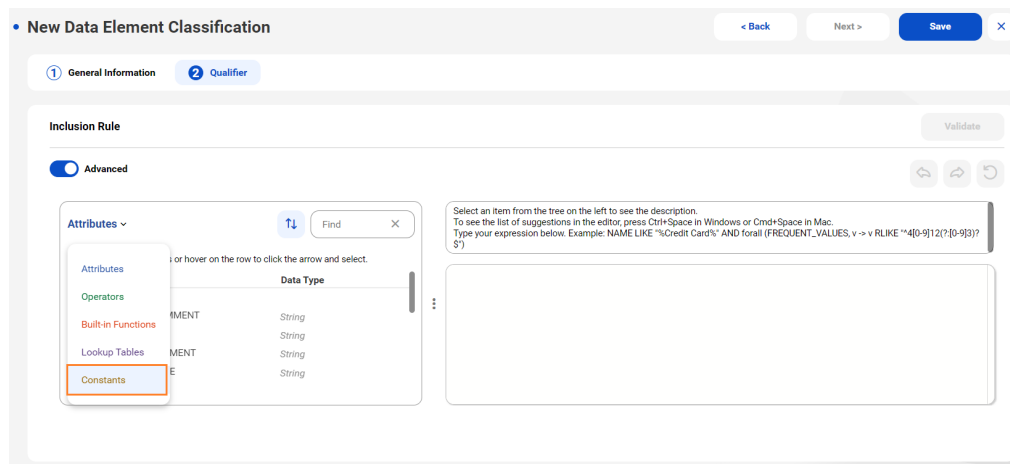
## Defining a constant for a data element classification rule

Use constants in data element classification rules to store lengthy values to improve the readability of complex data classification expressions.

Before you use a constant in a rule, you must define the constant. The scope of a constant is local, not global. This means that the constant that you create within a data classification rule can be used only within that rule.

To define a constant for a data element classification rule, perform the following steps:

1. In the **Inclusion Rule** section of the **Qualifier** tab, toggle to the **Advanced** mode.
2. From the list on top, select **Constants**.





- Click the Add Constant icon. The **Add Constant** dialog box appears.

### Add Constant

Name: \* ?

Value: \* ?

Enter a value for the constant.  
Example : '^([1-5][0-9]{14})2(22[1-9][0-9]{12})2[3-9][0-9]{13})\$'

Description:

Data Type: String

?
OK
Cancel

- Enter a name for the constant.  
The name should not exceed 31 characters. It should start with a letter and may contain letters, digits, and underscores.
- In the **Value** field, enter a value that does not exceed 1000 characters in length for the constant.
- Optionally, enter a description.
- Click **OK** to save the constant.

#### Example: Adding a constant for a data classification rule that validates credit card numbers

Consider the following data classification rule that validates all major credit cards:

```
(UPPER(NAME) LIKE '%CARD%NUMBER%' OR UPPER(NAME) LIKE '%CC%NUM%' OR LOWER(NAME) IN
lcp_ccn_col.header_col_names) AND (size(filter(FREQUENT_VALUES, v -> REGEXP_REPLACE(v, '-|
\s', '') _RLIKE '^3[47][0-9]{13}$|^5[1-5][0-9]{14}|2(22[1-9][0-9]{12})2[3-9][0-9]{13}|
[3-6][0-9]{14}|7[0-1][0-9]{13}|720[0-9]{12}))$|^4[0-9]{12}(?:[0-9]{3})?|^6(?:011\d{12}|
5\d{14}|4[4-9]\d{13}|22(?:1(?:2[6-9]|[3-9]\d)|[2-8]\d{2})9(?:[01]\d|2[0-5]))\d{10})$'
$')) / size(FREQUENT_VALUES)) >= 0.8f
```

To improve the readability of this lengthy rule, let us define a constant called **CCN\_EXP**, and assign the expression for credit card number patterns as the value to the constant in the following manner:

```
CCN_EXP='^3[47][0-9]{13}$|^5[1-5][0-9]{14}|2(22[1-9][0-9]{12})2[3-9][0-9]{13}|[3-6][0-9]{14}|
7[0-1][0-9]{13}|720[0-9]{12}))$|^4[0-9]{12}(?:[0-9]{3})?|^6(?:011\d{12}|5\d{14}|
4[4-9]\d{13}|22(?:1(?:2[6-9]|[3-9]\d)|[2-8]\d{2})9(?:[01]\d|2[0-5]))\d{10})$'
```

By using the constant **CCN\_EXP**, the data classification rule mentioned above can be rewritten as follows to reduce the length significantly:

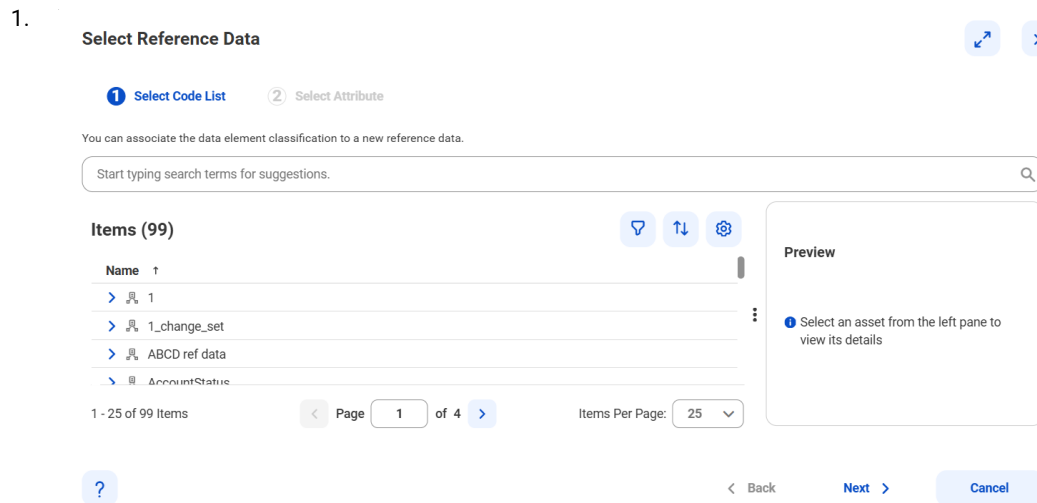
```
(UPPER(NAME) LIKE '%CARD%NUMBER%' OR UPPER(NAME) LIKE '%CC%NUM%' OR LOWER(NAME) IN
lcp_ccn_col.header_col_names) AND (size(filter(FREQUENT_VALUES, v -> REGEXP_REPLACE(v, '-|
\s', '') _RLIKE $CCN_EXP)) / size(FREQUENT_VALUES)) >= 0.8f
```

## Using reference data to define a data element classification

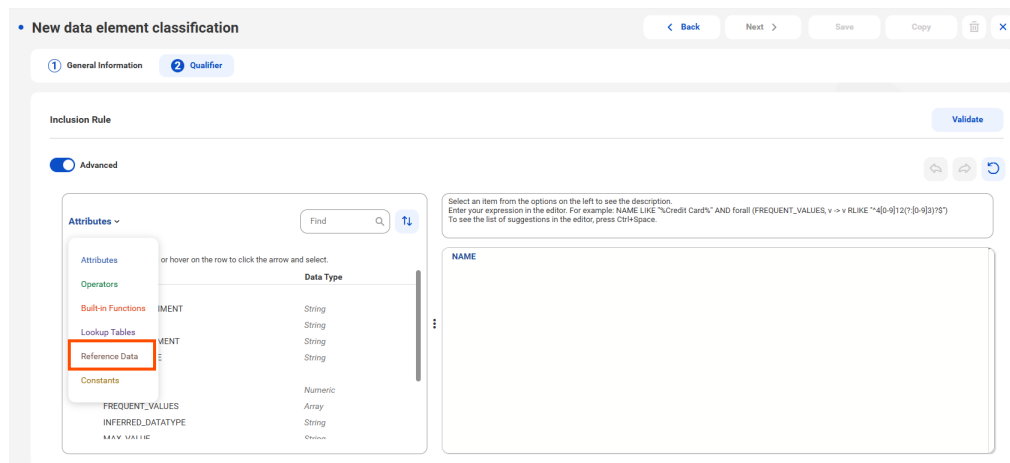
You can use reference data from Reference 360 while creating a data element classification to define rules that check for matching values in data elements during classification. You can specify these rules in basic or advanced mode in Metadata Command Center.

To use reference data when creating a data element classification, perform the following steps:

1. In the **Inclusion Rule** section of the **Qualifier** tab, select an attribute from the **Attribute** list.  
You can select either the **Name** or **Frequent Value** attribute to associate reference data.
2. From the **Operator** list, select **Appears in Reference 360**.
3. Select **Browse** to add attributes in the **Values** field.  
The **Select Reference Data** dialog box appears.
4. From the **Select Code List** tab, select the code list that you want to associate with your data element classification and click **Next**.



5. In the **Select Attribute** tab, select the attributes of the code values you want to associate with your data element classification.
6. Click **Finish**.
7. To manually enter a classification expression using reference data, toggle on the **Advanced** option.
8. From the list on top, select **Reference Data**.



- To add reference data, click to expand the reference data and select the attributes by clicking the arrow next to them.

The attributes appear in the classification editor.

- Click **Validate**.

If you select reference data attributes from multiple reference data sets that have the same name, the system will validate all the selected reference data attributes, but it will save only one of them.

## Example: Classify a column in a table as CUSIP numbers

CUSIP (Committee on Uniform Securities Identification Procedures) numbers identify North American securities and are usually 9 characters long. For example, a CUSIP number can be 3 9 2 6 9 0 Q T 3. Let us construct an expression that classifies a column in a table as CUSIP numbers. The expression checks if the column name contains the word 'cusip' and all the frequently occurring values in the columns of the data set follow the specified pattern. Depending on the matches, the expression classifies the columns in the data set as 'cusip\_number'. We can construct the expression in the following way:

```
LOWER(NAME) LIKE '%cusip%' AND forall(frequent_values,v->v=NULL OR LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}[0-9a-zA-Z]{2}[0-9]' OR LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}-[0-9a-zA-Z]{2}-[0-9]' OR LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}[0-9a-zA-Z]{2}[0-9]')
```

We use attributes (NAME, FREQUENT\_VALUES), operators (AND, IN, OR), and built-in functions (LOWER, FORALL) to construct the above expression. Let us simplify the expression to understand the function that each phrase performs:

- `LOWER(NAME) LIKE '%cusip%'`: This phrase returns the column name with all characters changed to lowercase and checks if the column name contains the word 'cusip'.
- `FORALL(FREQUENT_VALUES, v->v=NULL`: The FORALL function is used with FREQUENT\_VALUES to evaluate the expression for all the frequently occurring values in the columns of the data set. The `v=NULL` checks if there is a NULL value in the frequent value attribute.
- `LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}[0-9a-zA-Z]{2}[0-9]' OR LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}-[0-9a-zA-Z]{2}-[0-9]' OR LOWER(v) RLIKE '[0-9]{3}[0-9a-zA-Z]{3}[0-9a-zA-Z]{2}[0-9]'`: This phrase defines the pattern of the CUSIP number to check against the frequent values occurring in the column.

## Example: Frequent values in data classification

The FREQUENT\_VALUES attribute is an advanced option that enables you to determine the most frequent column values. The results depend on the sampling type that you select when you configure a catalog

source. You select the sampling type on the **Data Profiling and Quality** tab. Use the attribute in the form of an inclusion rule when you configure Data Classification.

The FREQUENT\_VALUES attribute includes all distinct values and displays them in order of most common values in the profile results.

If you use the FREQUENT\_VALUES attribute in a data element classification rule, the rule fetches all distinct records from the available values. Based on the records, the frequency percentage is calculated and appears in profiling results. You can construct rules with percentage values and conformance percentage.

For example, the rule can have the following structure: FREQUENT\_VALUES = [USA, UK, INDIA, CHINA, RUSSIA, CANADA, BRAZIL, CHILE].

The following table contains sample values that the FREQUENT\_VALUES attribute could apply to:

VALUES	COUNT	PERCENTAGE
USA	2	20%
UK	2	20%
INDIA	1	10%
CHINA	1	10%
RUSSIA	1	10%
CANADA	1	10%
BRAZIL	1	10%
CHILE	1	10%

## Creating a data entity classification

To identify the semantics of data entities in a data set, create a data entity classification and associate it with a catalog source. Data entities are collections of data elements and are derived based on an inclusion scope.

To create a data entity classification, perform the following steps:

1. In Metadata Command Center, click **New**.
2. In the **New** dialog box, select **Data Classification** from the list in the left pane.
3. Select **Data Entity Classification**, and click **Create**.

The **New Data Classification** window appears.

4. In the **General Information** section, enter a name for the data classification. Optionally, enter a description.

5. In the **Inclusion Scope** section, specify the following information:
  1. Select the data element classifications depending on the entity you wish to identify. For example, to identify the 'Address' entity, you may select data elements such as 'Address Line1', 'Postcode', 'City', 'District'.
  2. For the Include option, choose **All** if you want all the selected data element classifications to be present in the data for it to qualify as an entity classification. Or, choose **Any** and specify the number of data element classifications that should be present in the data for it to qualify as an entity classification. For example, if any three data element classifications from the selected classifications are identified in one or more columns of a table, then that table is classified as an 'Address' entity.
6. Click **Save** after you define the inclusion scope.

On the **Explore** page, you can view all the saved data classifications sorted by their type.

After you create a data entity classification, you can associate it with a catalog source to identify data entities in a data set. To associate a data classification with a catalog source, enable the data classification capability for that catalog source. For more information about enabling this capability while creating a catalog source, see the *Catalog Source Configuration* help.

## Updating a data classification

You can edit an existing data classification to update the name, description, sensitivity level, or the inclusion rule.

To edit an existing data classification, perform the following steps:

1. In Metadata Command Center, go to the **Explore** page.
2. Click the menu on the top of the page and select **Data Classifications**.

On this page, you can browse through all existing data classification assets and view basic information about each table.
3. Open the overview page of the selected data classification by performing one of the following steps:
  - Hover your mouse over the data classification that you want to edit and click the Action menu on the far right. Select **Edit** from the menu.
  - Click the data classification name.

The overview page of the selected data classification appears.

**Note:** The overview page of a data entity classification displays the name, description, and the previously created inclusion rule. The overview page of a data element classification displays the name, description and the sensitivity level.

4. Update the data classification. You can update or modify the following information:
  - Name of the data classification
  - Description of the data classification
  - Inclusion rule in a data entity classification
  - Sensitivity level in a data element classification
  - Category of the data element classification

**Note:** Metadata Command Center allows you to update or modify the predefined data classifications that you import. If you import the same classifications again, they retain their default names regardless of the changes that you made.

5. Click **Save**.

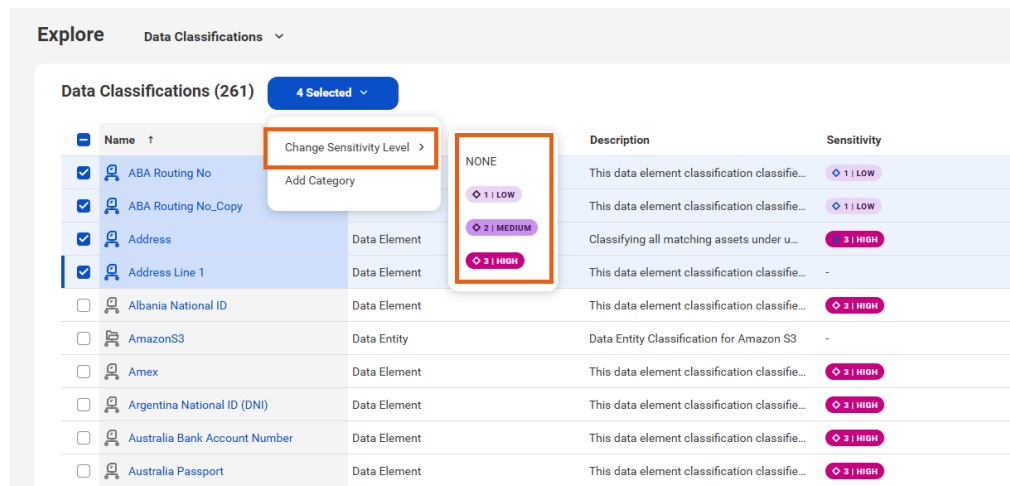
If you edit a data classification that is associated with a catalog source, you must rerun the data classification capability for that catalog source for your changes to appear.

## Updating sensitivity level of multiple data element classifications

You can update the sensitivity level of multiple data element classifications. You can update both the data classifications created by users and the predefined data classifications.

1. In Metadata Command Center, go to the **Explore** page.
2. Click the menu on the top of the page and select **Data Classifications**.  
On this page, you can browse through all existing data classifications.
3. Select the data element classifications for which you want to update the sensitivity level.
4. On the **Data Classifications** table, click the **Selected** button, and from the menu, select **Change Sensitivity Level**.

The following image shows the menu for changing sensitivity levels:



5. From the **Change Sensitivity Level** menu, select the sensitivity for the selected classifications. If the data element classifications that you select have different sensitivity levels, the levels are updated to the new sensitivity level that you selected.

**Note:** You can update the sensitivity level of predefined data classifications, but if you import them again, they maintain the original sensitivity level.

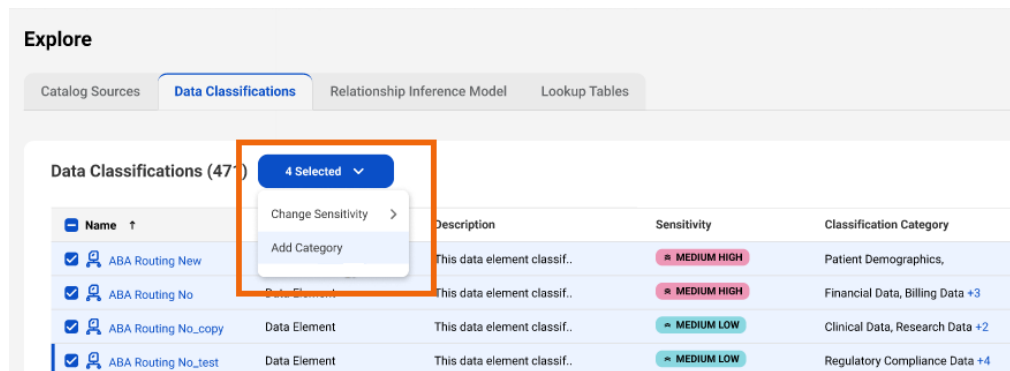
To change the sensitivity level of a single data element classification, see [“Updating a data classification” on page 49](#).

# Adding classification categories to multiple data classifications

You can add classification categories to multiple data element classifications. You can add classification categories to data classifications created by users and the predefined data classifications.

1. In Metadata Command Center, go to the **Explore** page.
2. On the top of the page, click the action menu and select **Data Classifications**.  
On this page, you can browse through all existing data classifications.
3. Select the data element classifications for which you want to update the classification category.
4. On the **Data Classifications** table, click the **Selected** button, and from the dropdown menu, select **Add Category**.

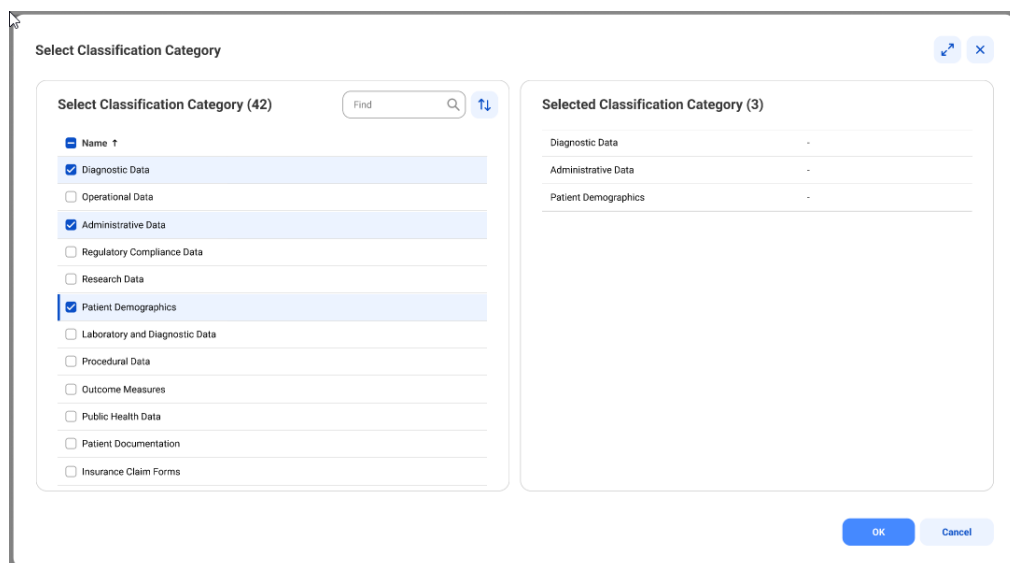
The following image shows the menu for adding classification category:



5. From the **Select Classification Category** dialog box, select one or more classification categories you want to add to the data element classification.

Classification categories you select appear on the right.

The following image shows the **Select Classification Category** dialog box for adding multiple classification categories:



6. Click **OK** to add the classification categories.

To add classification categories to a single data element classification, see [“Updating a data classification” on page 49](#).

## Cloning a data classification

You can clone data element and data entity classifications to create another classification with the same details.

To clone an existing data classification, perform the following steps:

1. In Metadata Command Center, go to the **Explore** page.
2. From the menu on the top of the page, select **Data Classifications**.  
On this page, you can browse through all existing element and data entity classifications and view basic information about each.
3. Select the data classification you want to clone and click **Clone** from the **Action** menu.  
The overview page of the cloned data classification appears in edit mode.  
**Note:** By default, the cloned data classification has the same name suffixed with \_Clone. You can change the name if needed.
4. For a data element classification, you can update the description, sensitivity level, classification category, and modify the data classification expression to update the inclusion rule. For a data entity classification, you can update the description, and select or clear data element classifications depending on the entity you wish to identify.
5. Click **Save**.

## Deleting a data classification

You can delete data classifications that you don't need. You can delete both data element classifications and data entity classifications. You can't delete data element classifications that are currently used in data entity classifications. To delete it, you must first remove the data element classification from the existing data entity classification. If you delete data entity classifications that contain data element classifications, the data element classifications don't get removed.

Deleting a data classification removes links between the classification and its associated data elements. Catalog sync jobs in the running state might fail when you initiate a job to delete a data classification. Before you delete a data classification, ensure that the sync job for catalog sources configured with this data classification are complete.

**Note:** You can't perform any actions on data classifications when a delete job is in progress.

1. In Metadata Command Center, go to the **Explore** page.
2. Select **Data Classifications** from the menu to open a list of data classifications.
3. You can delete data classifications in one of the following ways:
  - Select the data classifications that you want to delete and click **Delete** from the **Action** menu.
  - Open the data classification that you want to delete. On the **Data Classification** page, click **Delete**.A warning message appears.



4. Click **Delete**.

A confirmation message appears with a link to the **Monitor** page.

To view the job details, task status, and details of the deleted data classifications, click the job name on the **Monitor** page.

The following image displays job details of a sample deleted data classification on the **Job Details** page:

The screenshot displays the 'Job Details' page for 'OrderID\_DataClassification'. The page includes a header with navigation links and a status bar. The main content area is divided into sections: 'Job Details', 'Tasks (3)', and 'Delete Data Classification Details'.

**Job Details:**

- Job ID: 45555554f-8bde-42a1-94d4-839961630294
- User Name: cdp@exp\_06/06/2025
- Job Type: Delete Data Classification
- Trace ID: b249ed35f-1ea5-4e32-9353-11baed08b077

**Tasks (3):**

Name	Scheduled Time	Start Time	End Time	Run Duration	Status	Type
Delete Data Classification	Jul 4, 2025, 5:54:41 AM	Jul 4, 2025, 5:56:26 AM	Jul 4, 2025, 6:00:40 AM	00:04:14	Completed	Delete Data Classification
Bulk Ingestion	Jul 4, 2025, 5:56:49 AM	Jul 4, 2025, 5:58:38 AM	Jul 4, 2025, 6:00:27 AM	00:01:49	Completed	Bulk Ingestion
Data Classification Inference	Jul 4, 2025, 5:56:29 AM	Jul 4, 2025, 5:56:26 AM	Jul 4, 2025, 6:00:40 AM	00:04:14	Completed	Data Classification Inference

**Delete Data Classification Details:**

Properties Results

1  
Deleted Classification Count

## CHAPTER 6

# Relationship discovery

The relationship discovery capability for catalog sources identifies pairs of similar columns and relationships between tables within a catalog source.

In order to discover relationships, the relationship discovery service uses predictions made by relationship inference models. The relationships that this service infers are referred to as Inferred Relationships. The relationship discovery capability allows you to infer the following relationships:

- **Column Similarity:** The identification of semantically similar pairs of columns within a catalog source
- **Joinable Tables Relationships:** The identification of tables that can be joined based on the column similarity predictions.

To enable the relationship discovery capability for catalog sources, you must specify appropriate values for related parameters while configuring a catalog source. For information about enabling this capability while creating a catalog source, see the *Catalog Source Configuration* help.

To discover similar columns and joinable table relationships, ensure that you configure the following options:

- On the **Data Profiling and Quality** tab, enable data profiling.
- In the **Parameters**, select **Keep Signatures and Values** as the run mode.

These configuration options enable you to retain values of the columns in the profiling results and discover relationships.

### Using the relationship discovery capability

You can use the relationship discovery capability in several ways, including the following:

- Provide recommendations of tables that can be joined with other tables.
- Assist in migrating data to the cloud by analyzing related objects.

## Relationship inference model

The relationship inference model is a predefined model consisting of user-defined rules and machine learning components. You can use this model to discover the relationships between columns within a catalog source.

The relationship discovery capability infers table-level relationships on the basis of column similarity relationships.


Metadata Command Center provides a predefined relationship inference model called *Column Similarity Model v1.0*. This model discovers similar columns within a catalog source based on the similarity among column values. You can import this model and associate it with any catalog source to discover the relationships defined in the model. For information about importing predefined content, see the *Introduction and Getting Started* help.

To associate a relationship inference model with a catalog source, you must enable the **Relationship Discovery** option and specify parameters while creating a catalog source. For more information about creating a catalog source, see the *Catalog Source Configuration* help.

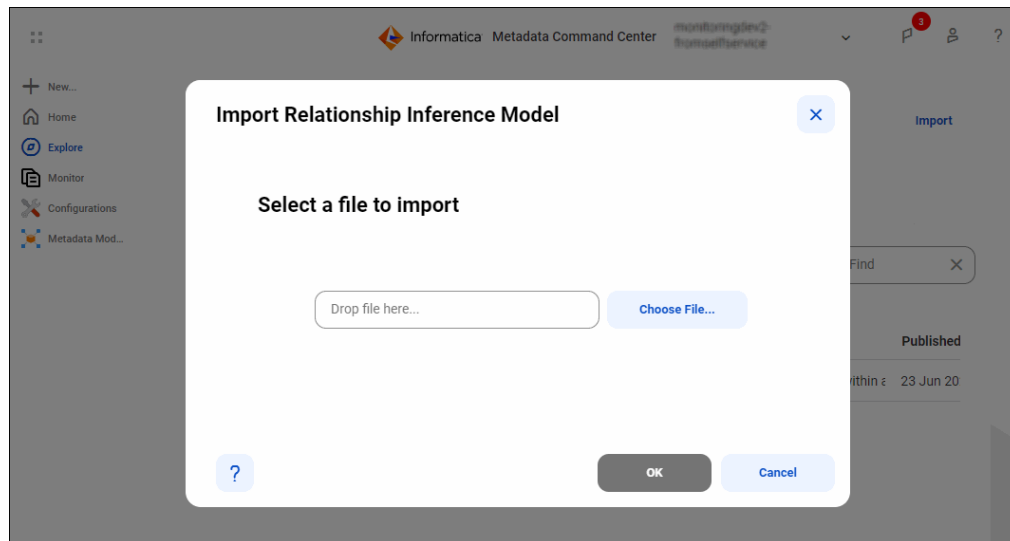
## Import a relationship inference model

Metadata Command Center allows you to import a relationship inference model to infer column-level and table-level relationships within a catalog source.

To import a relation inference model, perform the following steps:

1. In Metadata Command Center, go to the **Explore** page in the left navigation panel.
2. Click the arrow (  ) icon on the top of the page and select **Relationship Inference Model**.
3. On the **Relationship Inference Model** window, click **Import**.

The **Import Relationship Inference Model** dialog box appears.



4. Click **Choose File** to navigate to the predefined model file on your local machine. You can also drag and drop the file.
5. Click **OK**.

The imported model appears in the list of models on the **Relationship Inference Model** window.

After you import the relationship inference model, you can use the model to identify pairs of similar columns and table level relationships in a catalog source. You can associate the relationship inference model with a catalog source while creating a catalog source. For more information about creating a catalog source, see the *Catalog Source Configuration* help.

## CHAPTER 7

# Glossary association

You can associate terms that are in the glossary with technical assets to provide user-friendly business names to technical assets. The Glossary Association capability for a catalog source automatically associates glossary terms with technical assets, or recommends glossary terms that you can manually associate with technical assets in Data Governance and Catalog.

This capability associates glossary terms only with data elements, such as columns, and technical data sets, such as tables. When you configure a catalog source, select the **Glossary Association** capability on the **Configuration** wizard to get intelligent recommendations for the extracted technical assets in Data Governance and Catalog. After running the **Glossary Association** capability in Metadata Command Center, you can curate the glossary recommendations in Data Governance and Catalog. For more information about curating glossaries for technical assets, see the *Asset Management* help module in Data Governance and Catalog.

**Note:** Source systems such as SAP BW, SAP BW/4HANA, SAP ERP, and Salesforce can contain ambiguous data with technical field names. For such source systems, CLAIRE generates glossary associations from the source context. For SAP BW, SAP BW/4HANA, and SAP ERP catalog sources, CLAIRE uses the extracted **Business Name** attribute. For Salesforce catalog sources, CLAIRE uses the extracted **Label** attribute.

You can also manually associate glossary metric and business term assets with data element and data entity classifications in Data Governance and Catalog. To view the associations, you must run the catalog source job with the Glossary Association capability enabled after you associate the glossary assets with the classifications.

The following image shows the glossary association tab on the **Configuration** wizard while configuring a catalog source:

The screenshot shows the 'IGA\_011' Configuration wizard with the 'Glossary Association' tab selected. The wizard has four steps: 1. Registration, 2. Configuration, 3. Associations, and 4. Schedule. The 'Configuration' step is active, and the 'Glossary Association' sub-tab is selected. The configuration options are as follows:

- Assign Business Names and Descriptions:** Radio buttons for 'Yes' (selected) and 'No'. A toggle for 'Keep Existing Business Names and Descriptions' is turned on.
- Ignore Keywords:** Radio buttons for 'No' (selected) and 'Yes'.
- Glossary Association Scope:** Radio buttons for 'All Glossary Assets' (selected) and 'Top-level Glossary Assets'.
- Use Abbreviation and Synonym Definitions:** Radio buttons for 'Yes' (selected) and 'No'. A text input field contains 'Curation\_Lkp' and a 'Select' button is next to it. A 'Mimiccast for Outlook' button is also visible.

# Configuration settings

Based on your requirements, you can enable or disable the auto-acceptance of recommended glossary terms, set a threshold limit for auto-acceptance, ignore the prefix and suffix of a data element while making recommendations to associate business glossary terms, and use abbreviation and synonym definitions from a lookup table to associate glossary terms.

When you enable Glossary Association for a catalog source, you can configure the following options on the **Glossary Association** tab:

## Enable auto-acceptance

Select this option to automatically accept recommended glossary terms and assign them as business names to data elements extracted from the source system. The associated glossary term is selected on the basis of the confidence score threshold that you specify. If you don't select this option, you can manually accept or reject recommended glossary terms in Data Governance and Catalog.

## Confidence score threshold for auto-acceptance

Specify a percentage from 80 to 100 inclusive to set a threshold limit based on which the glossary association capability automatically accepts recommended glossary terms.

For example, consider a `cust_nm` column in an Oracle source system and a `Customer Name` glossary term. When you configure the Oracle catalog source, select the **Enable auto-acceptance** option for glossary association, set the confidence score threshold to 92%, and run the catalog source job. If the `Customer Name` glossary term matches the `cust_nm` column with a score of 92% or more, then the Glossary Association capability assigns the `Customer Name` business name to the `cust_nm` column in Data Governance and Catalog.

## Enable below-threshold recommendations

If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold. The recommendations are generated based on the confidence score threshold that you specify.

## Confidence score threshold for recommendations

If you enable auto-acceptance, specify a percentage from 80 to the selected auto-acceptance threshold to set a confidence score limit based on which the glossary association capability makes recommendations. You can accept or reject the recommended glossary terms that fall within this range in Data Governance and Catalog.

If you disable auto-acceptance, specify a percentage from 80 to 100 inclusive to set a confidence score limit based on which the glossary association capability makes recommendations. Accept or reject the recommendations in Data Governance and Catalog.

## Assign business names and descriptions

Select this option to automatically assign business names and descriptions to technical assets. You can then choose to retain existing assignments and only assign business names and descriptions to assets that don't have assignments, or allow overwrite of existing assignments.

By default, existing assignments are retained.

## Ignore specified keywords

Specify prefix and suffix values that you want to ignore from data elements during glossary association. Prefix and suffix values are case insensitive. If you don't select this option, the Glossary Association capability considers entire data elements while making recommendations to associate business glossary terms with your technical assets.

## Define the glossary association scope

Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well. Select **Top-level Glossary Assets** and specify the assets on the **Select Assets** page.

After you run the catalog source job, the following glossary associations are removed:

- All glossary associations that are not in scope based on the selected glossaries.
- All corresponding glossary associations if you deleted the top-level glossary assets that were previously defined in the glossary association scope.

**Note:** If the top-level glossary asset that you previously defined in the glossary association scope is no longer a top-level asset, the association is retained.

## Use abbreviation and synonym definitions

Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, click **Select**.

When you use abbreviation and synonym definitions, the glossary association capability finds accurate matches based on the lookup table and increases the confidence score of the glossary terms. This enables CLAIRE to prioritize glossary terms that match your defined synonyms, reducing false positives and enhancing confidence score for automated associations.

For example, without the lookup table for glossary association, `TRX_ID` might match 'Transfer ID' or 'Training ID', and `INV_DT` could match both 'Inventory Date' and 'Invoice Date'. If you enable glossary association with a lookup table, the algorithm boosts the confidence score for the matches and assigns the names with the correct business glossary terms, such as 'Transaction ID' and 'Invoice Date'.

## CHAPTER 8

# Lineage discovery

Use CLAIRE to discover complete lineage of catalog sources.

Due to technological limitations or security constraints, you might not always see complete lineage after metadata extraction. To build complete lineage, you can perform connection assignment from a reference catalog source connection to the endpoint objects in the reference source system. You can assign and unassign connections on the **Assign Connections** tab on the **Lineage** tab of the **Configure** page.

Manual connection assignment can be a time-consuming and error prone task. To simplify the task, you can use CLAIRE to build the complete lineage of a catalog source by recommending related catalog sources to assign to reference catalog source connections.

To view related catalog sources and CLAIRE recommendations, enable the lineage discovery capability when you configure a catalog source. When you run the catalog source job, Metadata Command Center assigns the reference catalog source connections to CLAIRE recommended endpoint catalog source objects. You can then view the list of CLAIRE recommendations and accept or reject them.

You can't view CLAIRE recommendations for catalog sources that don't have the lineage discovery capability. You can manually assign connections for such catalog sources on the **Assign Connections** tab.

For information about catalog sources that have the lineage discovery capability, see *Source systems* in the *Catalog Source Configuration* help.

For more information about how to enable lineage discovery for a catalog source, see *Creating a catalog source* in the *Catalog Source Configuration* help.

For relational database source systems, you can also link catalog sources and construct data lineage using the **Link Catalog Sources** tab on the **Lineage** tab of the **Configure** page. You can choose source and target catalog sources to link and create lineage.

## Prerequisites to view CLAIRE recommendations

To view CLAIRE recommendations, perform the following tasks:

- Define appropriate roles and select the **Manage Connection Assignments** feature for the roles when you configure privileges for Metadata Command Center in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.
- Verify that metadata is extracted from the endpoint catalog sources.
- Configure and run catalog sources with the lineage discovery capability. Optionally, add filters for lineage discovery to help CLAIRE generate better recommendations.

# Curate CLAIRE recommendations

After you run a catalog source with lineage discovery enabled, you can view the list of related catalog sources with the endpoint object recommendations. You can then accept or reject them.

When you run a catalog source with the lineage discovery capability, CLAIRE identifies matching objects in connected catalog sources and calculates the percentage of matched and unmatched objects. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog. You can accept or reject each CLAIRE recommendation individually. Alternatively, you can select multiple recommendations to accept or reject them in bulk. When you accept a CLAIRE recommendation, Metadata Command Center creates links between the endpoint objects in the connected catalog sources.

If you accept a CLAIRE recommendation, the selected catalog source is accepted, and future recommendations are also accepted. If you initially reject CLAIRE recommendations and later accept them, the status changes from rejected to accepted. When you accept a CLAIRE recommendation, the connection assignment job starts. You can check the status of the job on the **Monitor** page.

After you curate the CLAIRE recommendations, you can view the complete lineage in Data Governance and Catalog.

**Note:** Due to change in metadata and connection assignment of accepted catalog sources, CLAIRE recommendations can become outdated over time. Run the catalog source job again with the lineage discovery capability to refresh the recommendations.

## Accept or reject CLAIRE recommendations

You can accept or reject CLAIRE recommendations on the **Related Catalog Sources** tab on the **Lineage** tab of the **Configure** page.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, use filters to view the related catalog sources with CLAIRE recommendations. Click the **Add Filter** menu and add a filter with **Recommendations** as **True**.

You can filter the list by catalog source type or recommendations.

Catalog sources with CLAIRE recommendations are represented with a thunderbolt icon on the **Catalog Sources** panel.

3. Select a catalog source and click the **Related Catalog Sources** tab.

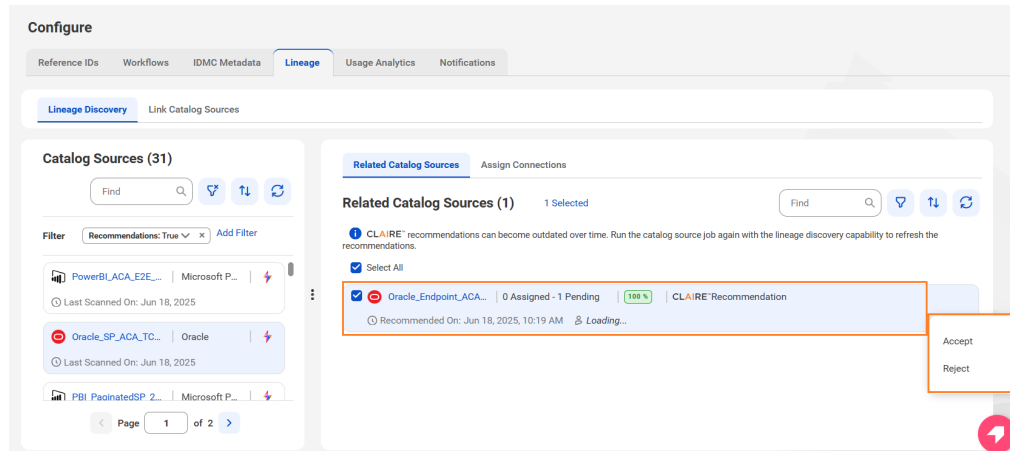
Based on the catalog source you select, the **Related Catalog Sources** tab displays a list of related catalog sources.



4. Hover your mouse over a related catalog source and click **Accept** or **Reject** from the **Action** menu.

For more details about each catalog source, click the catalog source name on the **Catalog Sources** panel or the **Related Catalog Sources** tab to view the catalog source configuration details.

The following image shows the **Related Catalog Sources** tab highlighting the options to accept or reject a CLAIRE recommendation:



After you accept the CLAIRE recommendation, the connection assignment job starts. You can check the status of the job on the **Monitor** page. When the job completes, the connection is successfully assigned and Metadata Command Center creates links between the recommended objects in the connected catalog sources. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog.

## Resolve conflicts

You might notice conflicts between connections in CLAIRE recommendations. If there are conflicts, resolve and accept the CLAIRE recommendations.

Conflicts between connections can occur in the following scenarios:

- Duplicate metadata across catalog sources.
- Duplicate catalog source configurations.
- Same metadata in the catalog from production and other non-production environments.
- High percentage of matches in multiple catalog sources for the same connection.

**Note:** When you configure a catalog source, add filters for lineage discovery to avoid duplicate recommendation conflicts.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, use filters to view the related catalog sources with CLAIRE recommendations. Click the **Add Filter** menu and add a filter with **Recommendations** as **True**.

You can filter the list by catalog source type or recommendations.

3. Select a catalog source for which you want to resolve conflicts and click the **Related Catalog Sources** tab.

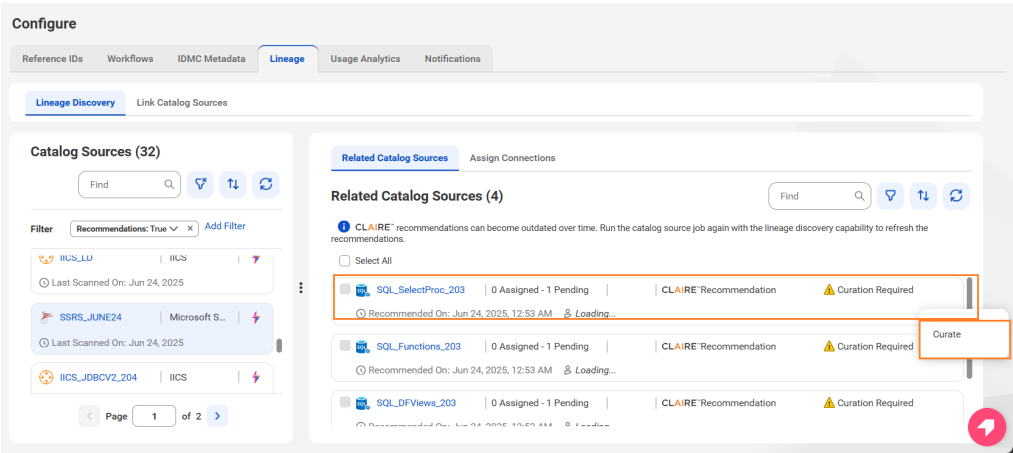
Based on the catalog source you select, the **Related Catalog Sources** tab displays a list of related catalog sources.

CLAIRE recommendations with conflicts are marked as Curation Required.

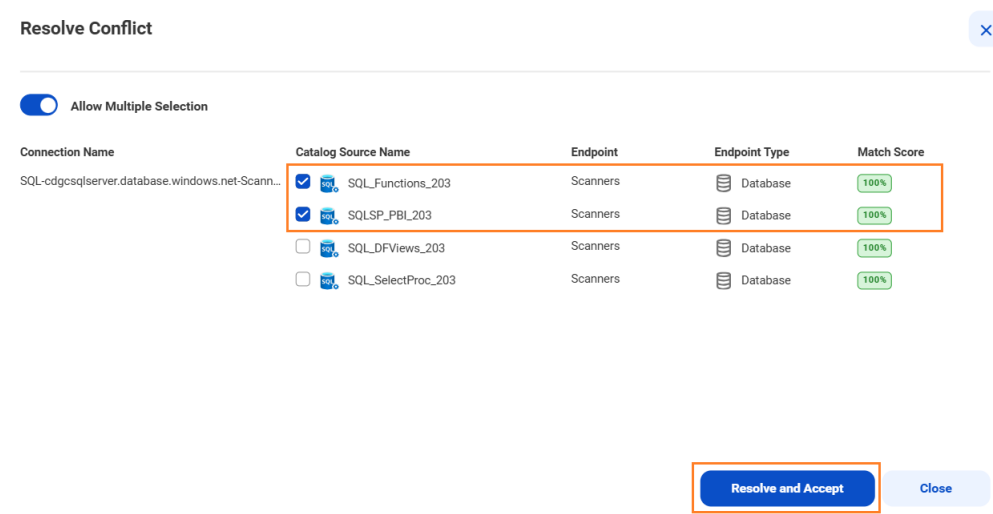
4. Hover your mouse over a related catalog source with conflicts and click **Curate** from the **Action** menu.

For more details about each catalog source, click the catalog source name on the **Catalog Sources** panel or the **Related Catalog Sources** tab to view the catalog source configuration details.

The following image shows the **Related Catalog Sources** tab for a catalog source highlighting the option to curate a CLAIRE recommendation with conflicts:



- The **Resolve Conflict** dialog box appears with a list of catalog sources and the endpoint objects that have conflicts in connections.
5. In the **Resolve Conflict** dialog box, click **Allow Multiple Selection** to select multiple catalog sources.
- Note:** If it is a conflict related to a duplicate catalog source, you don't need to select multiple catalog sources.
6. Select one or more catalog sources and click **Resolve and Accept**.
- The following image shows the **Resolve Conflict** dialog box:



After you resolve conflicts and accept the CLAIRE recommendations, the connection assignment job starts. You can check the status of the job on the **Monitor** page. When the job completes, the connection is successfully assigned and Metadata Command Center creates links between the recommended objects in the connected catalog sources. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog.

## CHAPTER 9

# Lookup tables

A lookup table contains predefined data that you can use to look up values and find matching patterns for data. Lookup tables usually contain finite non-overlapping sets of data that help you define a standard set of values for data elements.

In Metadata Command Center, you can import and publish CSV files as lookup tables that you can use in data classification and glossary association.

Lookup tables enable automatic classification of data elements through data classifications and enhance glossary association based on a predefined set of abbreviations and synonyms.

When you choose to look up values of a column in the lookup table in your data classification inclusion rule, the rule uses the column data in the lookup table to classify data.

For example, let us assume that your organization's data set contains company specific non-overlapping product IDs that follow a particular pattern. You can copy these product IDs in a CSV file, and then upload the CSV file as a lookup table in Metadata Command Center. You can then create a data classification rule using this lookup table to classify the columns in the specified data set as *Product ID*.

When you choose a lookup table with synonyms and abbreviations as an input in your glossary association task, CLAIRE uses the data from the lookup table to match and associate accurate glossary terms with technical assets.

For example, consider an organization where technical assets use specific naming conventions, such as `TRX` and `DT` to represent 'Transaction' and 'Date'. Without contextual information or synonym definitions, CLAIRE might misinterpret the abbreviations. For instance, `TRX_ID` can incorrectly match 'Transfer ID' or 'Training ID' instead of 'Transaction ID', while `DT_ID` can match either 'Date ID' or 'Decision Tree ID'.

To resolve this, you can add synonyms and abbreviations to a lookup table, then configure glossary association with the lookup table. The glossary association algorithm assigns higher confidence scores to the correct glossary terms, significantly improving the accuracy of automatic glossary associations. As a result, `TRX` explicitly maps to 'Transaction' and `DT` to 'Date'.

If you want to modify a lookup table, you can export it. Update the downloaded file and then re-import it.

**Note:** You must be a Catalog Administrator user to upload and publish lookup tables in Metadata Command Center.

For information about uploading lookup tables, see [“Importing and publishing a lookup table” on page 64](#).

# Importing and publishing a lookup table

Import and publish multiple lookup tables in Metadata Command Center that you can use to look up values with matching data patterns while classifying data and associating glossary terms.

To import and publish a lookup table, ensure that you define appropriate roles and select the **Manage Reference Data** feature for that role when configuring privileges for the Metadata Command Center service in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

1. Click **New**.
2. Select **Lookup Table** from the list of asset types.
3. Click **Create**.

The **New Lookup Table** page opens.

**New Lookup Table**

**General Information**

**Name:** \*  Enter a name for the lookup table

**Identifier:** ⓘ A system-generated unique identifier that you can use in data classification expressions with inclusion rules.

**Description:**  Enter a description for the lookup table

**Code Page for Delimited Files:** ⓘ UTF-8

**Glossary Association Synonyms:** ⓘ ☐

**Lookup Table File:** \* ⓘ  Select a CSV file

▼ Hide Lookup Table File Restrictions

- The file size must not exceed 5 MB.
- The file must contain headers, use a comma as the delimiter, and can contain up to 5 columns.
- The first line in the file must be a header based on which column names are identified.
- Column names can contain letters, digits, and underscores. They cannot contain special characters. ASCII punctuation symbols such as @ # & ? and ~ are not allowed.
- The column size must not exceed 150 characters.

4. Enter a name for the lookup table. The name can contain only letters, digits, underscores, and spaces.  
The name that you enter is converted into a unique identifier that you can use in classification expressions while creating a data classification rule.
5. Optionally, enter a description.
6. In the **Code Page for Delimited Files**, select a code page to match the encoding of the lookup table file that you upload. Use this option to ensure that lookup table files with non-English characters are displayed correctly when published. Default is UTF-8.

Select one of the following options:

- UTF-8. Select if the lookup file contains Unicode and non-Unicode characters.
  - Shift-JIS. Select if the lookup file contains double-byte characters.
7. Optionally, select **Glossary Association Synonyms** to use the data in a lookup table file as synonyms or abbreviations to associate glossary terms with technical assets.

Before you enable Glossary Association Synonyms, you must ensure that the CSV file contains only Abbreviation and Synonym column headers with a comma as the delimiter.

**Note:** You can't disable this option after you publish the lookup table.

8. Click **Browse** to import a CSV file. Read the following rules and guidelines before you upload a CSV file:
  - The size of the CSV file must not exceed 5 MB.
  - The file must contain headers, use a comma as the delimiter, and can contain up to 5 columns. Each column is considered as a string data type.
  - The first line in the file must be a header based on which column names are identified.
  - Column names can contain letters, digits, and underscores. They cannot contain special characters. ASCII punctuation symbols such as @ # & ? and ~ are not allowed.
  - The column size must not exceed 150 characters.
  - The row length must not exceed 750 characters.
9. Click **Save** to publish the lookup table.

A Lookup Table Import job is initiated. You can click **View Status** to monitor the status of the job on the **Overview** page for that import job. If the publishing is successful, the job status changes to **Published** and the last job status changes to **Completed**. You can see the top 20 sample values of the lookup table when the publishing is complete.

The screenshot shows the 'TestLKP' interface. It has a 'General Information' section with fields for Name (TestLKP), Identifier (testltp), and Description (a text box). There's a 'Code Page for Delimited Files' dropdown set to 'UTF-8'. Below that is a 'Glossary Association' section with a 'Synonyms' checkbox. The 'Lookup Table File' section shows a file named 'Curation\_Glossary\_Synonym\_LkpTable.csv' with a 'Browse' button. To the right, the 'Status' is 'Published', 'Published On' is 'Jun 25, 2025, 12:22 AM', and 'Last Job Status' is 'COMPLETED' with a 'View Status' link. At the bottom, there's a table titled 'Sample Data from the Last Published File: Curation\_Glossary\_Synonym\_LkpTable.csv (14)' showing columns for 'abbreviation' and 'synonym'.

abbreviation	synonym
AGE	MT_GlossarySynonym_Col_1
COI2*%*%\$1	BT_GlossarySynonym_Col_3
CREDITLIMIT	MT_GlossarySynonym_Col_3
CUSTOMER_ID	BT_GlossarySynonym_Col_1
CUSTOMERS	BT_GlossarySynonym_Tbl_2
DEMO	MT_GlossarySynonymREVIEW_Table_1
EMAIL	BT_GlossarySynonymDraft_Col_1
EMPLOYEES	MT_GlossarySynonym_Tbl_1
EMPLOYEES_VIEW	BT_GlossarySynonym_Tbl_1
FIRST_NAME	BT_GlossarySynonym_Col_2
JOB_ID	BT_GlossarySynonymObsolete_Col_1
LAST_NAME	MT_GlossarySynonym_Col_2

After successfully publishing a lookup table, you can perform any of the following actions:

- Use a lookup table in data classification expressions to define an inclusion rule. See [“Example: Use a lookup table in a data classification expression” on page 66](#).
- Use the data in a lookup table as synonyms and abbreviations to associate glossary terms with technical assets. See [“Example: Use the data in a lookup table for glossary association” on page 66](#).
- Edit a lookup table on the **Explore** page. See [“Editing a lookup table” on page 67](#).

## Example: Use a lookup table in a data classification expression

After you import and publish lookup tables, Metadata Command Center allows you to use the look up tables in data classification expressions to create inclusion rules. You can look up any attribute, such as the name, inferred data type and frequent values on a column in a lookup table.

Let us construct an expression that looks up city names from the lookup table named 'cities' that we have imported and published. The expression checks if all the frequently occurring values in the columns of the data set are names of cities that are present in the lookup table named 'cities'. Depending on the matches, the expression classifies the columns in the data set as 'city'. We can construct the expression in the following way:

```
NAME LIKE "%City%" AND FORALL(FREQUENT_VALUES,v->v IN cities.name)
```

We use attributes (NAME, FREQUENT\_VALUES), operators (AND, IN), and built-in functions (FORALL) to construct the above expression. Let us simplify the expression to understand the function that each phrase performs:

- NAME LIKE "%City%": This phrase evaluates the expression for column names that contain the word 'City'.
- FORALL: This function is used with frequent\_values to evaluate the expression for all the frequently occurring records in the specified column of the lookup table.
- FREQUENT\_VALUES,v->v IN cities.name: This phrase evaluates the items in the array for the most frequently occurring values in the column named 'name' of the lookup table called 'cities'.

## Example: Use the data in a lookup table for glossary association

After you import and publish lookup tables, you can use the data from the lookup tables for glossary association. You can look up any abbreviation and synonym for a technical asset in a lookup table.

Let's consider that your source system includes technical assets named TRX, TRN, NM, and DT. These asset names are often ambiguous and easily misunderstood and glossary association for such technical assets is inaccurate.

To remove ambiguity and ensure accurate glossary association, perform the following tasks:

1. Define your lookup synonym CSV file with common synonyms and abbreviations.  
The following table contains sample lookup synonym CSV file values for glossary association:

Abbreviation	Synonym
TRX	Transaction
TRN	Transaction
NM	Name
DT	Date


Abbreviation	Synonym
ADDR	Address
AMT	Amount
HR	Human Resources
IT	Information Technology

2. Create a lookup table and upload the lookup synonym CSV file for glossary association.
3. Import and publish the lookup table.
4. Enable glossary association for the catalog source and then upload the lookup synonym CSV file.

## Editing a lookup table

You can edit an existing lookup table to change the description or overwrite the last imported CSV file.

To edit an existing lookup table, perform the following steps:

1. In Metadata Command Center, go to the **Explore** page.
2. Click the arrow (  ) icon on the top of the page and select **Lookup Tables**.  
On this page, you can browse through all published and unpublished look up tables and view basic information about each table.
3. Hover your mouse over the lookup table that you want to edit, and click the Action menu on the far right.
4. Select **Edit** from the menu.  
The overview page of the selected lookup table appears. The overview page displays the name, description, the name of the CSV file that you had last imported, and the top 20 sample values from the lookup table.
5. Update the description of the lookup table, or click **Browse** to overwrite the last imported CSV file with another one.  
**Note:** You cannot change the attributes of the last imported CSV file. If you attempt to overwrite the last imported CSV file with another CSV file that contains different attributes, an error message appears.
6. Click **Save** to publish the lookup table.  
If the publishing is successful, the status of the job changes to **Published** and the last job status changes to **Completed**. You must refresh or reload the page for your changes to reflect.

# Exporting a lookup table

You can export a lookup table, download and modify the file, and then re-import it.

To export a lookup table, you need the **Manage Reference Data** feature privilege. For more information about feature privileges, see the *Introduction and Getting Started* help.

1. In Metadata Command Center, go to the **Explore** page.
2. Click the menu on the top of the page and select **Lookup Tables**.

On this page, you can browse through all published and unpublished lookup tables and view basic information about each table.

3. Hover your mouse over the lookup table that you want to export, and click the **Action** menu.
4. Select **Export**.

A job starts to export the lookup table. You can monitor the status of the job on the **Overview** page. If the publishing is successful, the job status changes to `Published` and the last job status changes to `Completed`. You can see the top 20 sample values of the lookup table when the job completes.

You can also click **Export** on the lookup table page.

5. Click **Download Export File** in the Job Details area to download the CSV file.
6. Optionally, curate the downloaded file based on business needs and re-import the file.

For information about importing lookup tables, see [“Importing and publishing a lookup table” on page 64](#).

**Note:** You can export predefined and user-created lookup tables, but you can only re-import user-created lookup tables.



## CHAPTER 10

# Connections

To build and analyze data lineage across catalog sources, assign or unassign objects from catalog sources to specific connections based on your requirements.

Connection assignments specify how objects in a catalog source can be related to matching objects in another catalog source. When you perform a sync job on an ETL catalog source, Metadata Command Center extracts connections from the ETL catalog source and creates a reference catalog source. A reference catalog source indicates that it contains references from other source systems along with the source and target tables mapping.

To ensure that the source connection maps accurately to the objects from the catalog source, you can manually assign these connections from reference catalog sources to objects from the configured catalog source. After you assign connections to objects in the catalog source, Metadata Command Center creates links between matching objects in the connected catalog sources and presents it in the form of percentage of matched objects versus unmatched objects. This percentage determines the accuracy of the data lineage information that you can view in Data Governance and Catalog.

Based on the percentage of matched and unmatched objects, you can assign or unassign connections on the **Assign Connections** tab of the **Configure** page. You can monitor the status of the assign or unassign jobs on the **Monitor** page. You can then verify that the data lineage flow is accurate in Data Governance and Catalog.

If you want to rerun already assigned connections to resolve any connection assignment failures, you can rerun the assignment job.

## Connection assignment overview

You can assign and unassign connections, and accept or reject discovered endpoint recommendations on the **Assign Connections** tab of the **Configure** page. To view **Assign Connections**, click **Lineage Discovery** on the **Lineage** tab.

You can modify connection assignments to endpoint catalog source objects.

After you assign connections, there can be both matched and unmatched objects in the catalog. You can export a list of matched and unmatched objects to a Microsoft Excel file. You can use this list for remediation or as a reference.

The **Assign Connections** tab displays the list of connections along with the following details for each connection:

Property	Description
Connection Name	The name of the connection.
Catalog Source	The catalog source to which the connection is assigned.
Endpoint	The object in the catalog source that has a connection to another object in another catalog source.
Endpoint Type	The type of the endpoint object.
Catalog Source Type	The type of catalog source.
Job Status	The status of the assign or unassign job.
Objects	Percentage of the matched objects versus unmatched objects in the catalog sources.

You can apply a filter or sort the list of connections by connection name. You can also search for a connection by using the connection name. For example, to find a connection name starting with `HE4CLNT`, you can search using the prefix or suffix, that is, `HE4*` or `*4CLNT`.

**Note:** If the source schema contains case-sensitive tables or if the reference objects contain multiple objects with the same name in different cases, perform case-sensitive connection assignment to get correct lineage.

Based on the catalog source you select on the **Catalog Sources** panel, the **Related Catalog Sources** tab displays a list of related catalog sources.

For more information about related catalog sources and lineage discovery, see *Lineage discovery* in the *Administration* help.

## Assigning connections

You can assign a connection to one or more catalog sources.

To assign or unassign specific connections to objects in the catalog source, ensure that you define appropriate roles and select the **Manage Connection Assignments** feature for that role when configuring privileges for Metadata Command Center in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

To assign connections to catalog sources, perform the following steps:

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, select the required catalog source.

You can filter the list by catalog source type or recommendations.

Catalog sources with CLAIRE recommendations are represented with a thunderbolt icon on the **Catalog Sources** panel.

3. Click the **Assign Connections** tab.

The **Assign Connections** tab displays a list of assigned and unassigned connections along with details for each connection. On the **Assign Connections** tab, use filters to view the connections based on the connection names. Click the **Add Filter** menu to add filters.

Based on the catalog source you select on the **Catalog Sources** panel, the **Related Catalog Sources** tab displays a list of related catalog sources.

4. On the **Assign Connections** tab, select the connection to the reference source system and click **Assign**.  
The connection name appears prefixed to the reference catalog source name on the **Hierarchy** tab of your catalog source in Data Governance and Catalog.

The **Assign Connection** dialog box appears with a list of recommended objects from the endpoint catalog sources. Click **All** to view all endpoint catalog source objects.

5. In the **Assign Connection** dialog box, select one or more objects from the endpoint catalog sources and click **Assign**.

You can filter the list in the **Assign Connection** dialog box by name, type, or endpoint.

6. To view CLAIRE recommended endpoint objects, click **Recommended**.

To view all the endpoint objects, click **All**.

7. Select or clear the **Case Sensitive** option to determine whether you want the endpoint object name to be considered as case insensitive during the object matching process between the connected source systems.

8. Click **Assign**.

A confirmation message appears. The **Jobs** tab of the **Monitor** page appears with the connection assignment jobs. On the **Assign Connections** tab, click **Refresh** and the job status of the connection changes to **Assigning**.

If your catalog source uses connection-aware scans, run the catalog source job again. If you configured the catalog source job to run on a regular schedule, the next scheduled run picks up the updated details. If you didn't configure a schedule, run the catalog source job again to view complete lineage.

When you click **Assign**, Metadata Command Center creates links between matching objects in the connected catalog sources, and it calculates the percentage of matched and unmatched objects. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog.

**Note:** If you run the catalog source sync job after assigning the connections, the `CatalogMergeOperationTask` is triggered. If this task fails or completes with errors during the catalog source sync job, then all the previously assigned connections to that catalog source are removed and its status changes to unassigned. You can then assign connections to that catalog source on the **Monitor** page as described in the steps above.

9. For catalog sources with lineage discovery enabled, if there are multiple connections with one endpoint recommendation, select the connection and click **Accept Recommendation** or **Reject Recommendation** from the **Action** menu.

**Note:** You can view CLAIRE recommendations for a catalog source if run with the lineage discovery capability.

If there are multiple connections with one endpoint recommendation, click the **Multiple** link available on the Endpoint, Endpoint Type, or Catalog Source Type properties, and accept or reject the CLAIRE recommendations in the **Catalog Sources** dialog box.

If there is a single connection, select the connection and click **Accept** or **Reject** from the **Action** menu.

After you accept the CLAIRE recommendation, the connection assignment job starts. You can check the status of the job on the **Monitor** page.

# Unassigning connections

You can unassign a connection from the assigned catalog sources.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, select the required catalog source.  
You can filter the list by catalog source type or recommendations.
3. Click the **Assign Connections** tab.  
Use filters to view connections based on the connection names. Click the **Add Filter** menu to add filters.
4. Select an assigned connection and click **Unassign** from the **Action** menu.  
A warning message appears.
5. Click **Unassign**.

A confirmation message appears. The **Jobs** tab of the **Monitor** page appears with the connection unassignment jobs. On the **Assign Connections** tab, click **Refresh** and the job status of the connection changes to **Unassigning**.

**Note:** When the job completes, the connection is successfully unassigned. The connection unassignment job updates the lineage to reference objects, but the reference objects might still appear as assigned until you re-run the catalog source job.

6. If you see reference objects after the connection unassignment job completes, re-run the catalog source job to update the lineage to the pre-assignment state.

After the connections are unassigned, Metadata Command Center refreshes the percentage of matched objects versus unmatched objects in the connected catalog sources. After you re-run the catalog source job, the lineage updates to the pre-assignment state.

# Modifying assigned connections

You can modify connection assignments to endpoint catalog source objects.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, select the required catalog source.  
You can filter the list by catalog source type or recommendations.
3. Click the **Assign Connections** tab.  
Use filters to view connections based on the connection names. Click the **Add Filter** menu to add filters.
4. Select an assigned connection and click **Edit** from the **Action** menu.  
The **Assign Connection** dialog box appears.
5. To modify connection assignments, clear the endpoint objects that you want to remove from the connection.  
Select endpoint objects that you want to assign to the connection.
6. Click **Assign**.

A confirmation message appears. The **Jobs** tab of the **Monitor** page appears with the connection assignment jobs. On the **Assign Connections** tab, click **Refresh** and the job status of the connection changes to **Assigning**. When the connection assignment job is complete, old connections are

unassigned, new connections are assigned, and Metadata Command Center creates links between matching objects in the connected catalog sources.

**Note:** The connection assignment job updates the lineage to reference objects, but the reference objects might still appear as assigned until you re-run the catalog source job.

7. If you see reference objects after the job completes, re-run the catalog source job to update the lineage to the pre-assignment state.

After the connections are modified, Metadata Command Center refreshes the percentage of matched objects versus unmatched objects in the connected catalog sources. After you re-run the catalog source job, the lineage updates to the pre-assignment state.

## Export lists of matched and unmatched objects

After you assign connections to endpoint catalog source objects, there can be both matched and unmatched objects in the catalog. Matched objects are objects that directly match the assigned endpoint objects. Unmatched objects are objects that don't directly match the assigned endpoint objects and are not found in the source system.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, select the required catalog source.  
You can filter the list by catalog source type or recommendations.
3. Click the **Assign Connections** tab.  
Use filters to view the connections based on connection names. Click the **Add Filter** menu to add filters.
4. Select an assigned connection and click **Export** from the **Action** menu.  
A confirmation message appears.
5. Click the link in the confirmation message or navigate to the **Monitor** page and click the required **Job Name**.  
The **Overview** tab appears with the export job details.
6. When the export job completes, click **Download Export File**.

The matched and unmatched objects are downloaded in a list to a Microsoft Excel file. You can use the list of unmatched assets for effective remediation and the list of matched assets for reference.

## Rerunning connections

You can rerun a connection assignment job to resolve failures that occur during connection assignment. When you rerun a connection assignment job, the job reassigns the existing endpoint objects to the selected connection.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab.
2. On the **Catalog Sources** panel, select the required catalog source.  
You can filter the list by a catalog source type or recommendations.
3. Click the **Assign Connections** tab.  
Use filters to view the connections based on connection names. Click the **Add Filter** menu to add filters.

4. Select a connection and click **Rerun Assignment Job** from the **Action** menu.  
A warning message appears.
5. Click **Rerun Assignment Job** to confirm.  
A confirmation message appears. The **Jobs** tab of the **Monitor** page appears with the connection assignment jobs. On the **Assign Connections** tab, click **Refresh** and the job status of the connection changes to **Assigning**.

When the job completes, Metadata Command Center refreshes the percentage of matched objects versus unmatched objects in the connected catalog sources.

## Types of connection scans

Depending on the accuracy and detail of the lineage required, you can choose to run connectionless or connection-aware scans.

### Connectionless scan

Connectionless scans are performed without connection assignment to external source systems. They generate incomplete or inaccurate lineage based on predictions of what the repository might be, instead of actual details that a connection to the databases provides. You run connectionless scans to identify preliminary configuration issues.

### Connection-aware scan

Connection-aware scans retrieve the exact database information from external source systems into the catalog. This external database information is then used to derive complete and accurate column-level lineage for external source systems that include stored procedures and select\* SQL statements. For example, you can extract metadata with an Informatica Intelligent Cloud Services catalog source that connects to an external Oracle source system to generate complete lineage.

To run connection-aware scans, perform the following tasks:

1. If you created catalog sources before the April 2023 release, purge the catalog sources.
2. Create the catalog source, and run the catalog source job.
3. Assign connections or database schemas to the respective catalog sources.  
For example, if you have connections to a source Oracle database and a target Teradata Data Warehouse, assign both source and target connections to the catalog sources that represent the databases.  
If you do not assign a connection to the catalog source, then the catalog source is a referenced catalog source.
4. Run the catalog source job again.

After you perform connection assignment, when you run the scan again, Metadata Command Center passes the actual connection names and database information of the source and target objects that is used to display complete column-level lineage for the catalog source in Data Governance and Catalog.

If you assign multiple catalog sources that use the same connection or endpoint, then Metadata Command Center uses the connection-aware approach to fetch the database information of the assigned catalog sources. If you assign multiple catalog sources that use different connections or endpoints, then Metadata Command Center switches back to the connectionless approach.

If you find reference objects that are not assigned to endpoint objects after a connection-aware scan, choose Delete in the Metadata Change Option when you run the next full scan. This deletes objects that are not included in the scan. If the unassigned reference objects are not included in the scan, they get deleted. You can then run subsequent full or incremental scans without the Delete option.

## CHAPTER 11

# Link catalog sources to generate lineage

You can link catalog sources to generate data lineage based on rules or by generating automated lineage with CLAIRE.

Due to technological limitations or security constraints, you might not always see complete lineage after metadata extraction. You can use Metadata Command Center to link catalog sources and construct data lineage. You can choose source and target catalog sources to link and create lineage. You can also choose source and target objects to restrict lineage inference to specific subsets of data objects within the data sources.

**Note:** You can link only relational databases and file system-based source systems to generate lineage.

You can either generate automated lineage with CLAIRE or define rules to generate catalog source links between assets of the source and target catalog sources.

You can link catalog sources and generate lineage automatically with CLAIRE. You can choose to automatically accept CLAIRE-generated lineage recommendations or manually accept them. CLAIRE-generated lineage recommendations are automatically accepted based on a threshold limit. If the confidence score of the CLAIRE-generated catalog source links between a source and target asset is higher than the configured threshold limit, the recommended links are automatically accepted.

When you define rules to generate lineage, you can use name-based matching or create an inclusion rule with expressions. Name-based matching matches objects based on their names, whereas expressions allow you to construct an inclusion rule. You can specify prefixes and suffixes to omit metadata from the source and target data sets and data elements. This removes extraneous naming conventions, as well as prefixes and suffixes that were added or removed to the asset names while moving data from one source system to another. You can use a combination of attributes, operators, functions, and comments to construct an inclusion rule with expressions.

You can create, view, update, run, delete, or purge a configuration. When you delete a configuration, Metadata Command Center first deletes generated catalog source links and then deletes the configuration. Purging a configuration deletes catalog source links generated from the configuration but retains the configuration. You can also clone a configuration to create another configuration with the same details. You can monitor the jobs that run when you create or perform other tasks on configurations on the **Monitor** page.

The linked assets and catalog source links generated based on rules are auto-accepted by default and appear on the **Catalog Source Links** page in Data Governance and Catalog. Stakeholders of the source and target catalog sources can reject the auto-accepted and manually accepted catalog source links from the **Action** menu. If stakeholders initially reject the generated catalog source links and later accept them, they are marked as accepted in Data Governance and Catalog. Stakeholders can also view the generated lineage on the **Lineage** tab of the asset.



For more information about curation of the generated catalog source links, see *Linked lineage* in Data Governance and Catalog help.

## Prerequisites to link catalog sources

Before you link catalog sources in Metadata Command Center, ensure that you configure and extract metadata from relational database and file system based source systems and enable the **Manage Lineage Settings** feature for the required user roles.

### General prerequisites

Perform the following tasks:

- Configure and run catalog sources that you want to link.
- Verify that metadata is extracted from the catalog sources.
- To generate lineage automatically with CLAIRE, ensure that your administrator allows the use of CLAIRE generative AI services.

### Privileges

To allow users within a user role to link catalog sources, go to Administrator, open the user role, and select the **Manage Lineage Settings** feature on the **Features** tab for the Metadata Command Center service.

For more information about feature privileges, see *Feature privileges* in Introduction and Getting Started.

## Linking catalog sources

Select source and target catalog sources and schemas to link and generate lineage.

Generate automated lineage with CLAIRE or define rules to use name-based matching or construct an inclusion rule with expressions. Save and run the configuration to start a lineage generation job.

### Step 1. Register general information

Provide general information about the configuration on the **Registration** tab.

1. In Metadata Command Center, go to the **Configure** page.
2. Select the **Lineage** tab and then select the **Link Catalog Sources** tab.
3. Click the Add icon.  
The **Registration** tab of the **Link Catalog Sources** page appears.
4. On the **General Information** area, enter a name and an optional description for the configuration.
5. Click **Next**.  
The **Configuration** tab appears.

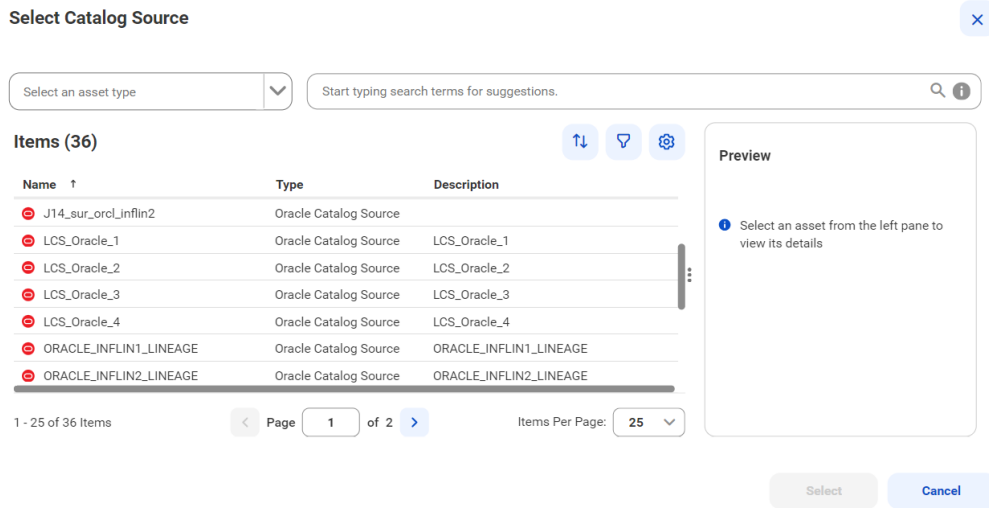
## Step 2. Configure source and target catalog sources

Select source and target catalog sources on the **Configuration** tab.

1. In the **Source Catalog Source** area of the **Configuration** tab, select a source catalog source from which you want to link and generate lineage.

The **Select Catalog Source** dialog box appears.

The following image shows the **Select Catalog Source** dialog box:

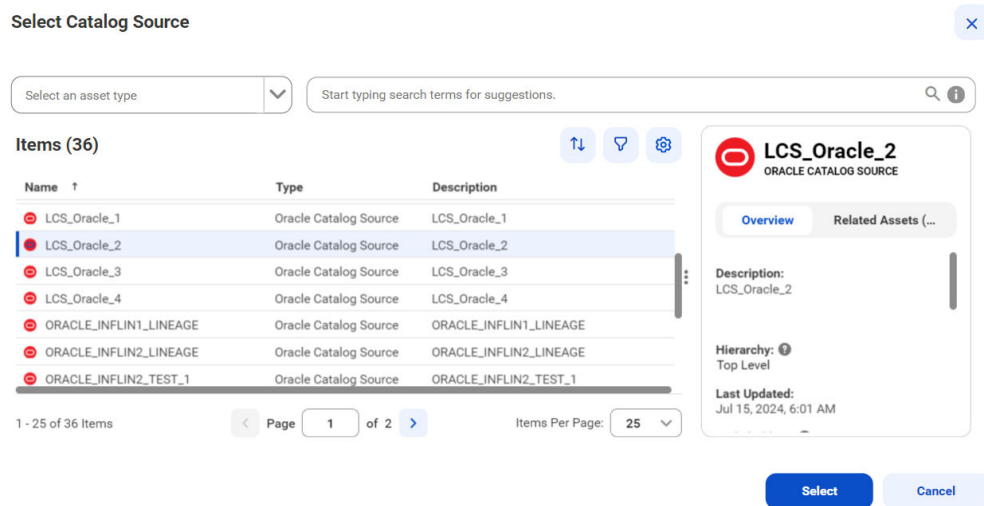


2. Choose a source catalog source and click **Select**.

The overview and related assets of the catalog source appear on the preview pane.

You can filter the list based on the catalog source type and name.

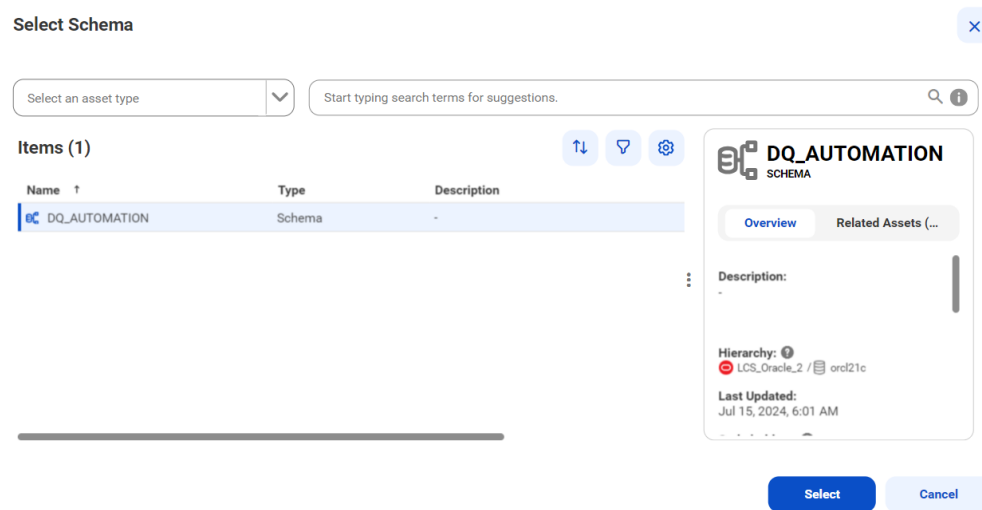
The following image shows a selected source catalog source on the **Select Catalog Source** dialog box:



3. Choose one of the following options from which you want to link and generate lineage:

- **Root Directory.** Select a root directory of the source catalog source. This field appears if you selected a file system-based catalog source.
- **Schema.** Select a schema of the source catalog source. This field appears if you selected a relational database-based catalog source.

The following image shows a selected schema of the source catalog source on the **Select Schema** dialog box:



4. Optional. In the **Filters** area, define one or more filters to apply.

If you selected a relational database-based catalog source, perform the following steps:

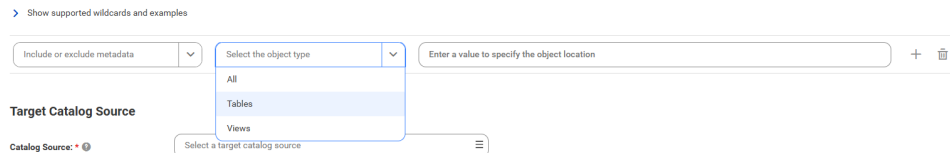
- From the Include or Exclude metadata list, choose to include or exclude metadata based on the filter parameters.
- From the Object type list, select All, Tables, or Views.
- Enter a value to specify the object location.

Filters can contain the following wildcards:

- Question mark. Represents a single character.
- Asterisk. Represents multiple characters.

For object hierarchies, use a dot as a separator. Enclose filter values in double quotes if you use a space or a dot in a single segment.

The following image shows the filter condition options:



For example:

- To include or exclude metadata from all tables with names that begin with 'Table', select **Tables** as the object type and enter `Table*` in the value field.
  - To include or exclude metadata from all columns in the Table1 table, select **Tables** as the object type and enter `Table1.*` in the value field.
  - To include or exclude all objects types from all tables with names that begin with 'Table' followed by a single character, select **All** as the object type and enter `Table?` in the value field.
  - To include or exclude metadata from the 'Table with space' table, select **Tables** as the object type and enter `"Table with space"` in the value field.
- d. To define an additional filter with an OR condition, click the **Add** icon.

If you selected a file system-based catalog source, perform the following steps:

- a. From the Include or Exclude metadata list, choose to include or exclude metadata based on the filter parameters.
- b. Enter a value to specify the object location.

Filters are case-insensitive.

Filters can contain asterisk as a wildcard to represent multiple characters.

Use the following rules when you enter filter values:

- Use an asterisk as a path placeholder as shown in the following example: `folder1/*/folder3`. Here, the filter includes all folders under `folder1`.
- Use two asterisks in the path filter to indicate zero or more levels of folders. The pattern with two asterisks is recursive. The processing time is longer as the data volume increases.
- For path hierarchies, use `'/'` as a separator. You can provide a path in the folder and path filters but not in the file filter.
- To include or exclude metadata from a file, specify only the file name.

The following image shows the filter condition options:

[Show supported wildcards and examples](#)

Include or exclude metadata	Path	Enter a value to specify the object location	+	⌵
-----------------------------	------	--	---	---

Path filters apply to the files and folders in the path that you filter. The path filter is non-recursive. If you provide only the file or folder names, the path filters apply on the first level files or directories.

For example:

- To include or exclude metadata from files and folders with names that start with 'Item1' in the first level directory, enter `Item1*` in the value field.
- To include or exclude metadata from the 'File1' file in the 'Folder1' folder, enter `Folder1/File1` in the value field.
- To include or exclude metadata from files or folders with names that contain the word 'Subfolder' in the 'Folder1' folder, enter `Folder1/*Subfolder*` in the value field.
- To include or exclude metadata from files or folders with the name 'File1' in any subfolder of the 'Folder1' folder, enter `Folder1/*/File1` in the value field.
- To include or exclude metadata from all files and subfolders in the 'Folder1' folder, enter `Folder1/*` in the value field.
- To include or exclude metadata from files or folders with the name 'File1' located at any level in the 'Folder1' folder, enter `Folder1/**/File1` in the value field. This is a recursive search, and therefore the processing time can be longer.

- c. To define an additional filter with an OR condition, click the **Add** icon.

**Note:** If you add a filter that includes metadata from all objects, or if you don't add a filter, Metadata Command Center generates additional lineage for a few objects. These objects might include parameter containers, result sets, stages, and other objects that belong to the `core.DataSet` super class within the metadata model.

5. In the **Target Catalog Source** area, select a target catalog source and schema or root directory to which you want to link and generate lineage. Optionally, you can add a filter.
6. Click **Next**.

The **Rule Definition** tab appears.

## Step 3. Perform rule-based or automated linking, save, and run the configuration

Generate automated lineage with CLAIRE or define rules to use name-based matching or construct an inclusion rule with expressions on the **Linking Method** tab.

1. On the **Linking Method** tab, choose to either generate automated lineage with CLAIRE or define rules to generate catalog source links between assets of the source and target catalog sources.
2. To refresh catalog source links whenever the source or target catalog source job is run, click **Refresh Lineage**.
3. Choose one of following linking methods:
  - **Rule-based Linking**. Define rules to use name-based matching or construct an inclusion rule with expressions.
  - **Automated Linking**. Generate lineage automatically with CLAIRE.

**Note:** This linking method is not applicable for file system-based source or target catalog sources.
4. If you choose the **Automated Linking** option, you can either automatically accept CLAIRE-generated lineage recommendations or manually accept them.

The following table describes the properties that you can enter for automated linking:

Property	Description
Enable auto-acceptance	Select to automatically accept CLAIRE-generated lineage recommendations. If disabled, you must manually accept the lineage recommendations.
Confidence Score Threshold for Auto-Acceptance	If you enable auto-acceptance, specify a threshold limit based on which the CLAIRE-generated lineage recommendations are automatically accepted. Specify a percentage from 80 to 100. If the confidence score of the catalog source links generated between a source and target asset is higher than the configured threshold limit, the recommended links are automatically accepted. Default is 95%.

Stakeholders of the source and target catalog sources can reject the auto-accepted and manually accepted catalog source links generated by CLAIRE in Data Governance and Catalog.

5. If you choose the **Rule-based Linking** option, choose the rule type.
  - **Name Matching**. Ignores specified prefixes and suffixes of an asset name and matches the rest of the asset name to generate catalog source links.
  - **Expression**. Constructs an inclusion rule using expressions. Use a combination of attributes, operators, functions, or comments to build an inclusion rule.
6. If you choose the **Name Matching** rule type, select the asset types to specify prefix and suffix strings to ignore.

The following table describes the properties that you can enter for name matching:

Property	Description
Source Data Set - Ignore Prefix	Specify the prefix of source data set names to ignore and match the rest of the source data set names with target data set names.
Source Data Set - Ignore Suffix	Specify the suffix of source data set names to ignore and match the rest of the source data set names with target data set names.
Target Data Set - Ignore Prefix	Specify the prefix of target data set names to ignore and match the rest of the target data set names with source data set names.
Target Data Set - Ignore Suffix	Specify the suffix of target data set names to ignore and match the rest of the target data set names with source data set names.
Source Data Element - Ignore Prefix	Specify the prefix of source data element names to ignore and match the rest of the source data element names with target data element names.
Source Data Element - Ignore Suffix	Specify the suffix of source data element names to ignore and match the rest of the source data element names with target data element names.
Target Data Element - Ignore Prefix	Specify the prefix of target data element names to ignore and match the rest of the target data element names with source data element names.
Target Data Element - Ignore Suffix	Specify the suffix of target data element names to ignore and match the rest of the target data element names with source data element names.

Prefixes and suffixes that you specify can contain alphanumeric characters, underscore (\_), and hyphen (-).

For example:

- To match the source data set, "STG\_CUSTOMER", with the target data set, "CUSTOMER", specify "STG\_" in the Ignore Prefix field for the source data set.
- To match the target data set, "TMP\_ACCOUNT\_STG", with the source data set, "ACCOUNT", specify "TMP\_" in the Ignore Prefix and "\_STG" in the Ignore Suffix fields for the target data set.
- To match the source data element, "CUSTOMER\_LND", with the target data element, "CUSTOMER", specify "\_LND" in the Ignore Suffix field for the source data element.
- To match the target data element, "TMP\_CUSTOMER\_LND", with the source data element, "CUSTOMER", specify "TMP\_" in the Ignore Prefix and "\_LND" in the Ignore Suffix fields for the target data element.

**Note:** If you don't select an asset type, you can't enter a prefix or suffix. In such cases, the lineage generation job searches for and matches exact source and target asset names.

7. If you choose the **Expression** rule type, construct an inclusion rule using expressions.

You can use a combination of attributes, operators, functions, and comments to define an inclusion rule. You can type your expressions directly and view autocompleted suggestions as you enter your expression in the editor. Expressions are created using a Spark SQL-based language. Expression values cannot exceed 5000 characters.

You can use the following components to construct an inclusion rule:

- **Attributes:** Attributes can be values that you obtain from the catalog. Values are case-sensitive.

You can use the following attributes:

- Source data set. For example: `srcDataSet.name == 'Customer'`
- Source data element. For example: `srcDataElement.name == 'email'`
- Source data set relative path.  
For example: `srcDataSet.relativePath == 'Folder1/Folder2/File.csv'`
- Target data set. For example: `tgtDataSet.name == 'employee'`
- Target data element. For example: `tgtDataElement.name == 'Age'`
- Target data set relative path.  
For example: `tgtDataSet.relativePath == 'Folder1/Folder2/File.csv'`

- **Operators:** Use operators to compare values of columns. For example, you can use an equality operator to check if the names of two columns are the same.  
For example: `tgtDataElement.name == ('MANAGER' || 'ID')`
- **Functions:** Use functions to calculate values and manipulate data. For example, a function can be changing a name to all upper case or lower case using the `upper` or `lower` functions.  
Other supported functions include, but are not limited to:

- `replace`
- `regexp_replace`
- `regexp_match`
- `substring`
- `length`

For example: `replace('EMPLOYEE', 'oyee', 'OYEE')`

- **Comments:** Use comments to summarize the constructed inclusion rule.  
For example: `/* source data element is changed to lowercase */`

Example of a valid inclusion rule:

```
srcDataElement.name == tgtDataElement.name and srcDataSet.name == tgtDataSet.name  
/* The source data element name must be the same as the target data element name, and the  
source data set name must be the same as the target data set name. */
```

**Important:** Construct expressions with both data sets and data elements to avoid generating unnecessary catalog source links.

8. Click **Validate** to validate your expression.

If the validation is successful, a success message appears.

9. To save and run the configuration, click **Save** and then **Run**.

A Lineage Generation job is created to link catalog sources and to generate catalog source links. Check the status of the job on the **Monitor** page.

# Manage configurations

You can view, update, run, copy, delete, or purge a configuration.

The following table describes the properties on the **Link Catalog Sources** tab of the **Configure** page:

Field	Description
Name	The name of the configuration.
Description	The description of the configuration.
Source Catalog Source	The source catalog source from which you want to link and generate lineage.
Target Catalog Source	The target catalog source to which you want to link and generate lineage.
Owners	The owners or stakeholders of the configuration.
Last Run By	The name of the user who started the last job.
Last Job Type	The type of job that was last run. It can be one of the following job types: <ul style="list-style-type: none"><li>- Lineage Generation</li><li>- Lineage Purging</li><li>- Lineage Deletion</li></ul>
Last Job Status	The status of the last run job. It can be one of the following job statuses: <ul style="list-style-type: none"><li>- Starting</li><li>- Completed</li><li>- Completed with Errors</li><li>- Running</li><li>- Failed</li><li>- Canceled</li></ul>

## Delete or purge a configuration

Delete or purge a configuration based on your business requirements. When you delete a configuration, Metadata Command Center first deletes generated catalog source links and then deletes the configuration. Purging a configuration deletes catalog source links generated from the configuration but retains the configuration.

1. In Metadata Command Center, go to the **Configure** page.
2. Select the **Lineage** tab and then select the **Link Catalog Sources** tab.
3. From the list of configurations, select the configuration that you want to delete or purge.
4. You can delete or purge a configuration in one of the following ways:
  - Right-click the configuration and click **Delete** or **Purge**.
  - Click the **Action** menu and click **Delete** or **Purge**.

**Note:** You can't delete or purge a configuration if the lineage generation job is in the running state.

5. To confirm delete or purge, click **Delete** or **Purge** on the warning message.

A Lineage Deletion job is initiated to delete and a Lineage Purging job is initiated to purge. You can monitor the status of the jobs on the **Monitor** page.



## Clone a configuration

You can clone a configuration to create another configuration with the same details.

**Note:** Cloning doesn't copy the catalog source links generated by the configuration.

1. In Metadata Command Center, go to the **Configure** page.
2. Select the **Lineage** tab and then select the **Link Catalog Sources** tab.
3. From the list of configurations, select the configuration that you want to clone.
4. You can clone a configuration in one of the following ways:
  - Right-click the configuration and click **Clone**.
  - Click the **Action** menu and click **Clone**.
  - Open the configuration and click **Clone**.

**Note:** By default, the cloned configuration has the same name suffixed with \_Clone. You can change the name if needed.

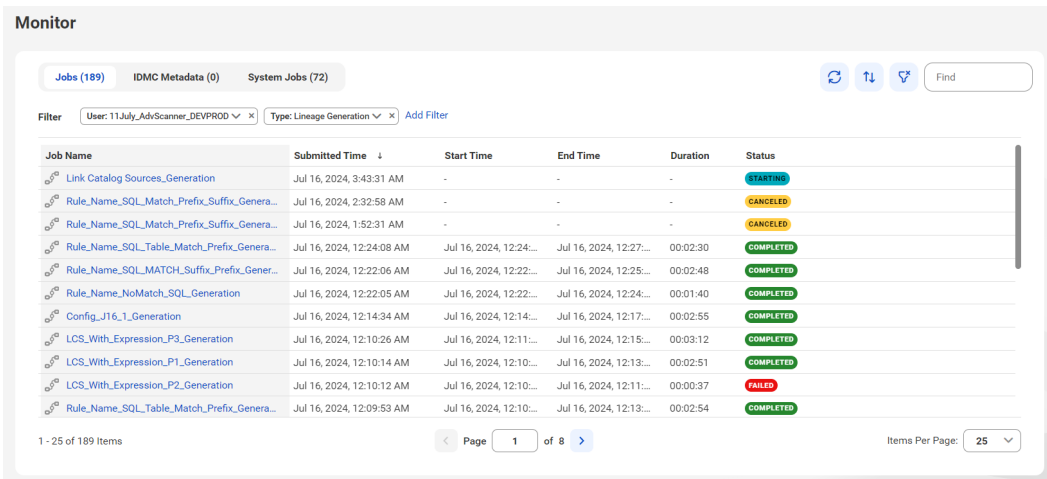
5. If needed, modify the configuration by updating the properties on each tab.
6. To save and run the configuration, click **Save** and then **Run**.

A Lineage Generation job is created to link catalog sources and to generate catalog source links. Check the status of the job on the **Monitor** page.

## Monitor lineage generation jobs

You can view the status of Lineage Generation, Lineage Purging, and Lineage Deletion jobs on the **Monitor** page in Metadata Command Center.

The following image shows the Lineage Generation jobs on the **Jobs** tab of the **Monitor** page:



The screenshot shows the 'Monitor' page with the 'Jobs' tab selected. The page displays a list of jobs with columns for Job Name, Submitted Time, Start Time, End Time, Duration, and Status. The jobs are filtered by 'User: 11July\_AdvScanner\_DEVPROD' and 'Type: Lineage Generation'. The status of the jobs is indicated by colored buttons: 'STARTING' (blue), 'CANCELED' (yellow), and 'COMPLETED' (green). The 'LCS\_With\_Expression\_P1\_Generation' job is marked as 'FAILED' (red).

Job Name	Submitted Time	Start Time	End Time	Duration	Status
Link Catalog Sources_Generation	Jul 16, 2024, 3:43:31 AM	-	-	-	STARTING
Rule_Name_SQL_Match_Prefix_Suffix_Genera...	Jul 16, 2024, 2:32:58 AM	-	-	-	CANCELED
Rule_Name_SQL_Match_Prefix_Suffix_Genera...	Jul 16, 2024, 1:52:31 AM	-	-	-	CANCELED
Rule_Name_SQL_Table_Match_Prefix_Genera...	Jul 16, 2024, 12:24:08 AM	Jul 16, 2024, 12:24:...	Jul 16, 2024, 12:27:...	00:02:30	COMPLETED
Rule_Name_SQL_MATCH_Suffix_Prefix_Gener...	Jul 16, 2024, 12:22:06 AM	Jul 16, 2024, 12:22:...	Jul 16, 2024, 12:25:...	00:02:48	COMPLETED
Rule_Name_NoMatch_SQL_Generation	Jul 16, 2024, 12:22:05 AM	Jul 16, 2024, 12:22:...	Jul 16, 2024, 12:24:...	00:01:40	COMPLETED
Config_J16_1_Generation	Jul 16, 2024, 12:14:34 AM	Jul 16, 2024, 12:14:...	Jul 16, 2024, 12:17:...	00:02:55	COMPLETED
LCS_With_Expression_P3_Generation	Jul 16, 2024, 12:10:26 AM	Jul 16, 2024, 12:11:...	Jul 16, 2024, 12:15:...	00:03:12	COMPLETED
LCS_With_Expression_P1_Generation	Jul 16, 2024, 12:10:14 AM	Jul 16, 2024, 12:10:...	Jul 16, 2024, 12:13:...	00:02:51	COMPLETED
LCS_With_Expression_P2_Generation	Jul 16, 2024, 12:10:12 AM	Jul 16, 2024, 12:10:...	Jul 16, 2024, 12:11:...	00:00:37	FAILED
Rule_Name_SQL_Table_Match_Prefix_Genera...	Jul 16, 2024, 12:09:53 AM	Jul 16, 2024, 12:10:...	Jul 16, 2024, 12:13:...	00:02:54	COMPLETED

To cancel an ongoing job, hover the mouse over the job and click **Cancel Job** from the **Action** menu. Click the job name to open the **Overview** and **Logs** tabs for more details about the job. The **Logs** page for a job displays detailed logs for each task that was run in the job.

You can view the status of the following jobs on the **Monitor** page:

### Lineage Generation jobs

A Lineage Generation job creates links between source and target assets and generates data lineage based on rules defined in the configuration. The **Overview** tab lists the tasks and the count of catalog source links generated and inserted into the catalog.

A Lineage Generation job consists of the following tasks:

- Bulk Ingestion. The **Results** tab of a Bulk Ingestion task displays the statistics of the linked data sets and data elements. Click the count to see the linked assets on the **Catalog Source Links** page in Data Governance and Catalog.
- Lineage Link Generation. The **Results** tab of a Lineage Link Generation task displays the statistics of the linked data sets and data elements inserted and updated into the catalog.

**Note:** When you link catalog sources, incomplete catalog source links are generated if the source or target catalog source contains a reference data element.

### Lineage Purging jobs

A Lineage Purging job deletes catalog source links generated from the configuration but doesn't delete the configuration. The **Overview** tab lists the tasks and the purging results.

### Lineage Deletion jobs

A Lineage Deletion job first deletes generated catalog source links and then deletes the configuration. The **Overview** tab lists the tasks and the deletion results.

For more information about monitoring jobs, see [“Monitor jobs for technical assets” on page 162](#).

## CHAPTER 12

# Asset customization

You can customize the attributes that are associated with one or more assets, and even modify the types of relationships that can be created between assets in Data Governance and Catalog.

In Metadata Command Center, you can modify or delete the attributes that are predefined for the Data Governance and Catalog assets. If the predefined attributes of an asset prove to be insufficient, you can create new custom attributes. You can also modify or delete the attributes that you created.

For assets that can be related to each other, you can add new relationship types or modify or remove existing relationship types. This allows you to accurately represent the relationships between assets according to how the associations are defined in your organization.

When you modify the attributes or the relationship types for assets, your changes affect dashboards, data lineages, Data Governance and Catalog APIs and the bulk import templates. To ensure that the users in your organization are able to perform governance tasks seamlessly, consider apprising them on your customizations.

## Manage attributes

Attributes are properties that capture information about an asset. You can modify or delete the predefined attributes of an asset. You can also create new attributes to capture additional information about an asset.

Predefined attributes and the attributes that you create are displayed in Data Governance and Catalog when a user creates an asset. For example, in Metadata Command Center, you can create a new attribute called **Department** with the allowed values of `HR`, `Finance`, `Sales`, or `Marketing`. Based on the selected asset type, the **Department** field appears while creating a new asset in Data Governance and Catalog, where you can enter or select any one of the allowed values. You can then use this attribute to filter your search for employees only in the HR department.

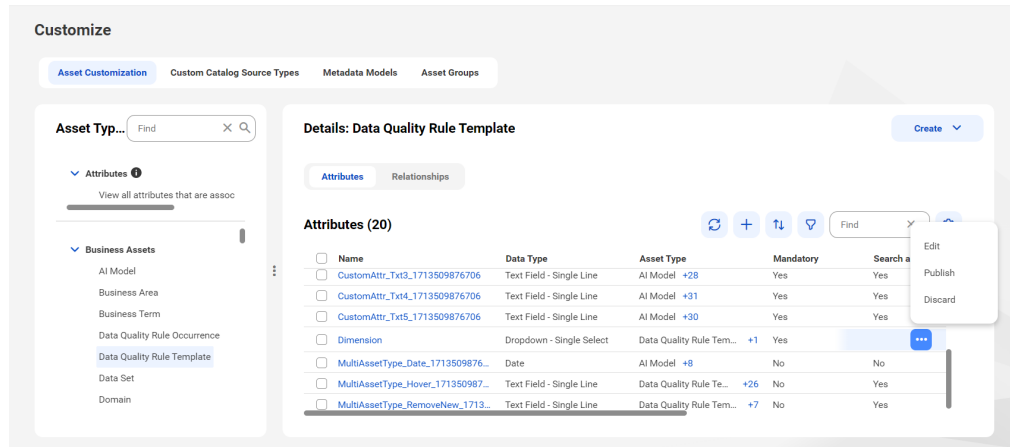
You can create custom attributes for predefined catalog sources. On the **Customize > Asset Customization** tab in Metadata Command Center, you can create, modify, or delete attributes for all asset types.

To have permissions to create, modify, or delete attributes, define appropriate roles and select the **Manage Custom Attributes** feature for that role when you configure privileges in Metadata Command Center in Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

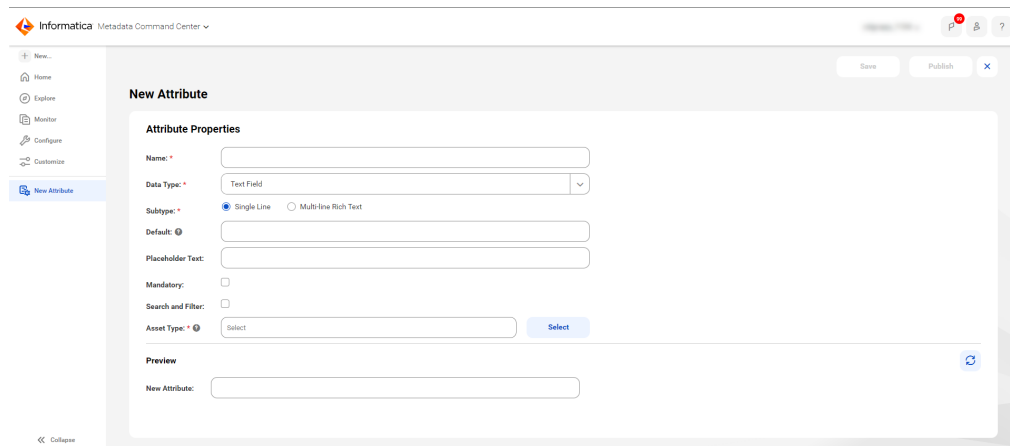
## Creating attributes

To create a new custom attribute, specify a name and data type, and select the asset type for which you want to create the attribute. You can also specify if you want to make the new attribute mandatory and searchable for a particular asset type.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select an asset type.
3. For the selected asset type, open the **Attributes** tab.



4. Click the **Add** icon.  
Alternatively, you can use the **Create** button to add a new attribute.



5. Configure the following properties of the new attribute:

Property	Description
Name	Unique name for the attribute that will be displayed in Data Governance and Catalog. Ensure that the attribute name doesn't match a name that already exists.

Property	Description
Data Type	<p>The type of value that users can enter in the attribute. You can choose one of the following data types:</p> <ul style="list-style-type: none"> <li>• <b>Text Field.</b> Allows string values.</li> <li>• <b>Numeric Value.</b> Allows an integer or a decimal value.</li> <li>• <b>Dropdown List.</b> Allows to select values from the list of values.</li> <li>• <b>Boolean/Check Box.</b> Allows to select one of two mutually exclusive options.</li> <li>• <b>Date Field.</b> Allows to select a date.</li> <li>• <b>URL Field.</b> Allows a URL or a hyperlinked label.</li> </ul> <p>Default value is <b>Text Field</b>.</p>
Subtype	Select a subtype based on the data type that you selected.
Default Value	<p>The value that should appear in the field by default.</p> <p>Consider using a maximum of 15 characters when specifying the default value.</p>
Placeholder Text	A description that informs the user about the purpose of the attribute.
Mandatory	Determines whether the field is mandatory or optional. Click <b>Mandatory</b> to create a mandatory field.
Search and Filter	<p>Determines whether you can use the attribute as search and filter criteria in Data Governance and Catalog. Additionally, this field also allows you to view the assets that will be impacted when you try to delete an attribute.</p> <p>This field is enabled by default.</p> <p><b>Note:</b> If you disable this field, you can't delete the attribute until you enable it again.</p> <p>For more information about how a user can search for assets, see the <i>Asset Discovery</i> help in Data Governance and Catalog.</p>
Asset Type	<p>The asset type in Data Governance and Catalog for which you want to create this attribute. You can select asset types in the following categories:</p> <ul style="list-style-type: none"> <li>• Business asset.</li> <li>• Data Marketplace asset.</li> </ul> <p><b>Note:</b> If you select a Data Marketplace asset type, ensure that you don't specify <b>URL Field</b> as the <b>Data Type</b>.</p> <ul style="list-style-type: none"> <li>• Technical asset. You choose technical asset types for each catalog source.</li> </ul> <p><b>Note:</b> Asset type hierarchy is a class inheritance hierarchy. If you select a superclass asset type, the subclass asset types also get selected.</p> <p>For more information about selecting asset types, see <a href="#">"Configuring asset types for attributes" on page 93</a>.</p>

6. Click **Save**.

This creates a draft version of the new attribute that you can view in the attributes list on the **Attributes** tab.

7. Click the name of the attribute that you saved to view and verify the details of the attribute. To modify the properties of the attribute, edit the values and click **Save**.

**Note:** If you do not want to proceed with your changes, use the **Discard** icon to discard the draft version of the attribute. You can also perform this action from the Action menu on the **Asset Customization > Attributes** tab of the **Customize** page. On the **Asset Customization > Attributes** tab, you can also discard

the draft version of multiple attributes. To do this, select the attributes for which you want to discard the draft state and click the **Discard** icon from the Action menu.

- Click **Publish** to publish the attribute in Data Governance and Catalog.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To publish the attribute, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

After the publishing is successful, the lifecycle state of the attribute changes from **Draft** to **Published**.

The new attribute appears when a user creates an object for the selected asset type in Data Governance and Catalog. Based on the data type that you selected, the user can enter an appropriate value for the custom attribute.

## Modifying attributes

You can modify a predefined attribute or a custom attribute that you created.

- On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
- In the **Asset Types** panel, select an asset type.
- For the selected asset type, go to the **Attributes** tab.
- On the **Attributes** tab, click the Action menu next to an attribute and select **Edit**.

The screenshot shows the 'Customize' interface with the 'Asset Customization' tab selected. On the left, the 'Asset Types' panel lists various asset types, with 'Data Quality Rule Template' highlighted. The main area shows the 'Attributes' tab for this asset type, displaying a table of attributes. An action menu is open for the attribute 'CustomAttr\_Txt4\_1713509876706', showing options like 'Edit', 'Publish', and 'Discard'.

Name	Data Type	Asset Type	Mandatory	Searchable
CustomAttr_Txt3_1713509876706	Text Field - Single Line	AI Model +28	Yes	Yes
CustomAttr_Txt4_1713509876706	Text Field - Single Line	AI Model +31	Yes	Yes
CustomAttr_Txt5_1713509876706	Text Field - Single Line	AI Model +30	Yes	Yes
Dimension	Dropdown - Single Select	Data Quality Rule Tem... +1	Yes	Yes
MultiAssetType_Date_1713509876...	Date	AI Model +8	No	No
MultiAssetType_Hover_171350987...	Text Field - Single Line	Data Quality Rule Te... +26	No	Yes
MultiAssetType_RemoveNew_1713...	Text Field - Single Line	Data Quality Rule Tem... +7	No	Yes

- On the **Attributes** tab, select the attribute that you want to modify.  
You can use filters to assist you in your search for attributes. You can also use filters to view only the predefined attributes for an asset type, or to view only the custom attributes for an asset type.
- Depending on the lifecycle state of the attribute, choose one of the following options:
  - If the attribute is in the Draft state, you can modify any property of the attribute.
  - If the attribute is in the Published state, open the attribute and click **Create a draft**. You can modify only some of its properties.

When you modify an attribute, you can modify its associated asset types and also configure its acceptable values. For more information about how you can modify the asset type associated with an attribute, see [“Configuring asset types for attributes” on page 93](#). For more information about how you can configure the acceptable values for an attribute, see [“Configuring dropdown values” on page 91](#).

**Note:** You can configure a non-searchable attribute to be searchable. However, you can't configure a searchable attribute to be non-searchable.

- Click **Save**.

**Note:** If you do not want to proceed with your changes, you can use the **Discard** icon to discard the draft version of the attribute. You can also perform this action from the Action menu on the **Asset Customization > Attributes** tab of the **Customize** page. On the **Asset Customization > Attributes** tab, you can also discard the draft version of multiple attributes. To do this, select the attributes for which you want to discard the draft state and click the **Discard** icon from the Action menu.

- Click **Publish** to publish your changes.

You can also perform this action from the Action menu on the **Asset Customization > Attributes** tab of the **Customize** page. On the **Asset Customization > Attributes** tab, you can also publish multiple attributes. To do this, select the attributes that you want to publish and click the **Publish** button from the Action menu.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

The status of the attribute changes to Published and the modified attribute appears in Data Governance and Catalog.

- After the publish job is completed, ensure that you refresh the web page on your browser to view your changes to the attribute.

## Configuring dropdown values

For an attribute of the dropdown data type, you can create, modify or remove the acceptable dropdown values when the attribute is in a Draft state.

- On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
- In the **Asset Types** panel, select an asset type.
- For the selected asset type, go to the **Attributes** tab.
- On the **Attributes** tab, click the Action menu next to an attribute and select **Edit**.

The screenshot shows the 'Customize' page with the 'Asset Customization' tab selected. On the left, the 'Asset Types' panel shows 'Data Quality Rule Template' selected. The main area displays the 'Attributes (20)' table. The table has the following columns: Name, Data Type, Asset Type, Mandatory, Searchable, and Actions. The 'Actions' column contains an 'Edit' icon (three dots) for the selected attribute 'CustomAttr\_Txt4\_1713509876706'. A dropdown menu is open for this attribute, showing options: Edit, Publish, and Discard.

Name	Data Type	Asset Type	Mandatory	Searchable	Actions
CustomAttr_Txt3_1713509876706	Text Field - Single Line	AI Model +28	Yes	Yes	...
CustomAttr_Txt4_1713509876706	Text Field - Single Line	AI Model +31	Yes	Yes	...
CustomAttr_Txt5_1713509876706	Text Field - Single Line	AI Model +30	Yes	Yes	...
Dimension	Dropdown - Single Select	Data Quality Rule Tem... +1	Yes	Yes	...
MultiAssetType_Date_1713509876...	Date	AI Model +8	No	No	...
MultiAssetType_Hover_171350987...	Text Field - Single Line	Data Quality Rule Te... +26	No	Yes	...
MultiAssetType_RemoveNew_1713...	Text Field - Single Line	Data Quality Rule Tem... +7	No	Yes	...

- To add a new value, click the **Add** icon in the **Values** field and enter the new value.

When you configure a new value, consider using a maximum 15 characters.

**Note:** If you are adding new sensitivity levels or dimensions, consider the following:

- For the Sensitivity Level attribute that is available for data element classifications, you can configure a maximum of 10 values in addition to the immutable value `None`. Furthermore, when you add new sensitivity levels, ensure that you enter the values from top to bottom in increasing order of sensitivity.
- For the Dimension attribute that is available for data quality rule template and data quality rule occurrence asset types, you can configure a maximum of 12 values.

**Dimension**

**Attribute Properties**

Name: \* Dimension

Data Type: \* Dropdown List

Subtype: \* Single Select

Values: \* 6

Default	Value
<input checked="" type="radio"/>	Accuracy
<input type="radio"/>	Validity
<input type="radio"/>	Completeness
<input checked="" type="radio"/>	Cleanliness
<input type="radio"/>	Uniqueness
<input type="radio"/>	Timeliness

Placeholder Text: One of the six data quality dimensions that applies to the data quality rule occurrence.

Mandatory: Yes

Search and Filter: Yes

Asset Type: \* Data Quality Rule Template Data Quality Rule Occurrence

**Preview**

Dimension: \* Cleanliness

6. To modify an existing value, click the value that you want to modify in the **Values** field .

**Note:**

- If you modify a value, you can't add the old value again as a separate value. For example, consider the Dimension attribute that is available for data quality rule template. You add a new dimension called `Compliance`. Later, you modify the newly added dimension to `Relativeness`. Now, if you try to add a new dimension called `Compliance`, the system will display an error. To add the dimension `Compliance` back to the list, you must either rename the dimension value that was originally labelled as `Compliance` or delete that value.
  - If you modify a dropdown value, the updated list of dropdown values will be available only to the new assets that you create. Your changes won't apply to an existing asset that uses the attribute.
  - For the Sensitivity Level attribute that is available for data element classifications, you can't modify the sensitivity level value `None`.
7. To modify the position of a value, click the navigational arrows next to the value.
- Note:** For the Sensitivity Level attribute that is available for data element classifications, you can't modify the position of the sensitivity level value `None`.
8. To remove an existing value, click the Delete icon next to the value that you want to remove from the **Values** field .



**Note:**

- If a dropdown value is already used by one or more Data Governance and Catalog assets, you can't delete the value until you remove it from the relevant assets.
- For the Sensitivity Level attribute that is available for data element classifications, you can configure a minimum of 3 values including the immutable value `None`. Additionally, you can't remove the sensitivity level value `None`.

9. Click **Save** and then click **Publish** to publish your changes.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

After the publishing is successful, the lifecycle state of the attribute changes from **Draft** to **Published**.

## View asset types for attributes

You can view all asset types assigned to an attribute. You can search for an asset type by name.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select an asset type.
3. For the selected asset type, go to the **Attributes** tab.
4. On the **Attributes** tab, select an attribute.
5. If an attribute has more than one asset type, hover over the **+<number of asset types>** icon in the **Asset Type** column to view the assets types in a pop up.
6. If an attribute has more than 20 asset types, click **Show All** to view all asset types.

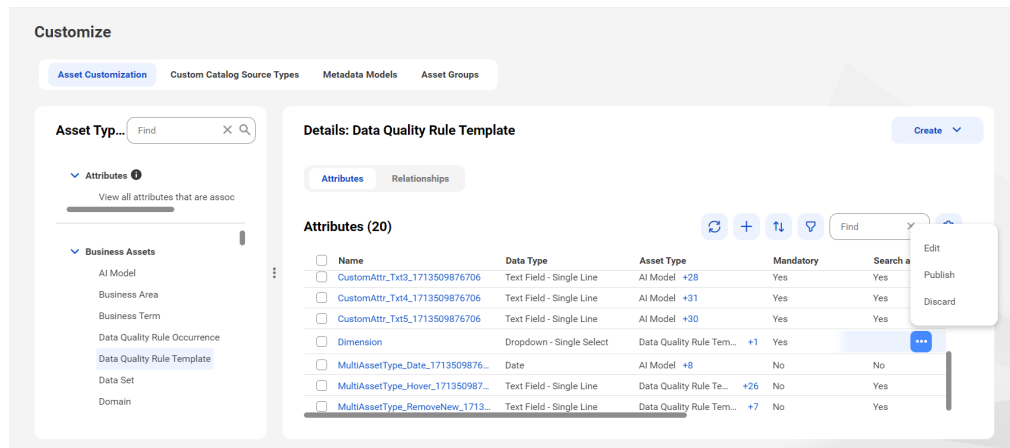
The **All Asset Types** dialog box appears.

7. Use the navigation and search options to find an asset type.
8. Click **Close** to return to the **Attributes** tab.

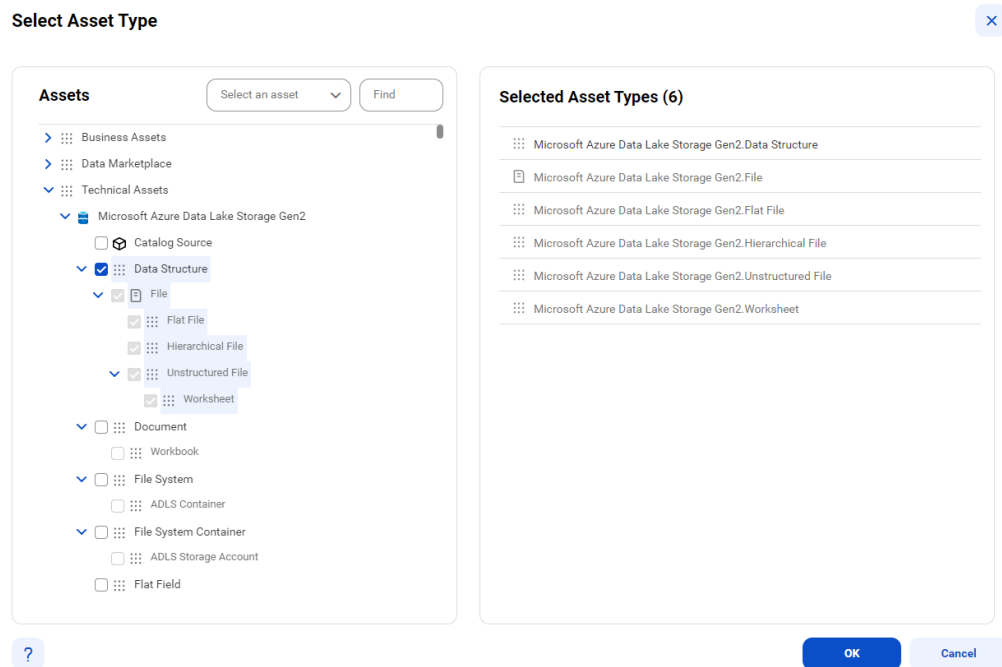
## Configuring asset types for attributes

You can add or remove the asset types for an attribute based on class inheritance rules when the attribute is in a Draft state.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select an asset type.
3. For the selected asset type, go to the **Attributes** tab.
4. On the **Attributes** tab, click the Action menu next to an attribute and select **Edit**.



- Click **Select** next to the **Asset Type** field.



- In the **Select Asset Type** dialog box, add or remove the asset types based on the rules of class inheritance.

If you select a superclass asset type, such as Data Structure, the subclass asset type File also gets selected.

Selected asset types appear in the right panel.

- Click **Save**.

8. Click **Publish** to publish your changes.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

After the publishing is successful, the lifecycle state of the attribute changes from **Draft** to **Published**.

If you added a predefined attribute to an asset type that isn't conventionally associated with the attribute, you must manually add the attribute to the custom layouts that you have created. For more information about custom layouts, see [Chapter 13, "Custom layouts" on page 102](#).

## Deleting attributes

If an attribute is no longer relevant to the asset type or if you want to modify the properties of an attribute, you can delete the attribute and create a new attribute. Deleting an attribute removes the attribute in Data Governance and Catalog along with all the values that are defined for this attribute for any asset.

To manage create, delete, or modify attributes, define appropriate roles and select the **Manage Custom Attributes** feature for that role when configuring privileges for the Metadata Command Center service in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

1. On the **Customize** page, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select an asset type.
3. For the selected asset type, go to the **Attributes** tab.

You can use filters to assist you in your search for attributes. You can also use filters to view only the predefined attributes for an asset type, or to view only the custom attributes for an asset type.

The screenshot shows the 'Customize' page with the 'Asset Customization' tab selected. On the left, the 'Asset Types' panel shows 'Data Quality Rule Occurrence' selected. The main area displays the 'Attributes' tab for this asset type, showing a table of 20 attributes. A context menu is open over the table, showing options: Edit, Publish, Discard, and Delete. The 'Delete' option is highlighted in blue.

Name	Data Type	Asset Type	Mandatory	Searchable
CustomAttr_Boolean_Y_17135098...	Boolean	Data Quality Rule Te...	+29 Yes	Yes
CustomAttr_Chkbox_1713509876706	Boolean	Data Quality Rule Te...	+29 No	No
CustomAttr_Date_1713509876706	Date	Data Quality Rule Te...	+28 No	Yes
CustomAttr_Drpdown_17135098767...	Dropdown - Multi Select	Data Quality Rule Te...	+30 No	Yes
CustomAttr_Drpdown_Single_17135...	Dropdown - Single Select	Data Quality Rule Te...	+29 Yes	No

4. Select the check box for one or more attributes.

**Note:** You can delete only some of the predefined attributes available for an asset type. For example, you can't delete the Dimension attribute for data quality rule template and data quality rule occurrence asset types.

5. Click the Action menu for any of the selected attributes and click **Delete**.

If you have selected more than one attribute to delete, then the Action menu for the selected group appears only if all the attributes in the group are in the **Published** or **Published with draft available** lifecycle states.

**Note:** If you haven't marked an attribute as searchable, then you can't delete the attribute until you enable the **Search and Filter** property for it.

6. Click **Delete** to confirm.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To delete the attribute, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

After the publishing is successful, the lifecycle state of the attribute changes from **Draft** to **Published**.

## Customize relationship types

A relationship between assets depicts how the assets relate to each another. In Data Governance and Catalog, you can use different types of relationships to connect business assets to each other and to relevant technical assets.

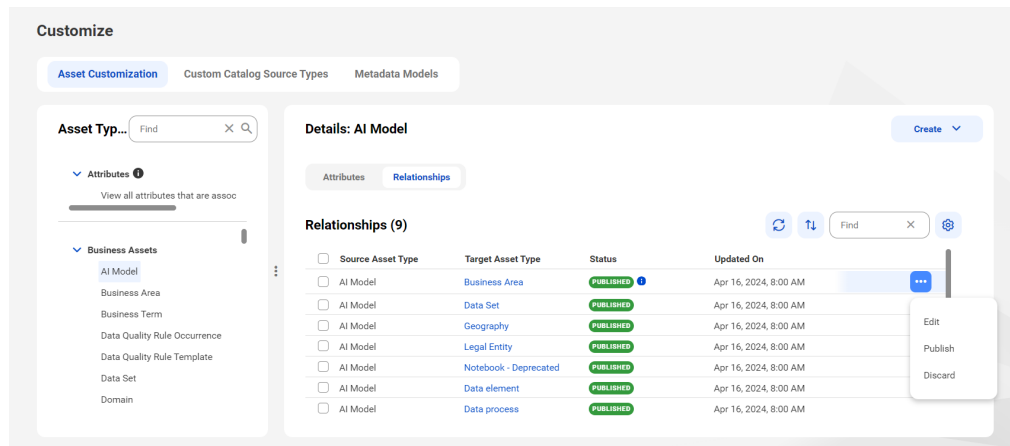
In Metadata Command Center, you can add new relationship types or modify or remove existing relationship types for assets that can be related to each other. You can't create a new relationship between assets that have no predefined relationship with one another. For more information about how assets relate to each other, see the *Asset Discovery* help for Data Governance and Catalog.

### Modifying relationship types

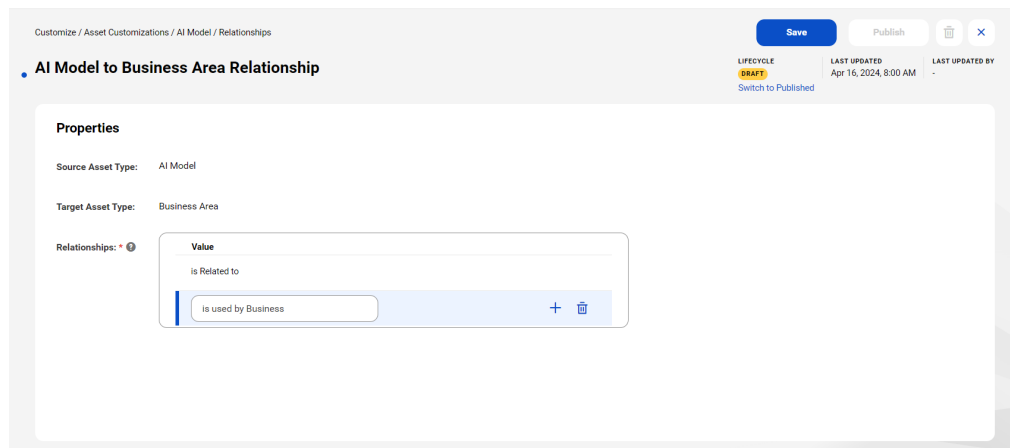
You can add, modify or remove the possible relationships between assets when the relationship is in a Draft state.

Define appropriate roles and select the **Manage Custom Attributes** feature for that role when you configure privileges for Metadata Command Center in Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select an asset type.
3. For the selected asset type, go to the **Relationships** tab.
4. On the **Relationships** tab, click the Action menu next to a relationship and select **Edit**.



- To add a new relationship type, click the Add icon in the **Relationships** field and enter a new value.



- To modify an existing relationship type, click the value that you want to modify in the **Relationships** field .
- To remove an existing relationship type, click the Delete icon next to the value that you want to remove from the **Relationships** field .

**Note:** When you remove existing relationship types, consider the following:

- If a relationship type is already being used in Data Governance and Catalog to describe the relationship between assets, you can't delete the relationship type until you remove the relationships.
- If only 1 relationship exists between assets, you can't delete the relationship.

- Click **Save**.

The draft version appears in the **Published with draft available** state.

**Note:** If you do not want to proceed with your changes, you can use the **Discard** icon to discard the draft version of the relationship. You can also perform this action from the Action menu on the **Asset Customization > Relationships** tab of the **Customize** page. On the **Asset Customization > Relationships** tab, you can also discard the draft version of multiple relationships. To do this, select the relationships for which you want to discard the draft state and click the **Discard** icon from the Action menu.

- Click **Publish** to publish your changes.

The system initiates the **Association Publish** job to publish your changes. If another job to create, modify or delete an attribute or relationship is active, the system informs you of the active job. To publish your

changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

After the publishing is successful, the lifecycle state of the relationship changes from **Draft** to **Published**.

10. After the publish job is completed, ensure that you refresh the web page on your browser to view your changes to the relationship type.

After your changes are published, all the relationship types are automatically arranged in an alphabetical order.

## Define evaluation metrics

Evaluation metrics enable you to record additional data that pertain to an AI model asset. You can use evaluation metrics to compare various models, identify potential biases, and monitor model behavior over time.

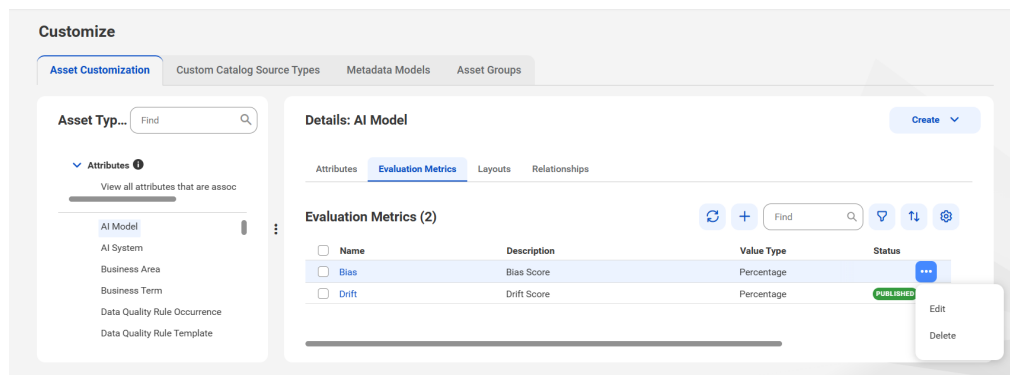
On the **Customize > Asset Customization** tab in Metadata Command Center, you can add new evaluation metrics or modify or remove existing evaluation metrics for AI Model assets. For more information about AI Model assets, see the *Understanding Business Assets* help for Data Governance and Catalog.

To have permissions to create, modify, or delete evaluation metrics, define appropriate roles and select the **Manage Custom Attributes** feature for that role when you configure privileges in Metadata Command Center in Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

## Creating evaluation metrics

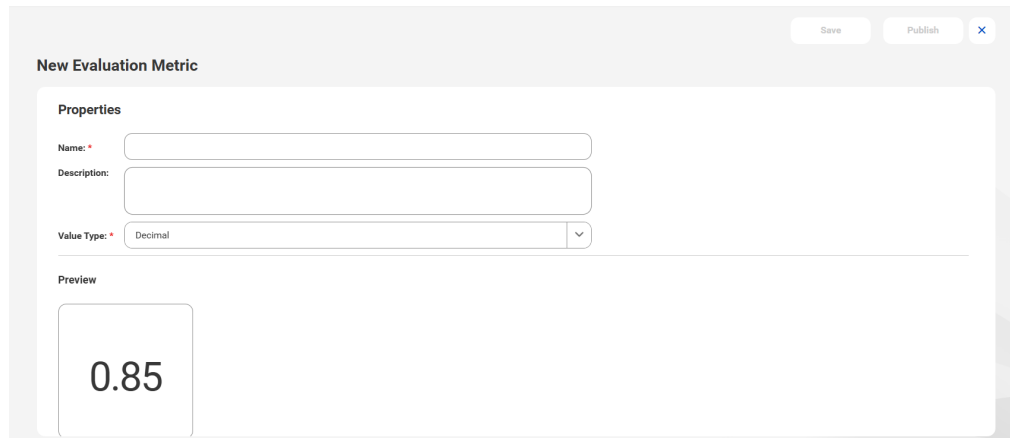
You can create new evaluation metrics for the AI model asset type.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select the **AI Model** asset type.
3. For the **AI Model** asset type, go to the **Evaluation Metrics** tab.



4. Click the **Add** icon.

Alternatively, you can use the **Create** button to add a new evaluation metric.



5. Configure the following properties of the new evaluation metric:

Property	Description
Name	Unique name for the evaluation metric that will be displayed in Data Governance and Catalog. Ensure that the metric name doesn't match a name that already exists.
Description	Description of the evaluation metric.
Value Type	The type of value that users can enter in the metric. You can choose one of the following value types: <ul style="list-style-type: none"><li>• Decimal</li><li>• Integer</li><li>• Percentage</li></ul> Default value is <b>Decimal</b> .

6. Click **Save**.

This creates a draft version of the new evaluation metric that you can view in the metrics list on the **Evaluation Metrics** tab.

7. Click the name of the evaluation metric that you saved to view and verify the details of the metric. To modify the properties of the metric, edit the values and click **Save**.

**Note:** If you do not want to proceed with your changes, you can use the **Discard** icon to discard the draft version of the evaluation metric. You can also perform this action from the Action menu on the **Asset Customization > Evaluation Metrics** tab of the **Customize** page. On the **Asset Customization > Evaluation Metrics** tab, you can also discard the draft version of multiple evaluation metrics. To do this, select the evaluation metrics for which you want to discard the draft state and click the **Discard** icon from the Action menu.

8. Click **Publish** to publish the metric in Data Governance and Catalog.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute, evaluation metric or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job has failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

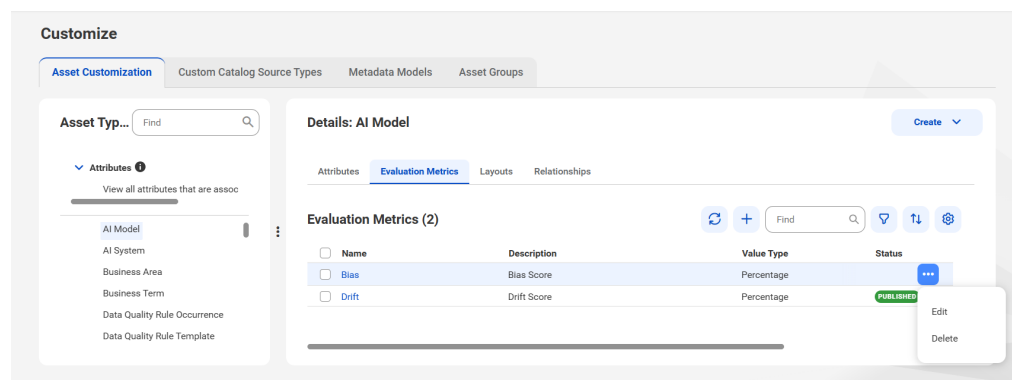
After the publishing is successful, the lifecycle state of the evaluation metric changes from **Draft** to **Published**.

The new metric appears on the **Overview** page of all AI Model assets in Data Governance and Catalog.

## Modifying evaluation metrics

You can modify a predefined evaluation metric or a custom evaluation metric that you created.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select the **AI Model** asset type.
3. For the **AI Model** asset type, open the **Evaluation Metrics** tab.



4. On the **Evaluation Metrics** tab, select the metric that you want to modify.

You can use filters to assist you in your search for evaluation metrics. You can also use filters to view only the predefined metrics or to view only the custom metrics.

5. Depending on the lifecycle state of the evaluation metric, choose one of the following options:
  - If the metric is in the **Draft** state, you can modify any property of the metric.
  - If the metric is in the **Published** state, open the metric and click **Create a draft**. You can modify only some of its properties.
6. Click **Save**.

**Note:** If you do not want to proceed with your changes, you can use the **Discard** icon to discard the draft version of the evaluation metric. You can also perform this action from the Action menu on the **Asset Customization > Evaluation Metrics** tab of the **Customize** page. On the **Asset Customization > Evaluation Metrics** tab, you can also discard the draft version of multiple evaluation metrics. To do this, select the evaluation metrics for which you want to discard the draft state and click the **Discard** icon from the Action menu.

7. Click **Publish** to publish your changes.



You can also perform this action from the Action menu on the **Asset Customization > Evaluation Metrics** tab of the **Customize** page. On the **Asset Customization > Evaluation Metrics** tab, you can also publish multiple evaluation metrics. To do this, select the evaluation metrics that you want to publish and click the **Publish** button from the Action menu.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute, evaluation metric or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job had failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

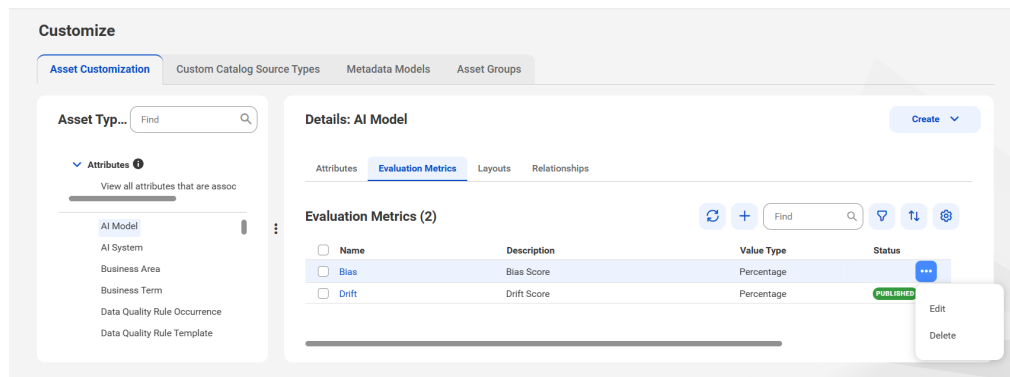
The status of the evaluation metric changes to **Published** and the modified attribute appears in Data Governance and Catalog.

8. After the publish job is completed, ensure that you refresh the web page on your browser to view the changes to the evaluation metric.

## Deleting evaluation metrics

If an evaluation metric is no longer relevant or if you want to modify the properties of a metric, you can delete the metric and create a new metric. Deleting an evaluation metric removes the metric in Data Governance and Catalog along with all the values that are defined for the metric.

1. On the **Customize** page in Metadata Command Center, go to the **Asset Customization** tab.
2. In the **Asset Types** panel, select the **AI Model** asset type.
3. For the **AI Model** asset type, open the **Evaluation Metrics** tab.



4. Select the check box for one or more evaluation metrics.
5. Click the Action menu for any of the selected metrics and click **Delete**.

If you have selected more than one evaluation metric to delete, then the Action menu for the selected group appears only if all the evaluation metrics in the group are in the **Published** or **Published with draft available** lifecycle states.

6. Click **Delete** to confirm.

The system initiates the **Attributes Publish** job to publish your changes. If another job to create, modify or delete an attribute, evaluation metric or relationship is active, the system informs you of the active job. To publish your changes, you must wait for the active job to be completed. On the **Job Monitoring Overview** page, you can click **View Status** to monitor the status of the job.

**Note:** The system displays an error if the previous job had failed. At this stage, you must resolve the errors and reinitiate the previous job and await its completion before you can start your own job.

## CHAPTER 13

# Custom layouts

You can define and modify the layout of the pages and preview panes in Data Governance and Catalog .

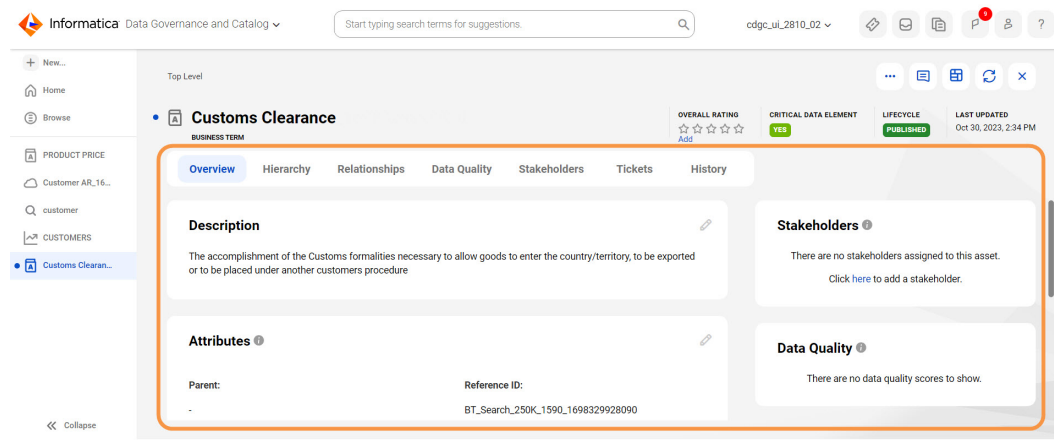
When a Data Governance and Catalog user opens an asset page or the **Browse** page, they see the attributes, panels, layout, and grid items in a predefined format. However, you might want to hide certain attributes or present a different layout for specific roles and users in your organization. For example, you might have experienced employees that need to see only a particular layout while searching for assets. Or you might want data engineers to see the related data elements of a business term first before they see the description. In such situations, you can modify the layouts for these roles and user groups so that they see the assets in the particular way that you configure.

**Note:** To customize a layout, your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. Consider creating a custom role with administrative abilities to which you can assign this privilege. For more information on feature privileges, see the *Introduction and Getting Started* help.

## Custom layout for asset pages

You can modify the layout of the various elements that a Data Governance and Catalog user sees on the main page of business and technical assets. An asset page refers to the primary page that displays the attributes of the asset. The asset page contains several tabs, and each tab contains corresponding panels and attributes.

The following image depicts the main page of an asset in Data Governance and Catalog:

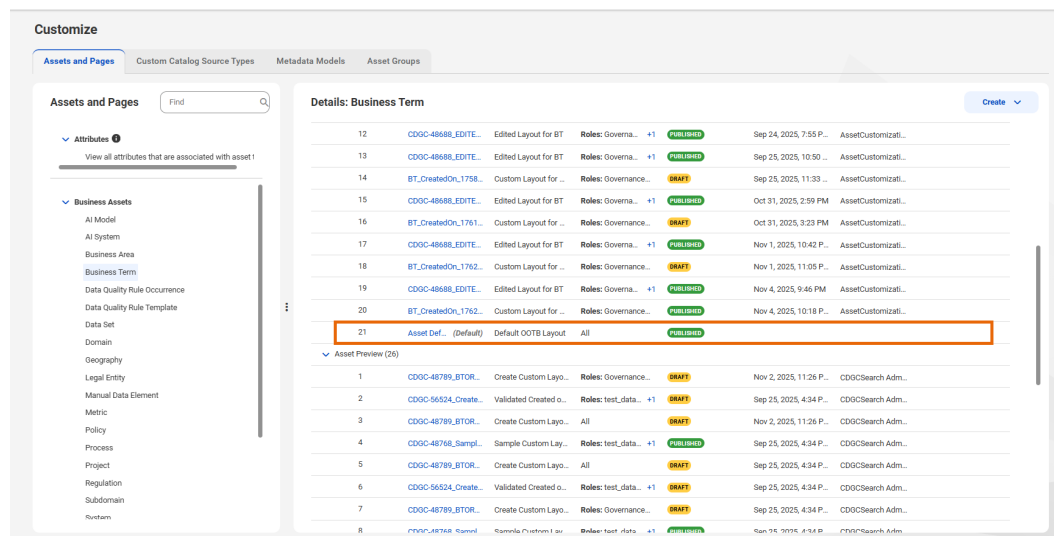


For asset pages, you can perform the following customization:

- Create a new layout for an asset from a blank canvas, or clone an existing layout to quickly make changes.
- Show, hide, and rearrange the order of tabs.  
**Note:** You cannot hide, move or delete the **Overview** tab.
- Show, hide, and rearrange the layout of panels within a tab.
- Split a wide panel into multiple narrow panels.
- Show, hide, and rearrange the position of attributes within a panel.
- Save a layout with a particular configuration and give it a unique name.
- Assign one or more layouts to users with specific roles, to users that are part of specific user groups, or to all users in your organization.
- Specify the default layout in which an asset appears when a user opens an asset of that asset type.

**Note:** A layout with the suffix 'Default' in the layout name comes predefined in Data Governance and Catalog. This layout appears for all users. You cannot modify or delete this layout. You can, however, clone this layout and create a custom layout from it.

The following image highlights the default page layout for an asset type in the list of layouts:



## Creating a custom layout for an asset page

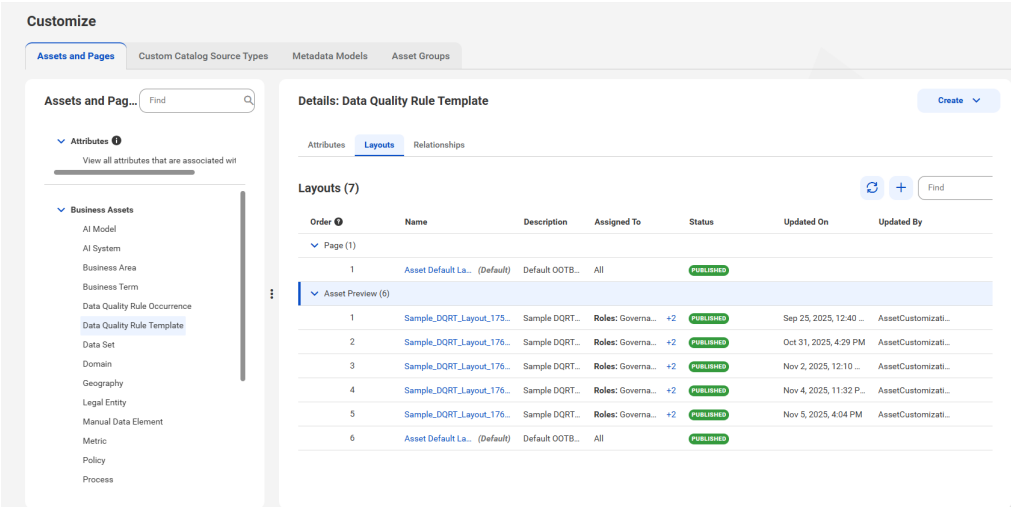
You can modify the layout of the asset page for specific asset types. Configure a layout, save it with a unique name, and then assign the layout to several roles and user groups or to all users in your organization. When a Data Governance and Catalog user opens an asset, they can view the assets as per the various layouts that are assigned for their user role or user group.

Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

1. In Metadata Command Center, navigate to the **Customize** page, and go to the **Assets and Pages** tab.
2. In the **Assets and Pages** list, select the asset type for which you want to create a layout.

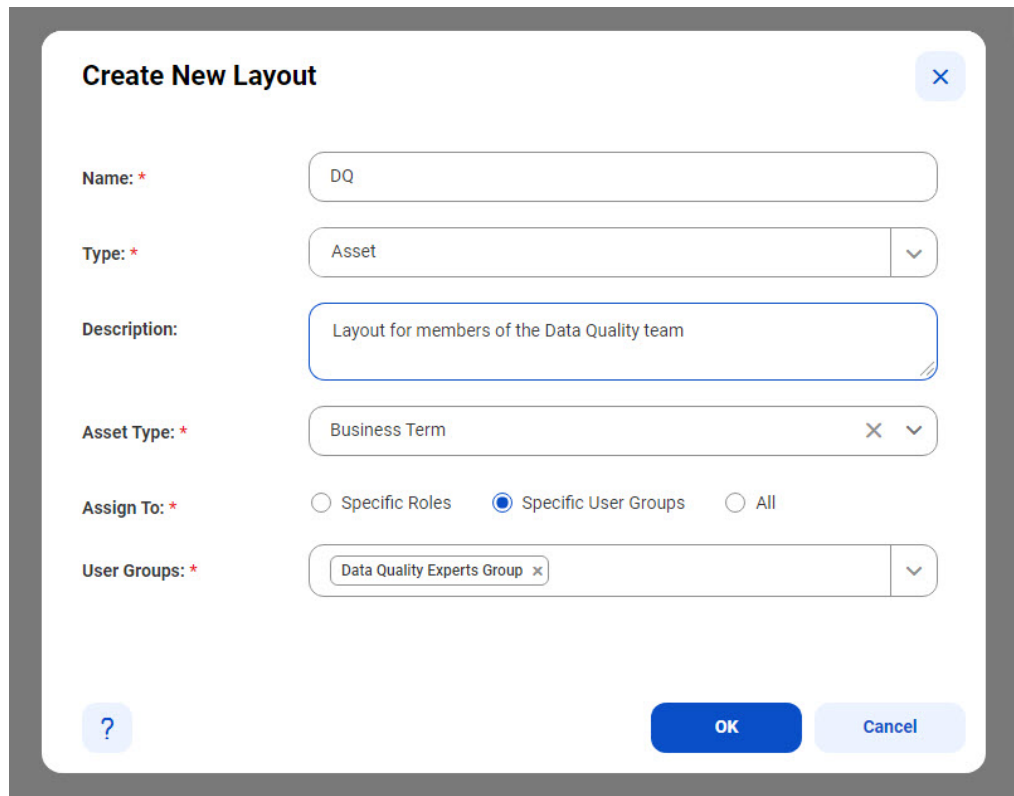
The **Asset and Pages** tab opens on the **Customize** page. The right pane shows the layouts that have been configured for the asset type. The **Page** header shows all layouts configured for the asset page,

and the **Asset Preview** header shows all layouts configured for the preview pane.



3. Click the add icon to create a new layout.
- Alternatively, you can click **New > Customization > Custom Layouts** to start creating a new layout.
4. Enter values for the following properties of the layout:

Property	Description
Name	Identifiable name for the layout. The name must be unique among the layouts for the asset type.
Type	Select <b>Asset</b> from the list.
Description	Description of the layout.
Asset Type	Select the business or technical asset type for which you want to configure the layout.
Assign To	<p>Specify the users to which you want to assign the layout.</p> <p>Select one of the following values:</p> <ul style="list-style-type: none"><li>• Specific roles. Assign the layout to users with specific roles. In the <b>Roles</b> field that appears, select the user roles.</li><li>• Specific user groups. Assign the layout to users that are part of specific user groups. In the <b>User Groups</b> field that appears, select the user groups.</li><li>• All. Assign the layout to users of all roles in your organization.</li></ul> <p><b>Note:</b> Only user roles that have the Read permission for the asset type will appear in this list. In Data Governance and Catalog, the users must have the Read permission for the asset type so that they can see the layout.</p>



**Create New Layout** [X]

**Name: \***

**Type: \***  [v]

**Description:**

**Asset Type: \***  [X] [v]

**Assign To: \*** ☐ Specific Roles ☒ Specific User Groups ☐ All

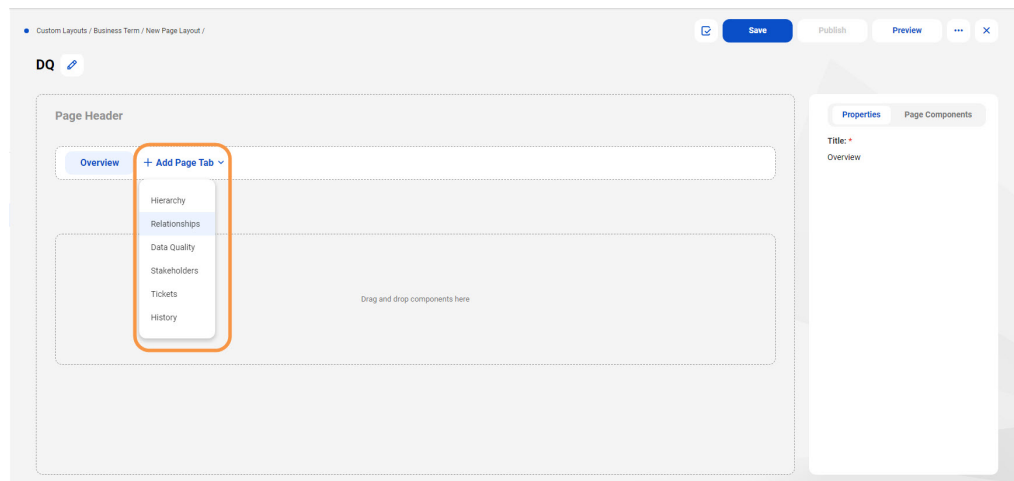
**User Groups: \***  [X] [v]

[?] [OK] [Cancel]

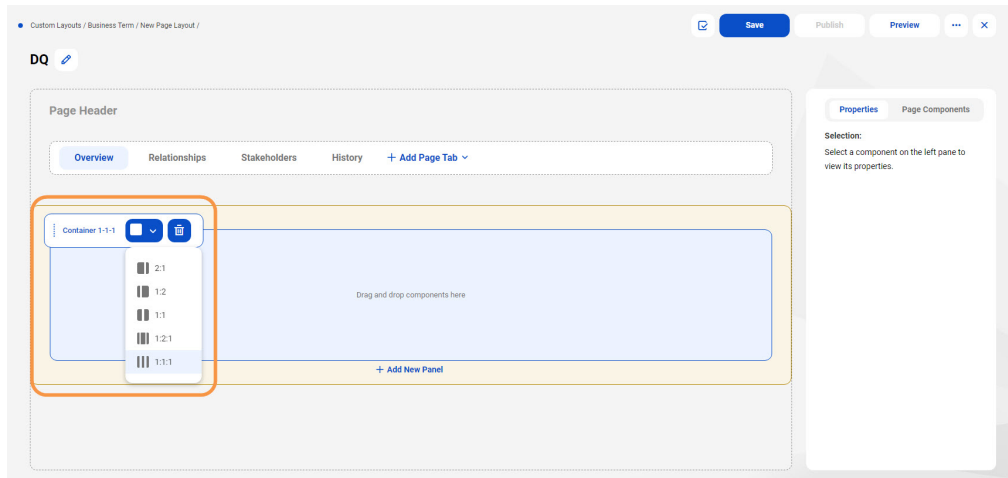
5. Click **OK**.

A blank layout canvas opens.

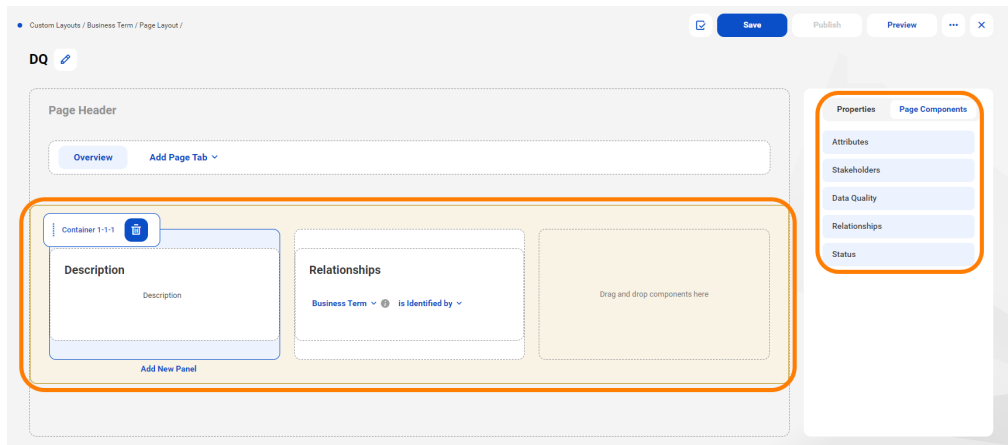
6. In the layout canvas, add one or more tabs.



7. For each panel group within a tab, select a column layout.



8. Within a panel, drag the components that you need from the available components in the **Page Components** tab.



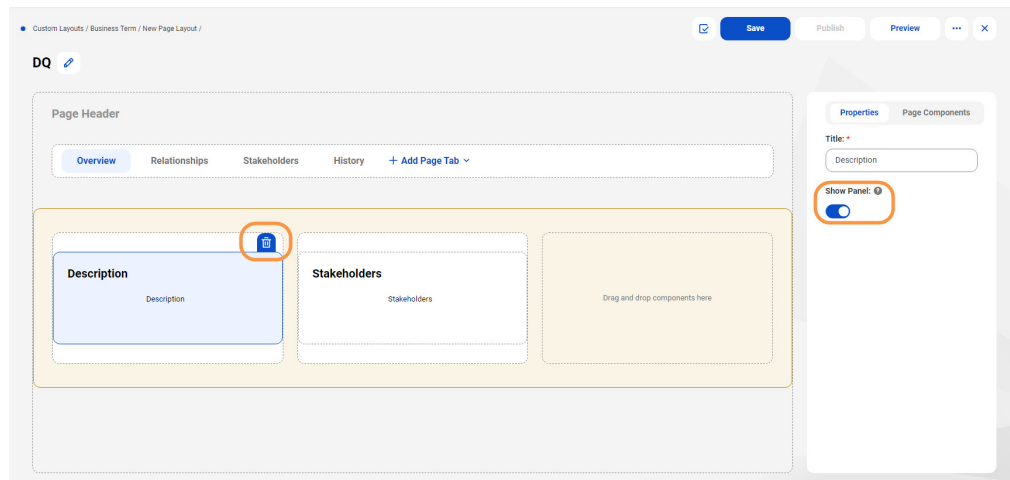
In a custom layout, you can also add a **Relationships** panel. You can configure the **Relationships** panel to display all related target assets or displays only the target assets that you specify. If you configure the **Relationships** panel to display only one target asset, Metadata Command Center allows you to specify the type of relationship the source asset has with the target asset.

If you want to add the **Relationships** panel to a layout, consider the following:

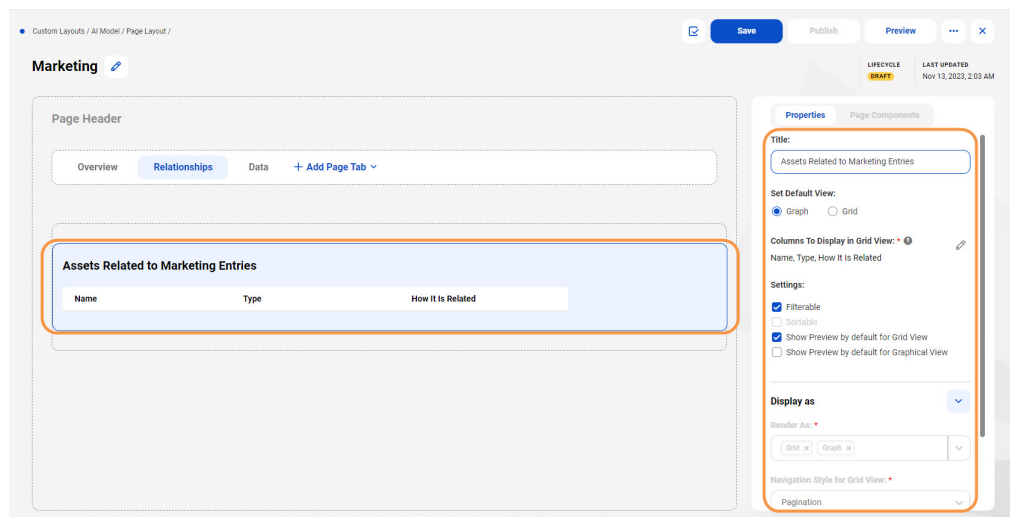
- You can add a maximum of 5 **Relationships** panels to a layout.
- You can't select a relationship type if you've selected more than one asset type.

**Note:** The **Relationships** panel isn't available on the default layout of an asset.

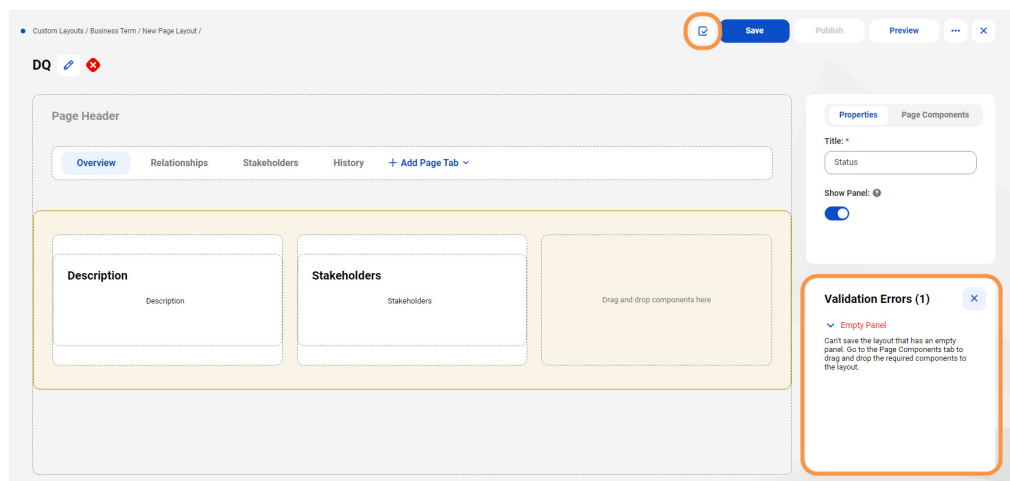
9. To suppress an attribute, slide the **Show Panel** slider in the **Properties** tab to off. To permanently remove an attribute, click the delete icon.



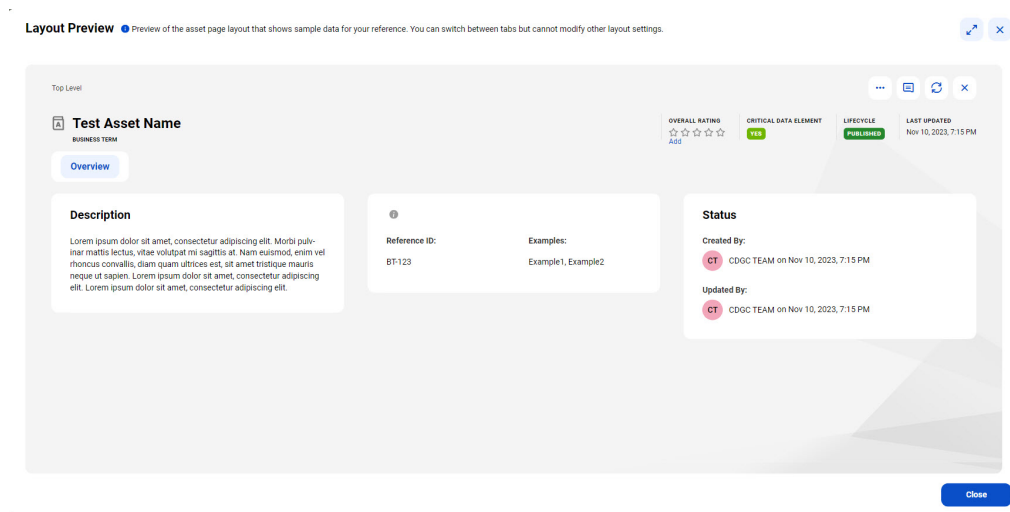
10. In other tabs, select a grid to specify further customization options.



11. Click the **Validate** icon to check if the layout is configured correctly. Fix the issues that appear in the **Validation Errors** panel.



- At any time, click **Preview** to visualize with sample data how the page will appear to Data Governance and Catalog users.



- When you are satisfied with the layout, click **Save**.  
The layout is saved for the asset type. However, it is not yet available to users.
- To make a saved layout available to users, open the layout and click **Publish**.  
The layout is now available in Data Governance and Catalog to all the users that you have specified. If the user has several layouts assigned to the role or user group, all the layouts are visible.

## Modifying, cloning and deleting a custom layout for an asset page

You can modify an existing asset page layout to make changes to the page. If you want to create a layout that is similar to an existing layout, you can clone a layout and modify it. If a layout is no longer needed, you can delete it.

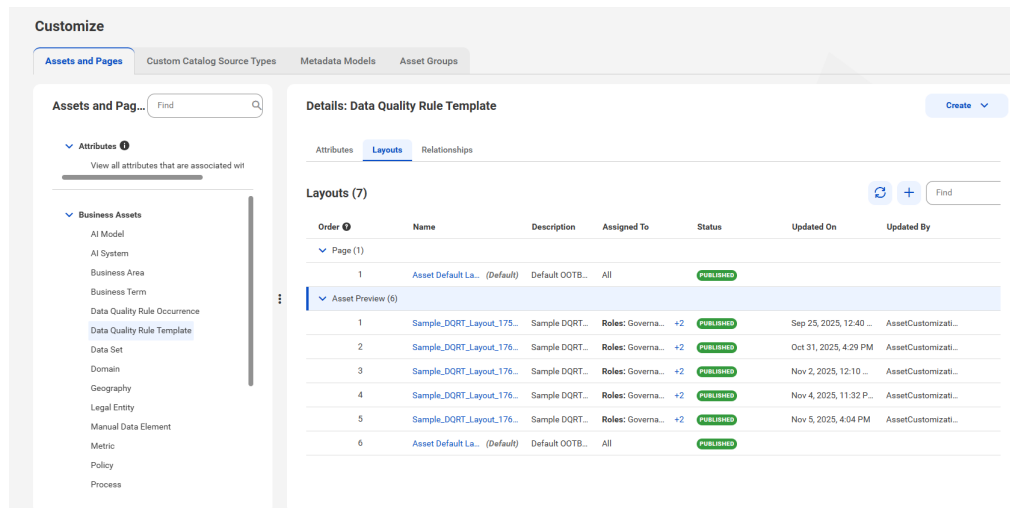
Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

You cannot modify or delete a predefined layout.

- In Metadata Command Center, navigate to the **Customize** page, and go to the **Assets and Pages** tab.
- In the **Assets and Pages** list, select the asset type for which you want to modify the layout.

The **Asset and Pages** tab opens on the **Customize** page. The right pane shows the layouts that have been configured for the asset type. The **Page** header shows all layouts configured for the asset page, and the **Asset Preview** header shows all layouts configured for the preview pane.



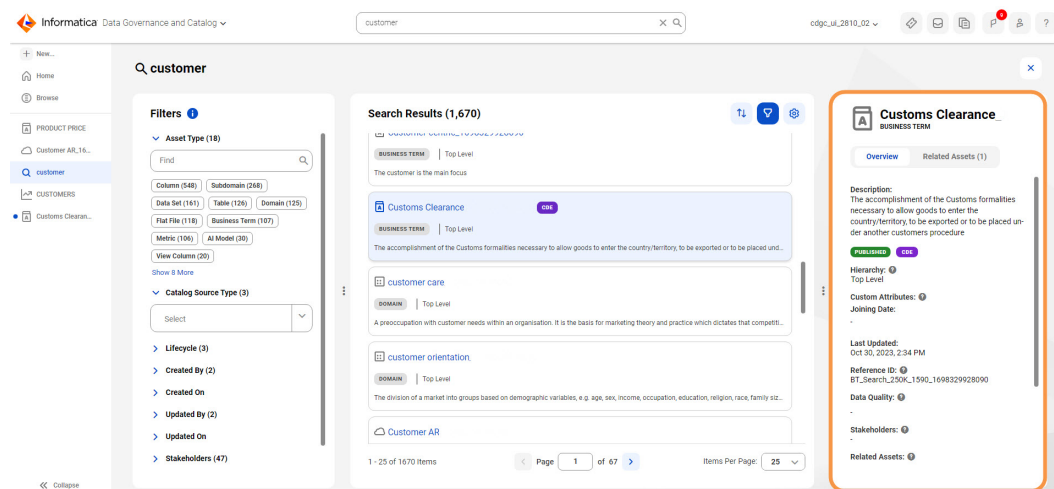


- To modify an existing layout, click on the layout or select **Edit** from the **Actions** menu.
  - To clone a layout, select **Clone** from the **Actions** menu. You can now modify the layout and save it with a new name.
  - To delete a layout, click **Delete** from the **Actions** menu.
- The layout is deleted. If this layout was configured as default by a Data Governance and Catalog user, the first layout in the list now becomes the default layout.

## Custom layout for preview panes

You can modify the layout of the various elements that a Data Governance and Catalog user sees on the preview pane of business and technical assets. The preview pane appears when you select an asset from a list that contains several assets.

The following image depicts the preview pane when you select an asset from a list of assets in Data Governance and Catalog:

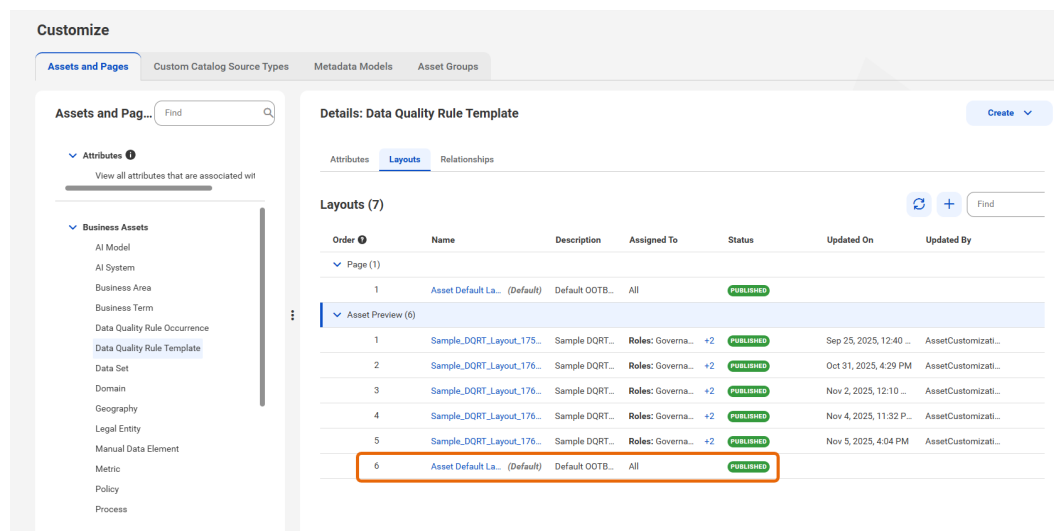


For preview panes, you can perform the following customization:

- Create a new layout for an asset from a blank canvas, or clone an existing layout to quickly make changes.
- Show, hide, or rearrange the position of attributes within a tab.
- For lists, select the specific values that you want the user to see.
- Save a layout with a particular configuration and give it a unique name.
- Assign one or more layouts to users with specific roles, to users that are part of specific user groups, or to all users in your organization.
- Specify the default layout in which a preview pane appears when a user opens an asset of that asset type.

**Note:** A layout with the suffix 'Default' in the layout name comes predefined in Data Governance and Catalog. This layout appears for all users. You cannot modify or delete this layout. You can, however, clone this layout and create a custom layout from it.

The following image highlights the default layout for a preview pane in the list of layouts:



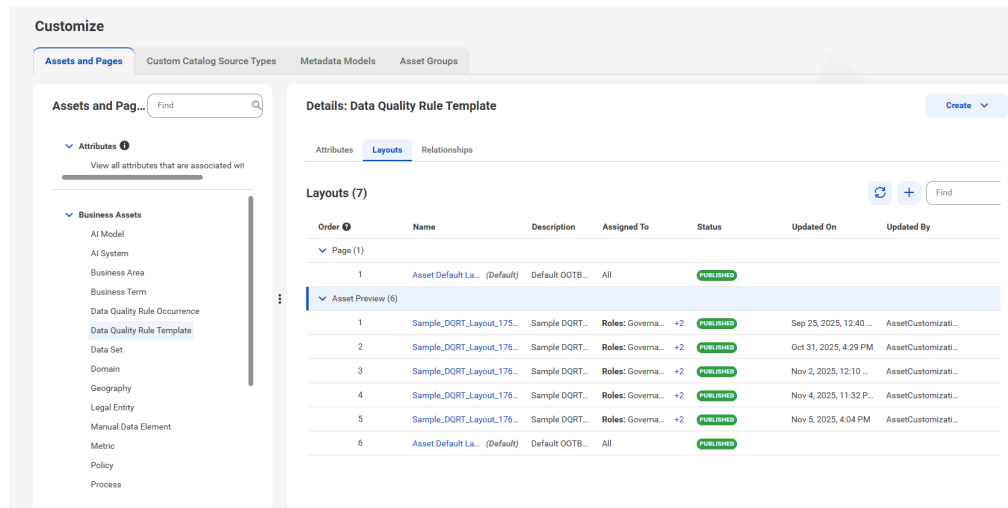
## Creating a custom layout for a preview pane

You can modify the layout of the asset preview pane for specific asset types. Configure a layout, save it with a unique name, and then assign the layout to several roles and user groups or to all users in your organization. When a Data Governance and Catalog user opens an asset preview pane, they can view the assets as per the various layouts that are assigned for their user role or user group.

Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

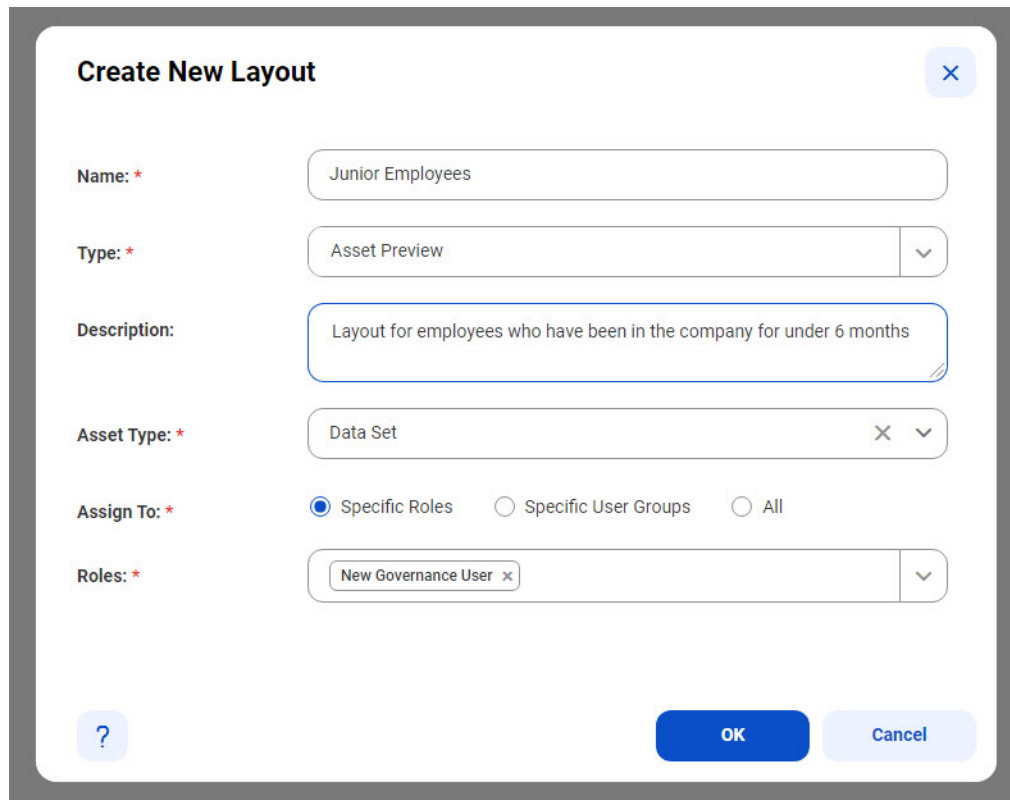
1. In Metadata Command Center, navigate to the **Customize** page, and go to the **Asset Customization** tab.
2. In the **Asset Types** list, select the asset type for which you want to create a layout.

The **Asset and Pages** tab opens on the **Customize** page. The right pane shows the layouts that have been configured for the asset type. The **Page** header shows all layouts configured for the asset page, and the **Asset Preview** header shows all layouts configured for the preview pane.



3. Click the add icon to create a new layout.  
Alternatively, you can click **New > Customization > Custom Layouts** to start creating a new layout.
4. Enter values for the following properties of the layout:

Property	Description
Name	Identifiable name for the layout. The name must be unique among the layouts for the asset type.
Type	Select 'Asset Preview' from the list.
Description	Description of the layout.
Asset Type	Select the business or technical asset type for which you want to configure the layout.
Assign To	<p>Specify the users to which you want to assign the layout. Select one of the following values:</p> <ul style="list-style-type: none"> <li>• Specific roles. Assign the layout to users with specific roles. In the <b>Roles</b> field that appears, select the user roles.</li> <li>• Specific user groups. Assign the layout to users that are part of specific user groups. In the <b>User Groups</b> field that appears, select the user groups.</li> <li>• All. Assign the layout to users of all roles in your organization.</li> </ul> <p><b>Note:</b> Only user roles that have the Read permission for the asset type will appear in this list. In Data Governance and Catalog, the users must have the Read permission for the asset type so that they can see the layout.</p>



**Create New Layout** [X]

**Name: \*** Junior Employees

**Type: \*** Asset Preview [v]

**Description:** Layout for employees who have been in the company for under 6 months

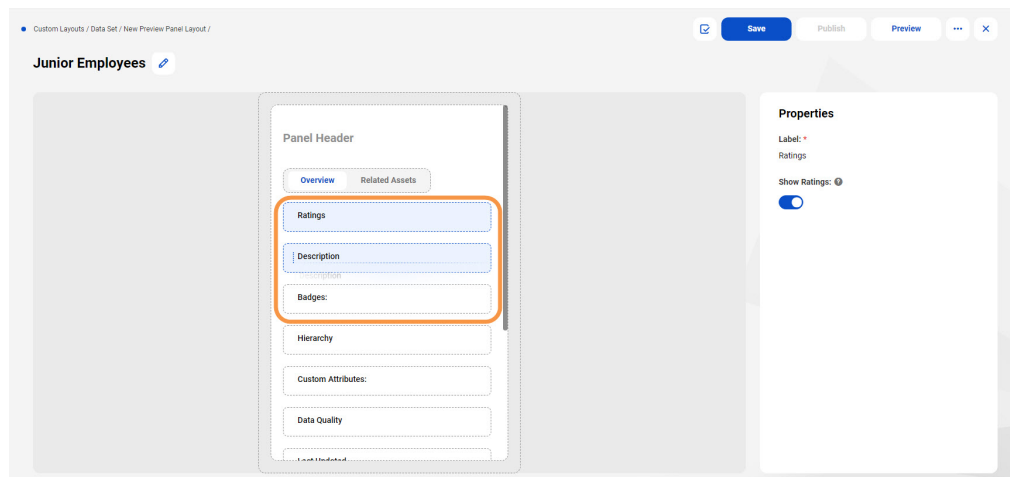
**Asset Type: \*** Data Set [X] [v]

**Assign To: \*** ☒ Specific Roles ☐ Specific User Groups ☐ All

**Roles: \*** New Governance User [X] [v]

[?] [OK] [Cancel]

5. Click **OK**.  
A blank layout canvas opens.
6. Drag the attributes to place them according to your preferred order.



Custom Layouts / Data Set / New Preview Panel Layout / [Save] [Publish] [Preview] [X]

**Junior Employees** [edit]

Panel Header

Overview Related Assets

Ratings

Description

Badges:

Hierarchy

Custom Attributes:

Data Quality

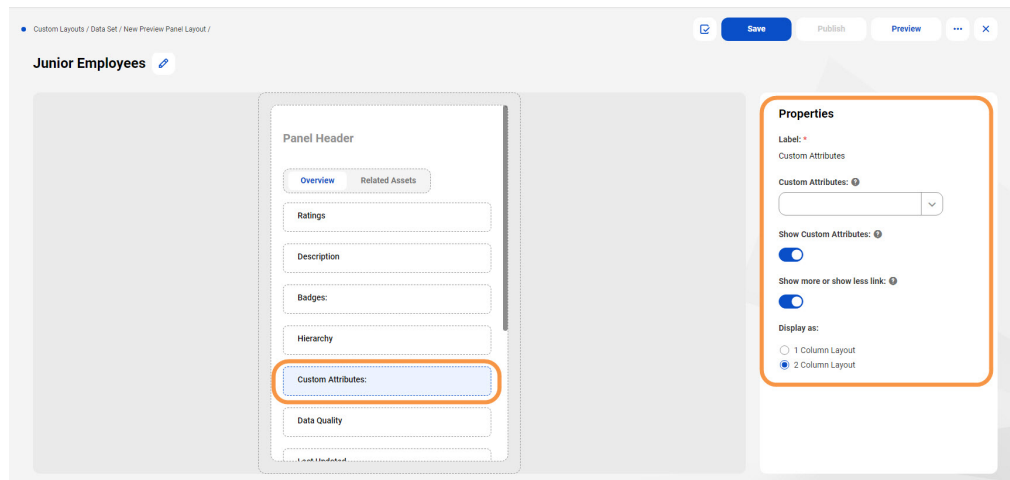
Properties

Label: \*

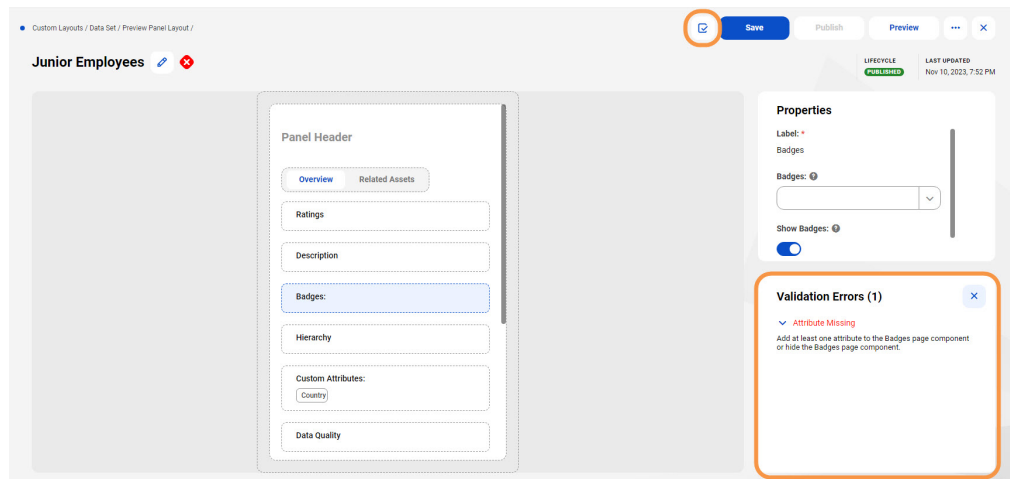
Ratings

Show Ratings: [toggle]

7. In the **Properties** pane, configure additional properties for each attribute.

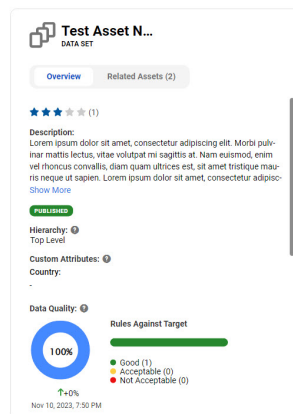


- Click the **Validate** icon to check if the layout is configured correctly. Fix the issues that appear in the **Validation Errors** panel.



- At any time, click **Preview** to visualize with sample data how the preview pane will appear to Data Governance and Catalog users.

**Layout Preview** Preview of the asset preview layout that shows sample data for your reference. You can switch between tabs but cannot modify other layout settings.



Close

- When you are satisfied with the layout, click **Save**.

The layout is saved for the asset type. However, it is not yet available to users.

- To make a saved layout available to users, open the layout and click **Publish**.

The layout is now available in Data Governance and Catalog to all the users that you have specified. If the user has several layouts assigned to the role or user group, all the layouts are visible.

## Modifying, cloning and deleting a custom layout for a preview pane

You can modify an existing preview pane layout to make changes to the pane. If you want to create a layout that is similar to an existing layout, you can clone a layout and modify it. If a layout is no longer needed, you can delete it.

Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

You cannot modify or delete a predefined layout.

- In Metadata Command Center, navigate to the **Customize** page, and go to the **Asset Customization** tab.
- In the **Asset Types** list, select the asset type for which you want to modify the layout.

The **Asset and Pages** tab opens on the **Customize** page. The right pane shows the layouts that have been configured for the asset type. The **Page** header shows all layouts configured for the asset page, and the **Asset Preview** header shows all layouts configured for the preview pane.

Order	Name	Description	Assigned To	Status	Updated On	Updated By
1	Asset Default La... (Default)	Default OOTB...	All	PUBLISHED		
Asset Preview (6)						
1	Sample_DQRT_Layout_175...	Sample DQRT...	Roles: Govern... +2	PUBLISHED	Sep 25, 2025, 12:40 ...	AssetCustomizati...
2	Sample_DQRT_Layout_176...	Sample DQRT...	Roles: Govern... +2	PUBLISHED	Oct 31, 2025, 4:29 PM	AssetCustomizati...
3	Sample_DQRT_Layout_176...	Sample DQRT...	Roles: Govern... +2	PUBLISHED	Nov 2, 2025, 12:10 ...	AssetCustomizati...
4	Sample_DQRT_Layout_176...	Sample DQRT...	Roles: Govern... +2	PUBLISHED	Nov 4, 2025, 11:32 P..	AssetCustomizati...
5	Sample_DQRT_Layout_176...	Sample DQRT...	Roles: Govern... +2	PUBLISHED	Nov 5, 2025, 4:04 PM	AssetCustomizati...
6	Asset Default La... (Default)	Default OOTB...	All	PUBLISHED		

- To modify an existing layout, click on the layout or select **Edit** from the **Actions** menu.
- To clone a layout, select **Clone** from the **Actions** menu. You can now modify the layout and save it with a new name.
- To delete a layout, click **Delete** from the **Actions** menu.

The layout is deleted. If this layout was configured as default by a Data Governance and Catalog user, the first layout in the list now becomes the default layout.

# Custom layouts for the Browse page

You can define the layout of the **Browse** page that a Data Governance and Catalog user views to explore assets.

When a Data Governance and Catalog user opens the **Browse** page, they can view how the catalog is structured and explore data by asset type. They can also easily drill down to see the child assets associated with the asset. However, you might want to hide certain settings or present a different layout for specific roles and users in their organization. You can create and save these layouts and they then appear listed in **Layouts** on the **Browse** page of Data Governance and Catalog. Users can switch between these layouts.

## Creating a custom layout for the Browse page

You can modify the layout of the **Browse** page, save it with a unique name and then assign the layout to specific roles and user groups or to all users in your organization. When a Data Governance and Catalog user opens the **Browse** page, they can view the **Browse** page as per the various layouts that are assigned to their user role or user group.

Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

1. In Metadata Command Center, navigate to the **Customize** page and click **Assets and Pages**.
2. From the **Assets and Pages** list, click **Browse Page**.

The **Details** pane shows the layouts that are configured for the **Browse** page.

The screenshot shows the 'Customize' page with the 'Assets and Pages' tab selected. On the left, a tree view shows 'Business Assets', 'Data Marketplace', 'Data Access Asset', 'Data Classification', and 'Technical Assets'. Under 'Technical Assets', 'Browse Page' is selected. The main pane, titled 'Details: Browse Page', shows a table of layouts. The table has columns: Order, Name, Description, Assigned To, Status, Updated On, and Updated By. There are 13 rows of layouts, mostly with status 'PUBLISHED' and one with 'DRAFT'.

Order	Name	Description	Assigned To	Status	Updated On	Updated By
1	CDGC-84732_1761902618...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Oct 31, 2025, 5:06 PM	AssetCustomizati...
2	CDGC-84737_1761902618...	Custom Layo...	Roles: test_data... +1	PUBLISHED	Oct 31, 2025, 5:07 PM	AssetCustomizati...
3	CDGC-84739_1761902618...	Custom Layo...	User Groups: U... +1	PUBLISHED	Oct 31, 2025, 5:07 PM	AssetCustomizati...
4	CDGC-84732_1762016811...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 10:17 P...	CDGCSearch Adm...
5	CDGC-84739_1762016811...	Custom Layo...	User Groups: U... +1	PUBLISHED	Nov 2, 2025, 12:34 ...	AssetCustomizati...
6	CDGC-84732_1762108588...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:09 ...	AssetCustomizati...
7	CDGC-84739_1762108588...	Custom Layo...	User Groups: U... +1	PUBLISHED	Nov 3, 2025, 12:10 ...	AssetCustomizati...
8	CDGC-84747_Clone_1762...	Cloned OOTB ...	User Groups: U... +1	PUBLISHED	Nov 3, 2025, 12:10 ...	AssetCustomizati...
9	CDGC-84749_1762108588...	Custom Layo...	Roles: test_workfl...	DRAFT	Nov 3, 2025, 12:12 ...	AssetCustomizati...
10	CDGC-85819_1762108588...	Custom Layo...	All	PUBLISHED	Nov 3, 2025, 12:14 ...	AssetCustomizati...
11	CDGC-85820_1762108588...	Custom Layo...	All	PUBLISHED	Nov 3, 2025, 12:15 ...	AssetCustomizati...
12	CDGC-84756_1762108588...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:15 ...	AssetCustomizati...
13	CDGC-84757_DEFAULT_17...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:16 ...	AssetCustomizati...

3. Click the **Add** icon to create a new layout.  
Alternatively, you can click **Create > New Layout** to create a new **Browse** page layout.
4. Enter values for the following layout properties:

Property	Description
Name	Identifiable name for the layout.
Type	The type of layout. By default <b>Browse Page</b> is selected.

Property	Description
Description	Description of the layout.
Assign to	<p>Specify the users to whom you want to assign the layout. Select one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>Specific roles.</b> Assign the layout to users with specific roles. In the <b>Roles</b> field that appears, select the user roles.</li> <li>• <b>Specific user groups.</b> Assign the layout to users that are part of specific user groups. In the <b>User Groups</b> field that appears, select the user groups.</li> <li>• <b>All.</b> Assign the layout to users of all roles in your organization.</li> </ul>

- Click **OK**.  
A blank layout canvas opens.
- On the layout canvas, add tabs that you want to include in the layout.
- Click the **Validate** icon to check if the layout is configured correctly. Fix the issues that appear in the **Validation Errors** panel.
- At any time, click **Preview** to visualize with sample data how the page will appear to Data Governance and Catalog users.
- Click **Save** to save the **Browse** page layout.
- Click **Publish** to make the saved layout available to users.

The layout is now available in Data Governance and Catalog to all the specified users. Users in multiple groups or roles see all the layouts assigned to each of their groups and roles.

## Modifying, cloning and deleting a custom layout for the Browse page

You can modify an existing **Browse** page layout to make changes to the page. If you want to create a layout that is similar to an existing layout, you can clone a layout and modify it. If a layout is no longer needed, you can delete it.

Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

You cannot modify or delete a predefined layout.

- In Metadata Command Center, navigate to the **Customize** page, and go to the **Assets and Pages** tab.
- From the **Assets and Pages** list, click **Browse Page**.



The **Details** pane shows the layouts that are configured for the **Browse** page.

**Customize**

**Assets and Pages** Custom Catalog Source Types Metadata Models Asset Groups

**Assets and Pages** Find

**Attributes** View all attributes that are associated with

- Business Assets
- Data Marketplace
- Data Access Asset
- Data Classification
- Technical Assets
- Browse Page**

**Details: Browse Page** Create

**Layouts (50)** Find

Order	Name	Description	Assigned To	Status	Updated On	Updated By
1	CDGC-84732_1761902618...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Oct 31, 2025, 5:06 PM	AssetCustomizati...
2	CDGC-84737_1761902618...	Custom Layo...	Roles: test_data_o... +1	PUBLISHED	Oct 31, 2025, 5:07 PM	AssetCustomizati...
3	CDGC-84739_1761902618...	Custom Layo...	User Groups: U... +1	PUBLISHED	Oct 31, 2025, 5:07 PM	AssetCustomizati...
4	CDGC-84732_1762016811...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 10:17 P...	CDGCSearch Adm...
5	CDGC-84739_1762016811...	Custom Layo...	User Groups: U... +1	PUBLISHED	Nov 2, 2025, 12:34 ...	AssetCustomizati...
6	CDGC-84732_1762108588...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:09 ...	AssetCustomizati...
7	CDGC-84739_1762108588...	Custom Layo...	User Groups: U... +1	PUBLISHED	Nov 3, 2025, 12:10 ...	AssetCustomizati...
8	CDGC-84747_Clone_1762...	Cloned OOTB ...	User Groups: U... +1	PUBLISHED	Nov 3, 2025, 12:10 ...	AssetCustomizati...
9	CDGC-84749_1762108588...	Custom Layo...	Roles: test_workfl...	DRAFT	Nov 3, 2025, 12:12 ...	AssetCustomizati...
10	CDGC-85819_1762108588...	Custom Layo...	All	PUBLISHED	Nov 3, 2025, 12:14 ...	AssetCustomizati...
11	CDGC-85820_1762108588...	Custom Layo...	All	PUBLISHED	Nov 3, 2025, 12:15 ...	AssetCustomizati...
12	CDGC-84756_1762108588...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:15 ...	AssetCustomizati...
13	CDGC-84757_DEFAULT_17...	Custom Layo...	Roles: test_data_o...	PUBLISHED	Nov 3, 2025, 12:16 ...	AssetCustomizati...

- To modify an existing layout, click the layout or select **Edit** from the **Actions** menu.
- To clone a layout, select **Clone** from the **Actions** menu. You can now modify the layout and save it with a new name.
- To delete a layout, click **Delete** from the **Actions** menu.

The layout is deleted. If this layout was configured as default by a Data Governance and Catalog user, the first layout in the list becomes the default layout.

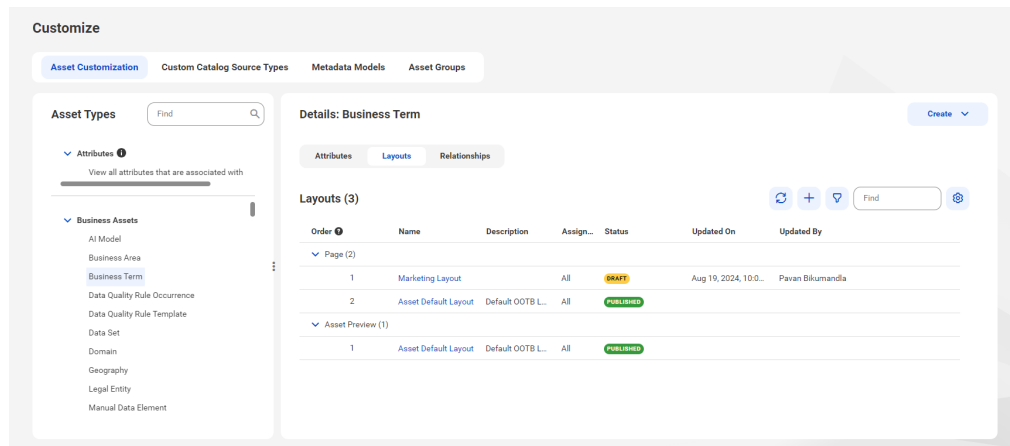
## Setting the default layout for an asset type

You can specify the default layout in which an asset appears when a Data Governance and Catalog user opens the asset.

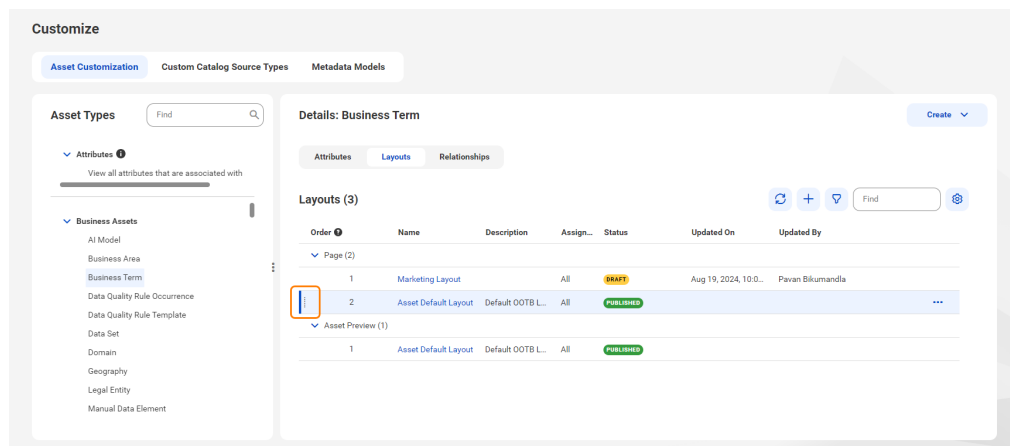
Your user role must have the **Asset Page Customization** privilege in Informatica Intelligent Cloud Services Administrator. For more information on feature privileges, see the *Introduction and Getting Started* help.

- In Metadata Command Center, navigate to the **Customize** page, and go to the **Asset Customization** tab.
- In the **Asset Types** list, select the asset type for which you specify the order of layouts.

The right pane shows the layouts that have been configured for the asset type. The **Page** header shows all layouts configured for the asset page, and the **Asset Preview** header shows all layouts configured for the preview pane.



3. Click on a layout and drag it to the first position.



**Note:** The predefined layouts for asset pages and preview panes always appear as the last items in the list in Metadata Command Center, and you cannot move them to a new position.

4. Click **Save Order**.

When a Data Governance and Catalog user opens an asset of this asset type, the asset opens in the layout that you specify as the first item here in Metadata Command Center. The user can then override this layout with another layout as default. However, the layouts in the layout switcher list in Data Governance and Catalog always appear in alphabetical order.

## CHAPTER 14

# Prefix values for asset reference IDs

Reference IDs are unique identifiers assigned to business assets in Data Governance and Catalog and to Marketplace assets in Data Marketplace.

You can create the reference IDs or allow Data Governance and Catalog or Data Marketplace to generate them automatically. A reference ID consists of a prefix, a separator, and a value. For example, a policy asset can have the reference ID 'POLIC-123'.

Prefix values are pre-configured and provided by default in Metadata Command Center. For auto-generated reference IDs, you can configure the prefix in Metadata Command Center.

## Configuring a prefix value

To configure a prefix value, you need the **Manage System Settings** feature privilege. If you don't have the **Manage System Settings** privilege enabled, you can view the prefixes, but you can't edit them.

Configuring the prefix for auto-generated reference IDs does not impact IDs that you manually assigned.

You cannot edit or update a manually-assigned reference ID in the auto-generated format of <prefix>-<reference ID number>.

1. In Metadata Command Center, go to the **Configure** page.
2. Click the **Reference IDs** tab.
3. Select an asset type from the list.
4. In **Edit Reference ID** window, modify the prefix value.
5. Click **Save**.

For more information about reference IDs for business assets, see *Working With Assets* in the Data Governance and Catalog help.

## Rules for creating prefixes

A prefix must meet the following requirements:

- It must be between two and eight characters long.

- It must start with a letter.
- It can contain only letters, numbers, or underscores.
- It must contain only upper case letters. The system automatically converts lower case letters to upper case.

## CHAPTER 15

# Workflows

You can design workflows and configure workflow events that services like Data Governance and Catalog can implement when users create or modify assets.

A workflow orchestrates a sequence of steps to manage and approve organizational change. You can use workflows to design and visualize the changes and ensure compliance with it. Workflows allow frequent repetition of steps in a clear and consistent manner and provide evidence that the steps are followed every time the workflow is run.

Informatica leverages the Business Process Modeling Notation (BPMN) infrastructure that allows you to design multi-step approval workflows in Metadata Command Center. You can design workflows that suit your organizational needs and configure events for the workflows in Metadata Command Center.

A workflow configured in Metadata Command Center determines the business process to be followed. Workflow events determine the events that can start the workflow and the user roles that can participate in the workflow.

A workflow specifies a series of predefined steps that begin when a user performs certain tasks in Data Governance and Catalog.

The following tasks start a workflow:

- Create a business or data access asset.
- Modify the description or other editable properties on the **Overview** tab of a business asset.
- Modify the description of a technical asset.
- Modify editable properties on the **Overview**, **Conditions**, **Rules**, **Techniques**, and **De-identification Rank** tabs of a data access asset.

A workflow also provides options to include the stakeholders who must be involved in providing inputs for the steps configured in the workflow. Each step is a task that a stakeholder of the asset must perform. A workflow ensures that the right people have the opportunity to provide inputs, challenge, and approve matters related to the asset that is created or modified.

Human intervention becomes necessary in business processes where a decision needs to be taken. For example, a human action is required for approvals. The workflows start when you work with assets in Data Governance and Catalog. For example, when a user attempts to create a business asset, Data Governance and Catalog creates a ticket for the approval process. This ticket starts the workflow associated with the asset and involves the relevant stakeholders in the process.

For more information about working with workflow tickets, see *Asset Management* in the Data Governance and Catalog help.

You can choose to use predefined workflows or configure custom workflows. A predefined workflow uses a predefined business process provided by Informatica that you can't modify. A custom workflow uses a business process that you design based on your organization's needs.

Effective in the July 2025 release, Informatica drops support for workflows created using Application Integration processes in Metadata Command Center. After you upgrade to the July 2025 release, redesign your existing workflows created using Application Integration processes. You can use predefined workflows that Informatica provides or build your own workflows in Metadata Command Center.

To use workflows, perform the following high-level steps:

1. Design and publish workflows in Metadata Command Center that suit your organizational needs or use the predefined workflows provided by Informatica.
2. Configure workflow events with the published workflows in Metadata Command Center.
3. Create or modify assets in Data Governance and Catalog to create tickets.

# Privileges for workflows

Each workflow defines one or more specific user roles. The users that can participate in a workflow depend on the steps and the user roles that are defined in the workflow.

Before you design workflows and configure workflow events in Metadata Command Center, you must assign additional privileges to existing user roles to work with workflow tickets. You can either modify existing user roles with additional privileges or create a separate user role and assign the role to existing users. The predefined Governance Administrator Stakeholder role in Metadata Command Center includes features and privileges that you need to configure and manage workflows.

You need specific privileges to perform different tasks related to configuring workflows. These privileges are related to and dependent on each other.

In addition to specific privileges, you need to have at least one access policy that grants you permission to configure and manage workflows. The predefined Governance Administrator Stakeholder access policy grants you permission to configure and manage workflows.

## Minimum privileges to design workflows in Metadata Command Center

To design workflows, ensure that your organization administrator grants the minimum required privileges and permissions to the user role.

The following table lists the minimum privileges and permissions needed to design workflows:

Service	Asset Privilege	Feature Privilege
Metadata Command Center	None	<b>Workflow Designer</b>

## Minimum privileges to manage workflows and event configurations in Metadata Command Center

To manage workflows, ensure that your organization administrator grants the minimum required privileges and permissions to the user role.

The following table lists the minimum privileges and permissions needed to manage workflows and event configurations:

Service	Asset Privilege	Feature Privilege
Metadata Command Center	None	<b>Manage Workflows</b>

## Minimum privileges to select and view workflows in Metadata Command Center

To ensure that a user role can select and view workflows while configuring workflow events in Metadata Command Center, assign the minimum required privileges to the role.

The following table lists the minimum privileges that must be configured in Administrator to select and view workflows while configuring workflow events:

Service	Asset Privilege	Feature Privilege
Metadata Command Center	None	<ul style="list-style-type: none"><li>- <b>Access Metadata Command Center Application</b></li><li>- <b>View Workflows</b></li></ul>
Data Governance and Catalog	None	<b>Participate in Change Approvals</b>

## Minimum privileges to create workflow tickets in Data Governance and Catalog

To create workflow tickets, ensure that your organization administrator grants the minimum required privileges and permissions to the user role.

The following table lists the minimum privileges and permissions needed to create workflow tickets:

Service	Privileges and Permissions
Metadata Command Center	<b>Read</b> permission for the technical, business, or data access asset types configured through access policies in Metadata Command Center
Data Governance and Catalog	<b>Access Data Governance And Catalog Application</b> feature privilege configured in Administrator

## Minimum privileges to work with workflow tickets in Data Governance and Catalog

If you're a stakeholder and you want to work with workflow tickets, ensure that your organization administrator grants the minimum required privileges and permissions to your user role.

The following table lists the minimum privileges and permissions needed for stakeholders to work with workflow tickets:

Service	Privileges and Permissions
Metadata Command Center	<ul style="list-style-type: none"><li>- <b>Read</b> permission for the technical, business, or data access asset types configured through access policies in Metadata Command Center.</li><li>- <b>Delete</b> permission for the business or data access asset types configured through access policies in Metadata Command Center. Required to reject workflows for creating a new asset.</li><li>- <b>Read</b> and <b>Update</b> permissions on the <b>Unpublished Changes</b> attribute group for the technical, business, or data access asset types configured through access policies in Metadata Command Center. Required to reject workflows for modifying an existing asset.</li></ul>
Data Governance and Catalog	<ul style="list-style-type: none"><li>- <b>Access Data Governance And Catalog Application</b> feature privilege configured in Administrator</li><li>- <b>Participate in Change Approvals</b> feature privilege configured in Administrator</li><li>- You must be a stakeholder on the asset.</li></ul>

## Minimum privileges to view all tasks in Data Governance and Catalog

To view all tasks that are available on the **Tasks Inbox** page in Data Governance and Catalog, ensure that your organization administrator grants the minimum required privileges and permissions to your user role.

The following table lists the minimum privileges needed for users to view all tasks on the **Tasks Inbox** page:

Service	Privileges and Permissions
Data Governance and Catalog	<b>Manage Workflow Tasks</b> feature privilege configured in Administrator

## Minimum privileges to assign or reassign a task in Data Governance and Catalog

To assign an unclaimed task or to reassign a task that is already claimed by a user, ensure that your organization administrator grants the minimum required privileges and permissions to your user role.

The following table lists the minimum privileges needed for users to assign tasks to other users:

Service	Privileges and Permissions
Data Governance and Catalog	<b>Manage Workflow Tasks</b> feature privilege configured in Administrator



## Minimum privileges to cancel open workflow tickets in Data Governance and Catalog

To cancel open workflow tickets without being a stakeholder on the asset, ensure that your organization administrator grants the minimum required privileges and permissions to your user role.

The following table lists the minimum privileges and permissions needed for users to cancel open workflow tickets:

Service	Privileges and Permissions
Metadata Command Center	<b>Read</b> permission for the technical, business, or data access asset types configured through access policies in Metadata Command Center
Data Governance and Catalog	<ul style="list-style-type: none"><li>- <b>Access Data Governance And Catalog Application</b> feature privilege configured in Administrator</li><li>- <b>Manage Tickets</b> feature privilege configured in Administrator</li></ul> <p><b>Note:</b> The <b>Manage Tickets</b> privilege is needed only if you are not a stakeholder of the asset.</p>

## Predefined workflows

Informatica provides predefined workflows in Metadata Command Center that you can use instead of designing your own workflows.

When you configure a workflow event in Metadata Command Center, you can choose a predefined workflow where the steps are already configured or design a BPMN-based workflow that meets your requirement. You can't make changes to predefined workflows.

The following predefined workflows are available in Metadata Command Center:

- **Manage Asset Single Step Approval.** A workflow with a single-step approval process to evaluate requests and take necessary action.
- **Manage Asset Two Step Approval.** A workflow with a two-step approval process to evaluate requests and take necessary action.
- **Manage Asset Three Step Approval.** A workflow with a three-step approval process to evaluate requests and take necessary action.

You can use predefined workflows as a reference to design your own workflows.

## Workflow components

A workflow can include multiple components that outline the steps needed to complete a process.

Use the following components to design workflows:

- **Swimlane.** Partitions a set of steps in a workflow and visually distinguish task responsibilities between different user roles.

- **Start.** Starts a workflow.
- **User Task.** A human action required for approvals. For example, you might want to add a user task step to a loan approval process.
- **Decision Gateway.** A control point in a workflow. Use to control the direction of the workflow based on your decision in a user task. For example, approve the request if it meets the requirements, reject if not, or return if more information is required.
- **Parallel Gateway.** A gateway pair that enables multiple tasks to run concurrently. A parallel gateway pair consists of a divergent and convergent gateway. A divergent gateway splits an incoming path into several concurrent outgoing paths, whereas a convergent gateway joins all the incoming paths into a single outgoing path. For example, when you create a workflow for processing a loan application, you can add multiple tasks that can run in parallel to speed up the process. Customer credit risk validation, KYC collection, asset details, and legal inputs are tasks that users can perform concurrently.
- **Connections.** Connects components in a workflow.
- **End.** Marks the completion of a workflow.
- **Terminal End.** Explicitly ends a workflow. Use in parallel gateways to terminate all active tasks and end the workflow.

You can use the following tools when you design workflows:

- **Hand Tool.** Moves the workflow around the canvas when zoomed in. This tool is useful in large workflows where components are not all visible at once.
- **Space Tool.** Adjusts spacing between components and create or remove space both horizontally and vertically in a workflow. This tool is helpful to maintain a clean and organized layout when you add new components or rearrange existing ones.
- **Select Tool.** Selects one or more components in a workflow.

## Configuring a workflow

If the predefined workflows don't meet your organizational needs, configure your own workflows.

You can configure multi-step approval workflows in Metadata Command Center that suit your organizational needs. The workflows start when you work with assets in Data Governance and Catalog.

Perform the following tasks to configure a workflow:

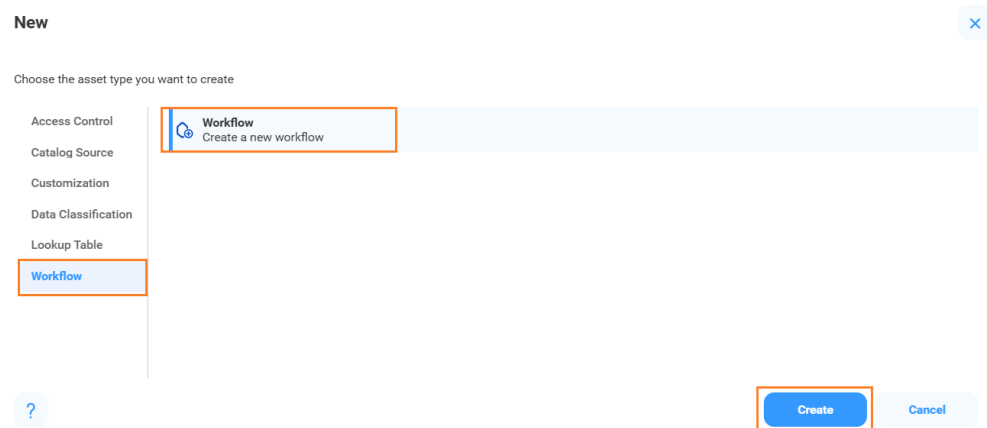
1. Configure workflow details with general information such as workflow name and description.
2. Design the workflow using various components of the BPMN infrastructure.
3. Validate the workflow to check for errors and resolve them.
4. Save and publish the workflow.

### Configuring workflow details

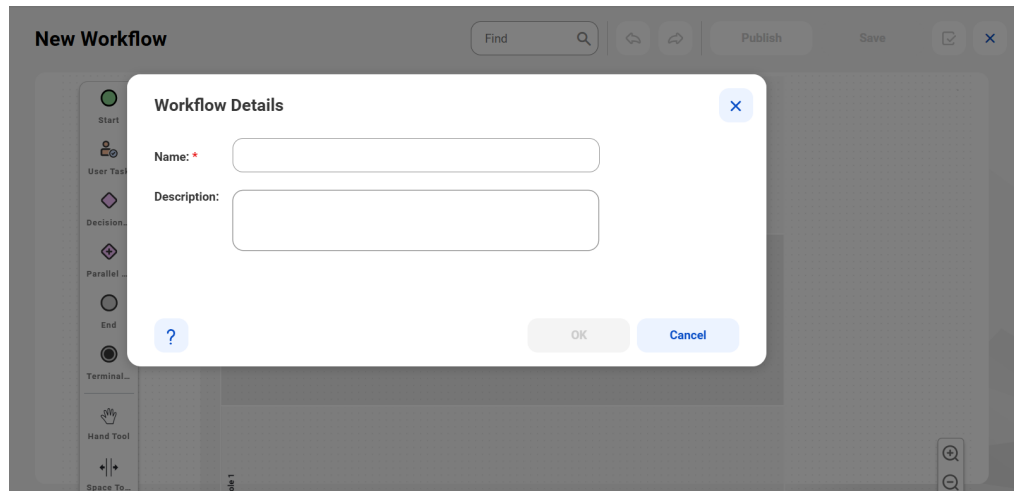
Provide general information such as workflow name and description to start configuring your own workflows.

1. In Metadata Command Center, click **New**.
2. Select **Workflow** from the list of asset types.
3. Select **Workflow** and click **Create**.

The **New** dialog box appears.



4. In the **Workflow Details** dialog box, enter a name and an optional description for the workflow. The **Workflow Details** dialog box appears.



5. To start designing a BPMN-based workflow, click **OK**.

## Designing a workflow

Use various components of the BPMN infrastructure to design a workflow.

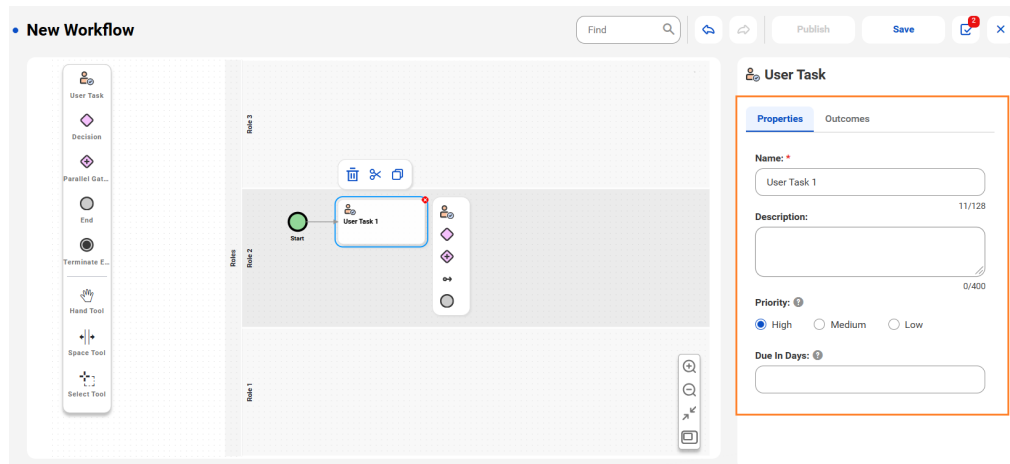
1. On the canvas, select a swimlane to enter a name and an optional description on the **Properties** tab.  
By default, the canvas has three swimlanes named Role 1, Role 2, and Role 3. You can add and delete swimlanes.
2. Drag the **Start** component from the palette to a swimlane on the canvas.  
You can delete, cut, copy, and paste components. You can also undo, redo, and search for components in a workflow.
3. Select the **Start** component and enter a name and an optional description.  
You can add additional components to a swimlane in one of the following ways:
  - Drag the required components from the palette on the left onto the swimlane.

- Select an existing component on the swimlane and choose the next component.
- To include a human decision in a workflow, add a **User Task** component.

**Note:** Workflows must include at least one user task.

- To enter the basic properties of a user task, select the **User Task** component.

The **Properties** tab of a user task appears.



The following table describes the properties that you can enter for a user task:

Property	Description
Name	Name of the user task.
Description	A short description that explains the user task.
Task Priority	Level of importance or urgency assigned to the task. Select one of the following values: <ul style="list-style-type: none"> <li>- High</li> <li>- Medium</li> <li>- Low</li> </ul> The <b>Tasks Inbox</b> page in Data Governance and Catalog shows a visual summary of the total number of tasks categorized by their priorities.
Due In Days	Number of days in which the task is due. If the user doesn't complete the task within the period, the task remains in an overdue status. Maximum value is 14.

- To add a task outcome for a user task, perform the following steps:
  - Click the **Outcomes** tab.
  - Click **Add** and enter a name.
  - To mandate that users enter comments to complete the task outcome, select **Enter comments to complete the task**.
  - Click **Save**.

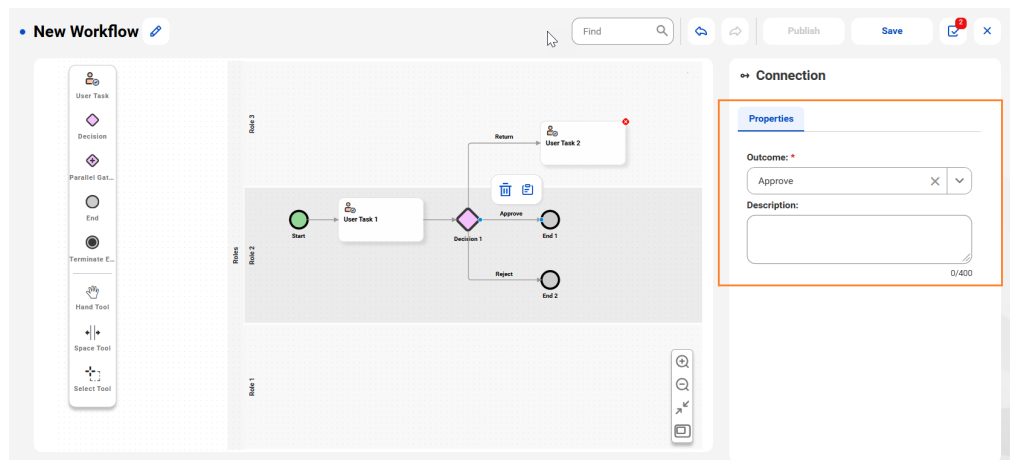
You can create a list of possible decisions that a task owner can take on the task. Outcomes defined in each user task appear as actions of workflow tickets in Data Governance and Catalog.

For example, you can add Approve, Reject, and Return as possible outcomes for a task. Task owners who need to approve a request can evaluate the request raised, make a decision, and take necessary action. They can approve the request if it meets the requirements, reject if not, or return if more information is required. If a request is returned, then another user task can be added to re-evaluate the request and to resubmit the request if it meets the requirements, or discard if not.

**Note:** User tasks in the workflow must have at least one task outcome. You can't use workflows that include user tasks without outcomes.

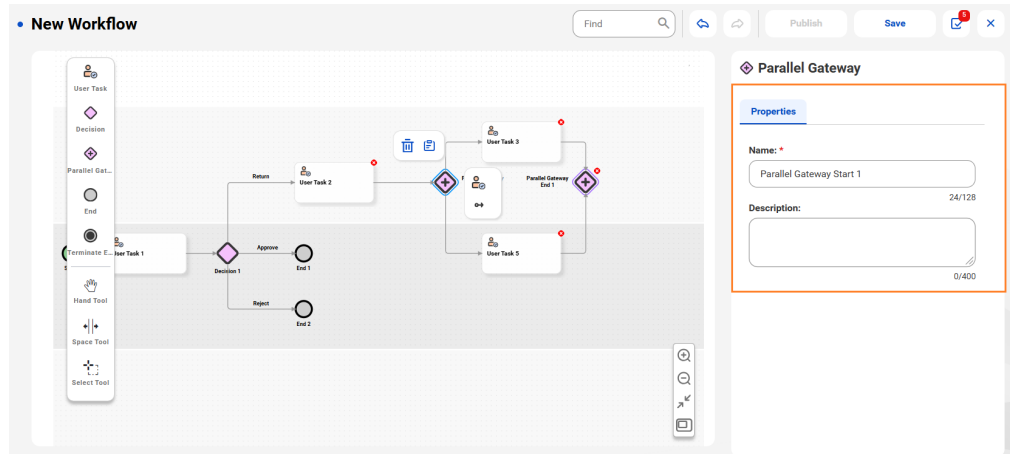
7. To allow a workflow to take different paths, add a **Decision Gateway** component. The workflow takes a decision based on the previous task outcomes you select.
8. Select the **Decision Gateway** component and enter a name and an optional description.
9. To configure the connection properties, perform the following steps:
  - a. Select an outgoing connection from the **Decision Gateway** component.
  - b. Select an outcome.
  - c. Specify an optional description.

The **Properties** tab of an outgoing connection from a **Decision Gateway** component appears.



10. To run multiple tasks concurrently, add the **Parallel Gateway** component and enter names and optional descriptions for the start and end components of the parallel gateway.
11. Select the outgoing connections from the **Parallel Gateway** start component and add user tasks.

The **Properties** tab of a **Parallel Gateway** start component appears.



Optionally, between the divergent and convergent gateway pair that comprise a **Parallel Gateway** component, you can add another **Parallel Gateway** component or a **Decision Gateway** component.

You can add a maximum of three consecutive levels of **Parallel Gateway** components or three **Decision Gateway** components.

For example, in a loan approval process, after the initial application review, a parallel gateway splits the workflow into independent concurrent tasks, such as credit risk assessment, KYC documentation collection, and legal compliance checks. Within these tasks, you can add an additional parallel gateway for credit risk assessment to concurrently analyze different risk factors. You can also add a decision gateway to the credit risk assessment task to branch the process further based on whether additional documentation is required.

If a **Decision Gateway** component has an outgoing path that loops back to the workflow task that precedes it, ensure that you add the task, the gateway, and the outgoing path to the same swimlane.

12. Optionally, to explicitly end the workflow, add a **Terminal End** component to the parallel gateway.  
The **Terminal End** component terminates all active tasks and ends the workflow.
13. Add more user tasks, decision gateways, and parallel gateways based on your business requirement.
14. To mark the completion of the workflow, add the **End** component and enter a name and an optional description.

You can validate and then save and publish the workflow.

## Validating and publishing a workflow

When you design a workflow, the **Validations** panel displays validation errors that the workflow components return. After validating, resolve the errors, and publish the workflow. You can save a workflow with errors and the status of the workflow changes to **Draft**. You can't publish a workflow that has errors.

1. Click the **Validations** icon in the toolbar.  
The **Validations** panel appears with errors grouped by components.
2. Click an error.  
The cursor moves to the erroneous component. Take the required corrective action to resolve the error. The **Validations** panel refreshes each time you correct an error.

3. Click **Save** to save the workflow, and then click **Publish**.

You can use the published workflow to configure workflow events in Metadata Command Center.

**Important:** You can select only published workflows when you configure workflow events.

## Configuring a workflow event

Configure the events that start the workflow, the user roles that can participate in the workflow, and the options available in each task associated with the workflow.

Perform the following tasks to configure a workflow event:

1. Configure general properties of the event and the event types that start the workflow.
2. Choose a published workflow that best fits your workflow event.
3. Configure the workflow components.
4. Save and enable the workflow event to make it available for use.

### Configuring event properties

Configure general properties of the event and the event types that start the workflow.

1. In Metadata Command Center, go to the **Configure** page.
2. Click the **Workflows** tab.
3. To configure a new workflow event, click the Add icon.

The **New Event** page appears.

The screenshot shows the 'Create AI Model' page with the 'Event Details' tab selected. The page has a header with 'Create AI Model', navigation buttons ('Back', 'Next', 'Save'), and a status toggle ('Status: Disabled'). Below the header, there are two tabs: 'Event Details' (active) and 'Workflow'. The 'Event Details' tab contains the following fields:

- Name:** A text input field with the value 'Create AI Model'.
- Event Category:** A dropdown menu with 'Asset Management' selected.
- Event Type:** A dropdown menu with 'Data Quality' selected.
- Description:** A text input field.

At the bottom of the page, there is a section titled 'Select Asset Types' with a search bar and a 'Find' button.

4. In the **Event Details** tab of the **New Event** page, enter the basic properties of the workflow event.

The following table describes the properties that you can enter:

Property	Description
Name	Provide a name for the event that starts the workflow. The event name is a descriptor that identifies the activity for which the workflow should start.  For example, to start a workflow each time a user creates an AI Model asset, you can enter the event name as <code>Create AI Model</code> .
Event Category	Select the category of event for which you want to select the event type. Choose from the following options: <ul style="list-style-type: none"> <li>- <b>Asset Management</b>. Select if you want to configure your workflow for <b>Approval Request for Create</b> or <b>Approval Request for Change</b> event types.</li> <li>- <b>Data Quality</b>. Select if you want to configure your workflow for the <b>Data Quality Failure</b> event type.</li> </ul>
Event Type	Select the type of event for which you want to configure the workflow. Choose from the following options: <ul style="list-style-type: none"> <li>- <b>Approval Request for Create</b>. Select if you want to start a workflow each time a user creates a business asset or a data access asset.</li> <li>- <b>Approval Request for Change</b>. Select if you want to start a workflow each time the user performs the following tasks: <ul style="list-style-type: none"> <li>- Modifies the description or other editable properties on the <b>Overview</b> tab of a business asset.</li> <li>- Modifies the description of a technical asset.</li> <li>- Modifies editable properties on the <b>Overview</b>, <b>Conditions</b>, <b>Rules</b>, <b>Techniques</b>, and <b>De-identification Rank</b> tabs of a data access asset.</li> </ul> </li> <li>- <b>Data Quality Failure</b>. Select if you want to remediate a poor data quality score in a rule occurrence with a workflow.</li> </ul>
Description	Enter a description for the workflow event.
Select Assets	Click the Add icon to select the asset type to which the workflow applies.  In the <b>Select Asset Type</b> dialog box, select the technical, business, or data access assets to which the workflow applies.

- To choose a published workflow, click **Next**.

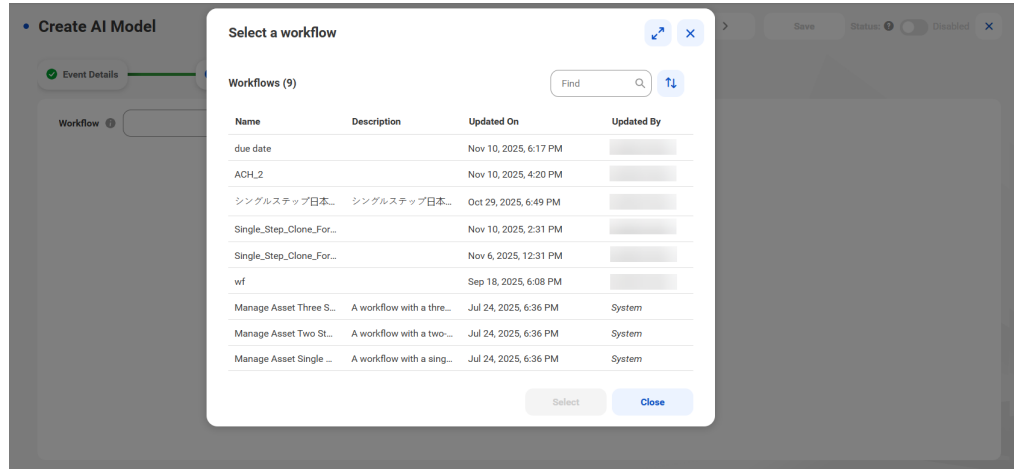


## Choosing a published workflow

Choose a published workflow that best fits your workflow event.

1. On the **Workflow** tab, to select a published workflow, click **Browse**.

The **Select a workflow** dialog box appears.



2. Choose a published workflow that meets your requirement and click **Select**.

The selected workflow appears on the **Workflow** tab. You can view and modify the properties of components in each step of the workflow.

**Note:** Modifying the component properties of a workflow in a workflow event doesn't impact the workflow.

## Configuring workflow components

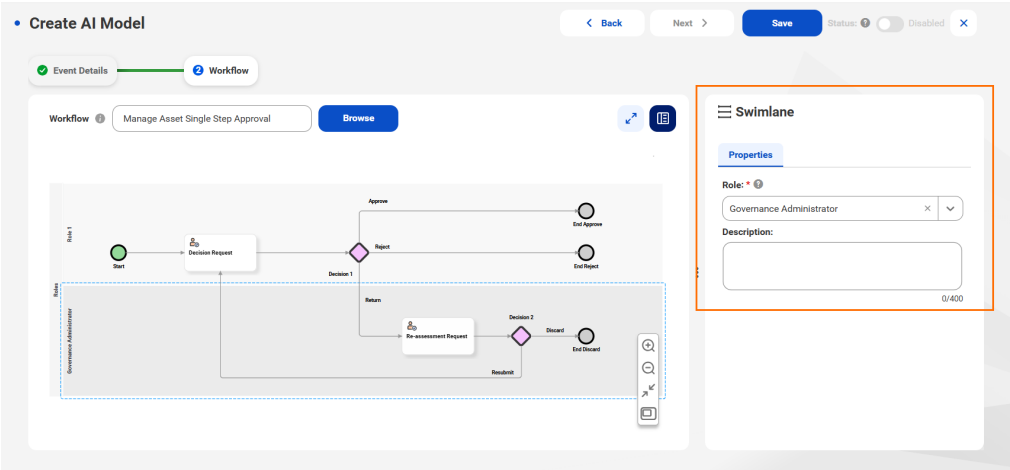
Configure the user roles that can participate in the workflow and the options available in each task associated with the workflow.

1. To configure the properties of a swimlane, select the swimlane.

The following table describes the properties of a swimlane on the **Properties** tab:

Property	Description
Role	<p>Select the user role for the swimlane. When you select a role, only users configured for the selected role can perform the tasks within the swimlane.</p> <p>Roles that have the <b>Participate in Change Approvals</b> privileges and permissions appear in this list. You can also select <b>Requestor</b> from the list of roles. A requestor is a user who creates the ticket. If you assign requestor to a swimlane, when the workflow runs, Data Governance and Catalog identifies the user who created the ticket and assigns the user tasks in the swimlane to the user. The user must have at least the minimum required privileges to view and perform the user tasks.</p> <p><b>Note:</b> When you select the <b>Requestor</b> role, consider the following:</p> <ul style="list-style-type: none"><li>- If you assign a user group as a stakeholder for an asset and assign the <b>Requestor</b> role to a swimlane, the requestor does not need to claim the task in Data Governance and Catalog if the approver returns it. The task is assigned directly to the requestor.</li><li>- You can't reassign a task that is assigned to the requestor, even if you have the privileges to assign or reassign tasks</li><li>- When you design a workflow for the <b>Data Quality Failure</b> event type, ensure that you don't assign the <b>Requestor</b> role to a swimlane.</li></ul>
Description	<p>The description of the swimlane in the workflow.</p> <p>By default, the value specified in the workflow appears here.</p>

The **Properties** tab of a swimlane appears.

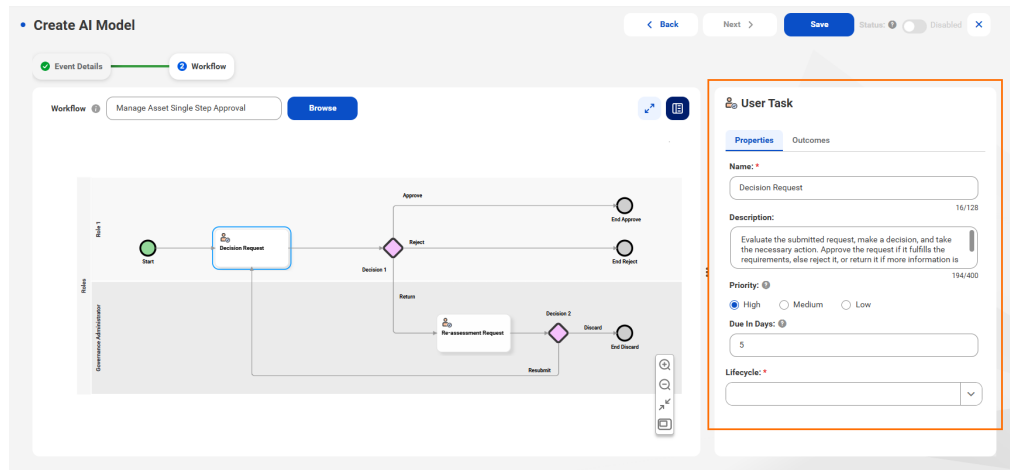


2. Configure the properties of each swimlane in the workflow.
3. To configure the properties of a user task, select the task.

The following table describes the user task properties:

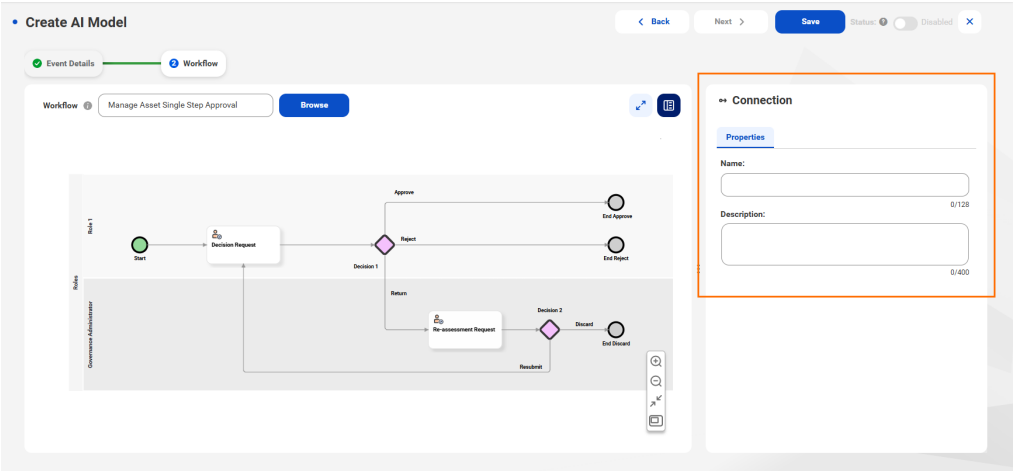
Property	Description
Name	The user task name in the workflow. By default, the value specified in the workflow appears here.
Description	The description of the user task in the workflow. By default, the value specified in the workflow appears here.
Task Priority	The priority of the user task. By default, the value specified in the workflow appears here.
Due In Days	The number of days in which the task is due. If the user doesn't complete the task within the period, the task remains in an overdue state. You must specify a value for each user task. Maximum value is 14. By default, the value specified in the workflow appears here.
Lifecycle	Select the lifecycle that applies to the asset when the workflow user performs the task. The asset moves to the corresponding lifecycle when the task is performed. Select one of the following options: <ul style="list-style-type: none"> <li>- No Change</li> <li>- Discard Draft</li> <li>- Draft</li> <li>- In Review</li> <li>- Published</li> </ul> For more information about lifecycles, see <a href="#">Lifecycle on page 137</a> .

The **Properties** tab of a user task appears.



- On the **Outcomes** tab of a user task, you can edit the task outcome names. By default, the value specified in the workflow appears here. To edit the task outcome name, click Edit.
- Configure the properties of each user task in the workflow.
- To modify the name and description of a connection, select the connection.  
By default, the values specified in the workflow appear here.

The **Properties** tab of a connection appears.

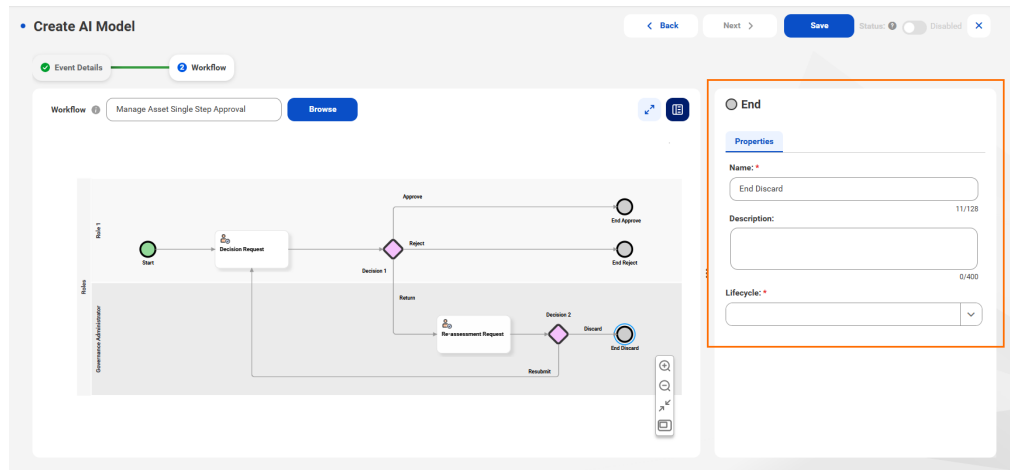


7. Configure the properties of each connection in the workflow as required.
8. To configure the properties of an **End** component, select the component.

The following table describes the properties of an **End** component:

Property	Description
Name	The name of the <b>End</b> component in the workflow. By default, the value specified in the workflow appears here.
Description	The description of the <b>End</b> component in the workflow. By default, the value specified in the workflow appears here.
Lifecycle	Select the lifecycle that applies to the asset when the workflow user performs the task. The asset moves to the corresponding lifecycle when the task is performed. Select one of the following options: <ul style="list-style-type: none"><li>- No Change</li><li>- Discard Draft</li><li>- Draft</li><li>- In Review</li><li>- Published</li></ul> For more information about lifecycles, see <a href="#">"Configuring lifecycles" on page 137</a> .

The **Properties** tab of an **End** component appears.



- Configure the properties of each **End** component in the workflow.

## Configuring lifecycles

Configure lifecycles for applicable steps in a workflow. Select the lifecycle that applies to an asset when a workflow user performs a task.

For example, if a workflow requires approval to create an asset, you can configure the component to change the value of the **Lifecycle** field from "Draft" to "Published" when an approver approves the asset.

Select one of the following options:

### No Change

No change to the **Lifecycle** field of the asset and the associated ticket remains in the "Open" status. This action is useful in multi-level workflows when multiple approvers need to approve the changes of an asset but don't want the asset lifecycle to change to Published until the last component action.

### Discard Draft

Discards the draft version of an asset. If an asset was not previously published, the Discard Draft action permanently deletes the Draft version of the asset and also deletes the associated ticket. If the asset was previously published, the Discard Draft action deletes the Draft version of the asset and resolves the associated ticket. The previously published copy of the asset remains in Data Governance and Catalog in the Published status.

**Note:** Informatica recommends that you select Discard Draft when the component action doesn't require a draft copy of the asset.

### Draft

Changes the status of the asset to "Draft" and the asset becomes editable for the next component owner. The next component owner then has to perform the actions configured for the component.

The associated tickets of the Draft asset will always be in the "Open" status. If the conclusive action of a workflow is Draft for any asset, the associated tickets will be open forever and they can't be reused. In such situations, the requestor or users with the Super Admin privilege can cancel the open ticket to start the workflow activity again for the same asset.

### In Review

Changes the status of the asset to "In Review". The asset will be locked for editing for all stakeholders and its associated tickets will be in the "Open" status.

**Note:** When you start the workflow, the lifecycle status of the asset changes to "In Review".

### Publish

Changes the status of the asset to "Published". If you select the lifecycle as Publish, the asset lifecycle status changes to "Published" and the associated ticket moves to the "Resolved" status.

**Note:** Informatica recommends that you map the lifecycle of the last component in a path to Publish. This is to ensure that the asset can only be published after all stakeholders for each component in that path have responded.

### Important:

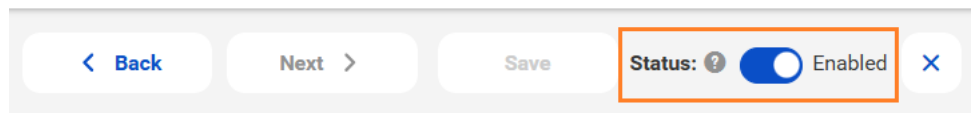
- For Reject and Discard actions, select the lifecycle as "Discard Draft".
- Configure at least one lifecycle as "Publish".
- If you select the lifecycle as Publish for a user task that starts at the beginning of the workflow, the asset lifecycle status changes to "Published" and the associated ticket moves to the "Resolved" status.
- When you use a **Parallel Gateway** component in your workflow, ensure that you map the same lifecycle to all the components in the paths between the divergent and convergent gateways in the **Parallel Gateway** workflow component.

## Saving and enabling a workflow event

You can save and enable the workflow event to make it available for use.

1. To save a workflow event, click **Save**.
2. To enable the workflow event, set the **Status** of the event to **Enabled**.

The following image shows the enable option that appears when you configure a workflow event:



You can also enable workflow events from the **Workflow Events** page. For more information about enabling or disabling workflow events, see ["Enabling or disabling a workflow event" on page 141](#).

Once enabled, you can't edit the workflow event. To edit a workflow event, disable the event and then edit it. The event must have no active tickets.

## Manage workflows

View, update, clone, and change lifecycles of workflows.

On the **Explore** page, you can select workflows in the **Draft** lifecycle and publish them. If you want to create a workflow that is similar to an existing one, you can clone an existing workflow and modify the name and other details.

If you don't want to use existing workflows, select the draft or published workflows and change the lifecycle to **Obsolete**. You can't perform actions on obsolete workflows.

You can view the workflow events that are dependent on a workflow. If you want to change the lifecycle of a published workflow with dependent workflow events to obsolete, first disable all the dependent workflow events, and then change the workflows to obsolete.

## Editing a workflow

You can edit an existing workflow in the **Draft** or **Published** lifecycle.

1. In Metadata Command Center, go to the **Explore** page.
2. To open the list of workflows on the **Workflows** page, select **Workflows** from the menu.
3. Select the workflow that you want to modify and click **Edit** from the **Action** menu.
4. Edit the workflow.
5. To save the workflow as a draft, click **Save**.
6. To check if the workflow has errors, click the **Validations** icon in the toolbar.
7. To publish the workflow, click **Publish**.

The **Disable Events and Publish Workflow** dialog box appears with a list of workflow events that are associated with the workflow.

Disable Events and Publish Workflow

To publish an updated workflow, disable all associated workflow events. After you publish the workflow, enable each workflow event individually.

Workflow Events (1)

Name	Type	Asset Type	Created By
ACH_SYSTEM	Approval Request for Create, Approval ...	AI System, System	

?

Disable and Publish

Close

8. To disable the workflow events and publish the workflow, click **Disable and Publish**.

After you publish the workflow, you need to enable each workflow event individually. For more information about enabling a workflow event, see [“Enabling or disabling a workflow event” on page 141](#).

## Cloning a workflow

If you want to create a workflow that is similar to an existing one, you can clone an existing workflow and modify the name and other details. You can clone workflows of any lifecycle.

1. In Metadata Command Center, go to the **Explore** page.
2. To open the list of workflows on the **Workflows** page, select **Workflows** from the menu.
3. Select the workflow you want to clone and click **Copy** from the **Action** menu.

The **Workflow Details** page of the cloned workflow appears in edit mode.

**Note:** By default, the cloned workflow has the same name with “copy” as the suffix. You can change the name if needed.

4. Update the workflow as per your business requirement.
5. To save the workflow as a draft, click **Save**.

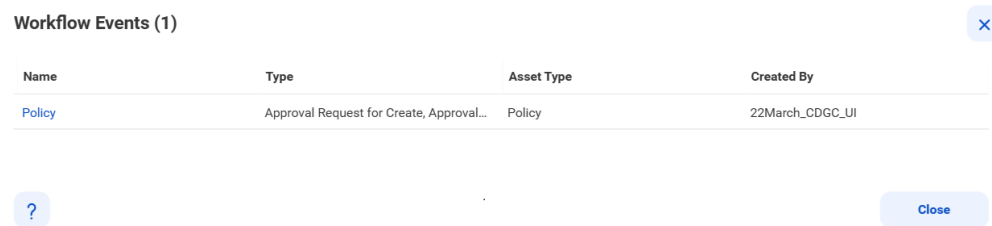
6. To check if there are errors, click the **Validations** icon in the toolbar.
7. To publish the workflow, click **Publish**. You can configure workflow events only on published workflows.

## Viewing dependent events of a workflow

You can view the workflow events that are dependent on workflows.

1. In Metadata Command Center, go to the **Explore** page.
2. To open the list of workflows on the **Workflows** page, select **Workflows** from the menu.
3. Select the workflow for which you want to view the dependent events and click **Show Dependencies** from the **Action** menu.

The **Workflow Events** dialog box appears with the list of dependent events.



Name	Type	Asset Type	Created By
Policy	Approval Request for Create, Approval...	Policy	22March_CDGC_UI

4. To open the workflow event, click the workflow event name.

## Changing a workflow lifecycle to obsolete

Change the lifecycle of workflows that you don't need to obsolete. You can't perform any actions on obsolete workflows. You can change both draft and published workflows to obsolete. You can't change a published workflow that is currently used in a workflow event to obsolete. You must first disable all the dependent workflow events, and then change the published workflow to obsolete.

1. In Metadata Command Center, go to the **Explore** page.
2. To open the list of workflows on the **Workflows** page, select **Workflows** from the menu.
3. Select the workflows and click **Change to Obsolete** from the **Action** menu.

You can select workflows in different states and change them to obsolete.

4. Confirm that you want to change the lifecycle of the workflow to obsolete.

## Manage workflow events

You can view, update, enable, disable, and delete workflow events.

On the **Workflows** tab of the **Configure** page, you can view existing workflow events. You can edit disabled workflow events. To edit an enabled workflow event, first disable the event and then edit it. You can't edit any workflow events that have active tickets. If there are active tickets, wait until the tickets reach their terminal state or close the open tickets, and then edit the workflow event.

You can select multiple disabled workflow events and enable them. Only enabled workflow events create tickets.

If you don't want to use existing workflow events, select the required events and disable them. You can delete workflow events that you don't need. You can't delete workflow events that have active tickets. If there are



active tickets, wait until the tickets reach their terminal state or close the open tickets, and then delete the workflow event.

## Editing a workflow event

You can edit existing workflow events as per changing organizational business needs.

Ensure that the workflow event is in disabled state and that there are no active tickets. You can't edit workflow events that have active tickets. If there are active tickets, wait until the tickets reach their terminal state or close the open tickets, and then edit the workflow event.

1. In Metadata Command Center, go to the **Configure** page.
2. Click the **Workflows** tab.  
On the **Workflow Events** page, you can browse through all existing workflow events and view basic information about each workflow event.
3. To open an event, click the workflow event name.
4. Edit the workflow event as per your business requirement.
5. To save the workflow event, click **Save**.

## Enabling or disabling a workflow event

You can enable or disable workflow events.

1. In Metadata Command Center, go to the **Configure** page.
2. Click the **Workflows** tab.  
The **Workflow Events** page appears with existing workflow events.
3. To open an event, click the workflow event name.
4. On the event page, enable or disable the event.

When you try to enable a workflow event associated with a workflow that was updated, you may not be able to do so. Before you can enable the event, reconfigure the workflow components. For more information about reconfiguring a workflow, see [“Configuring workflow components” on page 133](#).

You can also select multiple workflow events to enable or disable and click **Enable** or **Disable** from the **Action** menu.

**Note:** The **Action** menu appears only if the events that you selected have the same event properties.

The status of the workflow event updates.

## Deleting a workflow event

You can delete workflow events that you don't need. You can't delete workflow events that have active tickets. If there are active tickets, wait until the tickets reach their terminal state or close the open tickets, and then delete the workflow event.

Before you delete a workflow event, ensure that there are no active tickets.

1. In Metadata Command Center, go to the **Configure** page.
2. Click the **Workflows** tab.  
The **Workflow Events** page appears with existing workflow events.
3. Select the workflow events that you want to delete and click **Delete** from the **Action** menu.

**Note:** You can delete enabled workflow events if there are no active tickets.

4. Confirm that you want to delete the workflow event.

## CHAPTER 16

# IDMC metadata

You can enable IDMC metadata in Metadata Command Center to synchronize metadata from Data Integration tasks and Application Integration design-time objects with the catalog.

A data integration task is a process that you configure to analyze, extract, transform, and load data. You can run individual tasks manually or set tasks to run on a schedule. Application Integration allows you to design, integrate, and implement business processes spanning different cloud and on-premises applications.

IDMC metadata synchronizes metadata from tasks in Data Integration and Application Integration design-time objects with the catalog, and incrementally updates design-time and run-time metadata associated with tasks. Design-time metadata from Data Integration implies metadata from mappings and task definitions. For example, definitions of mapping tasks, data synchronization tasks, taskflows, and dynamic mapping tasks. Run-time metadata implies metadata resulting from tasks run, such as lineage and mappings.

IDMC metadata synchronizes metadata from the following design-time task types in Data Integration:

- Mapping
  - ELT (Extract Load Transform) Mapping
  - ETL (Extract Transform Load) Mapping
- Mapping Task
- Project
- Folder
- Synchronization Task
- PowerCenter Task
- Dynamic Mapping Task
- Replication Task
- Masking Task
- Linear Taskflow
- Taskflow

IDMC metadata synchronizes metadata from the following design-time objects in Application Integration:

- Process
- Process Object
- Service Connector
- Connection
- Guide
- Human Task

If you enable IDMC metadata in Metadata Command Center, you don't have to configure the Informatica Intelligent Cloud Services catalog source to extract metadata from Data Integration tasks. IDMC metadata synchronizes the design-time changes that you make to tasks in Data Integration in near-real time with the catalog.

**Note:** IDMC metadata synchronizes run-time metadata for tasks that are run after you enabled IDMC metadata.

After you enable IDMC metadata, you can view details related to the task assets such as the asset overview, hierarchy, lineage, relationship, stakeholders, and referenced source systems in Data Governance and Catalog.

## Synchronized metadata

IDMC metadata synchronizes the following metadata from Data Integration tasks and Application Integration design-time objects:

- ID
- Name
- Description
- Type
- Path
- Hierarchy
- Status
- Created by
- Created on
- Update by
- Updated on
- Dependent objects

## Prerequisites

Before you enable IDMC metadata in Metadata Command Center, ensure that you configure runtime environments and enable IDMC metadata on the required tenant.

### General prerequisites

Perform the following general prerequisite tasks:

- Verify that Data Integration, Application Integration, and Data Governance and Catalog are included in the same IDMC organization for catalog synchronization to succeed.
- Create a directory on the Data Integration service Secure Agent to store files from Data Integration tasks run. IDMC metadata extracts metadata from these files based on the filters you specify in the configuration.
- In Administrator, identify runtime environments that run the Data Integration server.

- The Data Integration mapping task jobs must run on the runtime environments that you selected.

## Runtime environment prerequisites

Complete the following prerequisite tasks on each runtime environment on which the Data Integration server runs:

1. Verify that the Metadata Platform Service is running on the runtime environment that you select.
2. In Administrator, open a runtime environment.
3. Click the ellipsis next to the runtime environment, and click **Edit Secure Agent** from the context menu that appears. The Secure Agent details page appears.
4. In the **System Configuration Details** area, perform the following actions:
  - a. From the Service list, select **Data Integration Server**.
  - b. From the Type list, select **AUTO\_CATALOG**.

See the following image for reference:

Type	Name	Value	Sensitive
AUTO_CATALOG	AutoCatalogServiceMappingFileCopyEnabled	true	<input type="checkbox"/>
AUTO_CATALOG	AutoCatalogServiceMappingFileLocation	/data/mREL_MKQGE_AC_1214v05/appx/Metadata_Plattl	<input type="checkbox"/>

5. Enter the following properties for the runtime environment that you selected:

Property	Description
AutoCatalogServiceMappingFileCopyEnabled	To enable IDMC metadata, enter: 'true'
AutoCatalogServiceMappingFileLocation	Directory that you created on the Secure Agent machine to store files from which you want to extract IDMC metadata. <b>Note:</b> Don't enter the default directory where Data Integration XML files are stored. If you use the default directory, all Data Integration tasks fail.

**Note:** The term "Auto Catalog" refers to IDMC metadata.

6. Click **Save**.
7. Wait for the Data Integration service to return back to the **Up and Running** state, and then restart the Metadata Platform Service.

**Note:** You need to perform this step every time you update the IDMC metadata properties in the Data Integration Service.

## Privileges to synchronize metadata

To allow users within a user role to synchronize metadata from Data Integration tasks and Application Integration objects with the catalog, configure the **Manage IDMC Metadata Settings** privilege for the user role.

**Note:** If you don't have the **Manage IDMC Metadata Settings** privilege, you can view the **IDMC Metadata** tab on the **Monitor** page but you can't retry the IDMC metadata jobs.

For more information about feature privileges, see *Feature privileges* in Introduction and Getting Started.

## Privileges to view IDMC metadata assets

To view the IDMC metadata assets synchronized in the catalog, you need not configure any privileges for the users. The user privileges configured on the tenant where Metadata Command Center runs take effect.

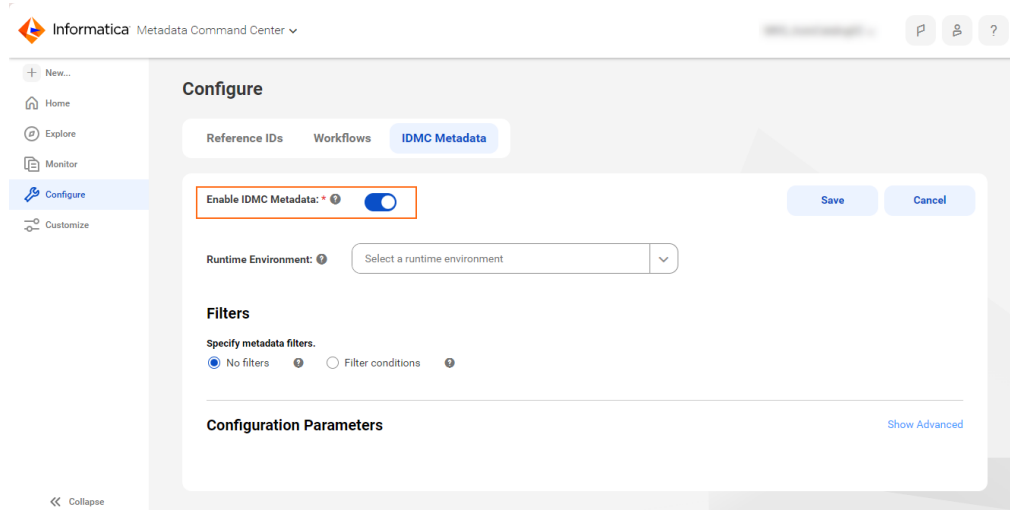
For more information about feature privileges, see *Feature privileges* in Introduction and Getting Started.

# Configuring IDMC metadata

To generate lineage with IDMC metadata, enable and configure IDMC metadata in Metadata Command Center.

1. In Metadata Command Center, go to the **Configure** page.
2. On the **IDMC Metadata** tab, enable IDMC metadata.

The following image shows the configuration page where you enable IDMC metadata:



3. From the Runtime Environment list, select a runtime environment on which you want to process metadata to generate lineage.

**Note:** The run time environment that you select does not need to be the environment used to run the Data Integration workload.

4. In the **Filters** area, define one or more filter conditions to apply for metadata extraction:
  - a. Select **Include Metadata**.
  - b. Select **All Types**.
  - c. Enter the filter values.

Filters can contain the following wildcards:

- Question mark. Represents a single character.
  - Asterisk. Represents multiple characters or empty text.
- d. To define an additional filter with an OR condition, click the Add icon.

The following image shows sample filter options:

**Filters**

Specify metadata filters.

☐ No filters
 ☒ Filter conditions
 ☐

> Show supported wildcards and examples

5. In the **Configuration Parameters** area, enter expert parameters.

This property appears when you click **Show Advanced**.

**Note:** Use expert parameters when it is recommended by Informatica Global Customer Support.

6. Click **Save**.

The IDMC Metadata Bulk Sync and IDMC Metadata Realtime Sync jobs start and you can monitor the status of these jobs on the **Jobs** tab of the **Monitor** page.

You can view lineage results in Data Governance and Catalog.

## Configure run-time metadata synchronization intervals

You can configure how often you want to synchronize run-time metadata into the catalog. You can configure the frequency based on the number of successfully completed Data Integration tasks, the amount of time that the Metadata Command Center service waits before synchronizing the run-time metadata, or both.

1. In Administrator, click Runtime Environments. The **Runtime Environments** page appears.
2. Expand the Secure Agent group that includes the Secure Agent that you use to run IDMC Metadata jobs.
3. Click the Secure Agent. The **Details** page appears.
4. Scroll down to the **System Configuration Details** section.
5. Select **Metadata Platform Services** from the **Service** list and update the following property values:

Property	Description
mps_data360StreamingBatchSize	<p>The batch size based on which the run-time metadata is synchronized.</p> <p>For example, if you enter the value 5, run-time metadata is synchronized after every five successfully completed tasks.</p> <p>Recommended value is 5.</p>
mps_data360StreamingBatchWaitTimeInMin	<p>The maximum amount of time, in minutes, that the Metadata Command Center service waits before synchronizing the run-time metadata. If you configure both properties, this property takes precedence over the mps_data360StreamingBatchSize value. The Metadata Command Center service synchronizes the metadata after the time you set even if the specified number of tasks are not complete.</p> <p>For example, consider the following values:</p> <ul style="list-style-type: none"> <li>- mps_data360StreamingBatchSize = 5</li> <li>- mps_data360StreamingBatchWaitTimeInMin = 15</li> </ul> <p>This means that run-time metadata is synchronized after every 5 successful tasks even if it takes less than 15 minutes. After 15 minutes, run-time metadata is synchronized regardless of how many tasks are complete.</p> <p>Recommended value is 15.</p>

Jobs of the following tasks start only when the synchronization interval criteria is met:

- Mapping Task
- Synchronization Task
- Linear Taskflow
- Taskflow

When the synchronization interval criteria is met, the job starts and the status changes from **Submitted** to **Running**.

**Note:** The Metadata Platform Service restarts every time you update the Metadata Platform Service properties of the Secure Agent.

## Disabling IDMC metadata

Disabling IDMC metadata deletes all IDMC metadata from the catalog.

When you disable IDMC metadata, an IDMC Metadata Purge job starts and the IDMC Metadata Realtime Sync job moves to the completed state. When the IDMC Metadata Purge job completes successfully, Metadata Command Center deletes all the design-time and run-time IDMC metadata extracted, along with enrichments made to the associated metadata. The IDMC Metadata Purge job unassigns and deletes IDMC metadata connections assigned on the **Connection Assignment** tab of the **Monitor** page.

**Note:** You can't disable IDMC metadata if an IDMC Metadata Bulk Sync job or IDMC metadata run-time execution jobs are in the running state.

1. In Metadata Command Center, go to the **Configure** page.
2. On the **IDMC Metadata** tab, disable IDMC metadata.
3. To confirm, click **Disable** in the warning message.

An IDMC Metadata Purge job starts. You can monitor the status of the job on the **Jobs** tab of the **Monitor** page.

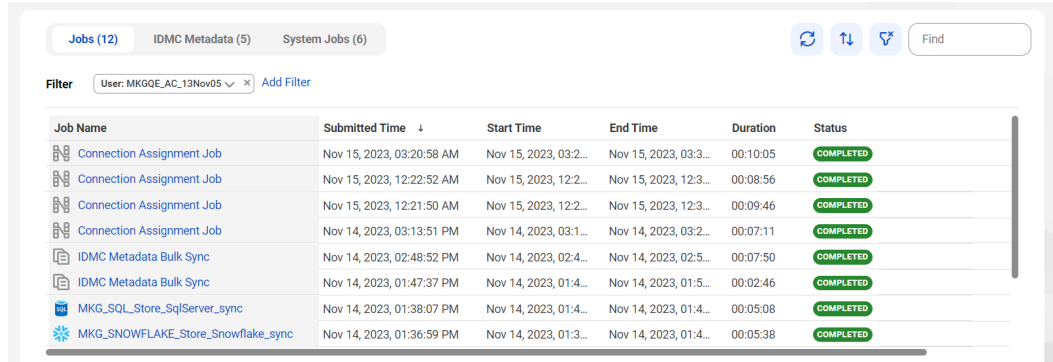
**Note:** You can't cancel an IDMC Metadata Purge job.



# Monitor IDMC metadata jobs

You can view the status of IDMC metadata jobs on the **Monitor** page in Metadata Command Center.

The following image shows the **Jobs** tab of the **Monitor** page:



The screenshot shows the 'Jobs' tab of the Monitor page. It displays a table of jobs with columns: Job Name, Submitted Time, Start Time, End Time, Duration, and Status. The filter is set to 'User: MKGQE\_AC\_13Nov05'. The table lists several 'Connection Assignment Job' and 'IDMC Metadata Bulk Sync' jobs, all with a status of 'COMPLETED'.

Job Name	Submitted Time	Start Time	End Time	Duration	Status
Connection Assignment Job	Nov 15, 2023, 03:20:58 AM	Nov 15, 2023, 03:2...	Nov 15, 2023, 03:3...	00:10:05	COMPLETED
Connection Assignment Job	Nov 15, 2023, 12:22:52 AM	Nov 15, 2023, 12:2...	Nov 15, 2023, 12:3...	00:08:56	COMPLETED
Connection Assignment Job	Nov 15, 2023, 12:21:50 AM	Nov 15, 2023, 12:2...	Nov 15, 2023, 12:3...	00:09:46	COMPLETED
Connection Assignment Job	Nov 14, 2023, 03:13:51 PM	Nov 14, 2023, 03:1...	Nov 14, 2023, 03:2...	00:07:11	COMPLETED
IDMC Metadata Bulk Sync	Nov 14, 2023, 02:48:52 PM	Nov 14, 2023, 02:4...	Nov 14, 2023, 02:5...	00:07:50	COMPLETED
IDMC Metadata Bulk Sync	Nov 14, 2023, 01:47:37 PM	Nov 14, 2023, 01:4...	Nov 14, 2023, 01:5...	00:02:46	COMPLETED
MKG_SQL_Store_SqlServer_sync	Nov 14, 2023, 01:38:07 PM	Nov 14, 2023, 01:4...	Nov 14, 2023, 01:4...	00:05:08	COMPLETED
MKG_SNOWFLAKE_Store_Snowflake_sync	Nov 14, 2023, 01:36:59 PM	Nov 14, 2023, 01:3...	Nov 14, 2023, 01:4...	00:05:38	COMPLETED

IDMC metadata jobs older than 30 days are automatically deleted from the Monitor page.

You can view the status of the following jobs on the **Monitor** page:

## Metadata synchronization jobs

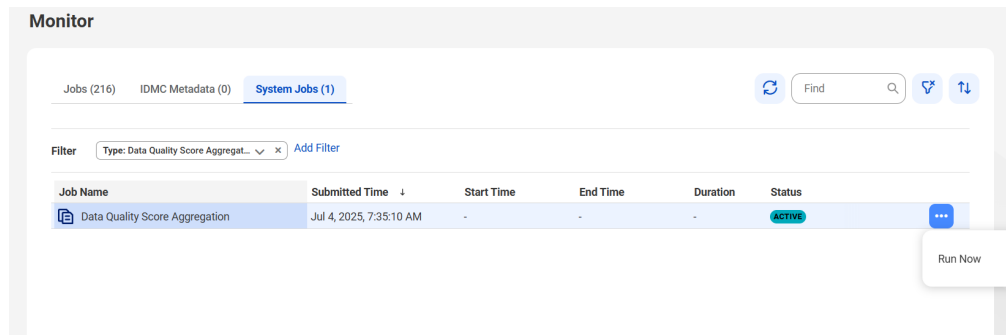
You can view the metadata synchronization job status on the **Jobs** tab. The IDMC Metadata Bulk Sync job synchronizes metadata from the assets into the catalog. After the job status changes to **Completed**, you can click the job to view the **IDMC Metadata Bulk Sync** page. The page lists the number of task assets and the type of assets synchronized into the catalog. For example, after the synchronization, the page lists the number of mapping tasks, mappings, maskings, processes, human tasks, and data synchronization tasks synchronized into the catalog.

## Design-time metadata synchronization jobs

You can view the status of design-time metadata synchronization jobs on the **System Jobs** tab. The IDMC Metadata Realtime Sync job synchronizes design-time metadata updates from the assets into the catalog. After the job status changes to **Completed**, you can click the job to view the **IDMC Metadata Realtime Sync** page.

**Note:** The jobs in the **System Jobs** tab are internal jobs needed for application functioning and maintenance.

On the **System Jobs** tab, you can view the data quality score aggregation job that is created when a data quality score is uploaded through API. When the score aggregation job is in **Active** state, you can run the job manually to propagate the updated scores to the data elements of a data quality rule occurrence, or you can wait for it to run automatically according to the configured time interval.



The screenshot shows the 'System Jobs' tab of the Monitor page. It displays a table of jobs with columns: Job Name, Submitted Time, Start Time, End Time, Duration, and Status. The filter is set to 'Type: Data Quality Score Aggregat...'. The table lists one job, 'Data Quality Score Aggregation', with a status of 'ACTIVE'. A 'Run Now' button is visible next to the job.

Job Name	Submitted Time	Start Time	End Time	Duration	Status
Data Quality Score Aggregation	Jul 4, 2025, 7:35:10 AM	-	-	-	ACTIVE

### Run-time metadata synchronization jobs

You can view the status of run-time metadata synchronization jobs on the **IDMC Metadata** tab. The tab lists the status of metadata synchronization for all mapping tasks and data synchronization tasks run after you enabled IDMC metadata. You can rerun mapping and data synchronization tasks on the **IDMC Metadata** tab. To rerun a task, hover the mouse over the task and click **Retry** from the **Action** menu.

### IDMC Metadata Purge job

You can view the status of the IDMC Metadata Purge job on the **Jobs** tab. An IDMC Metadata Purge job starts when you disable IDMC metadata. The IDMC Metadata Purge job deletes all design-time and run-time IDMC metadata extracted from assets, along with enrichments made to the associated metadata. It also unassigns and deletes the IDMC metadata connections assigned on the **Connection Assignment** tab of the **Monitor** page.

**Note:** You can't cancel an IDMC Metadata Purge job.

## Connect to reference source systems

If a mapping task references another source system, you can perform connection assignment to view the complete data lineage. When the IDMC metadata jobs run, if a mapping task references another source system, a reference catalog source and connection get created that point to the reference source system. To view the complete lineage for your mapping task, you can perform connection assignment from the reference catalog source connection to the objects in the reference source system. You must first create and run an endpoint catalog source that connects to the reference source system. A reference source system might be a database, such as Oracle.

Before you assign a connection, ensure that you have created and run an endpoint catalog source for each reference source system.

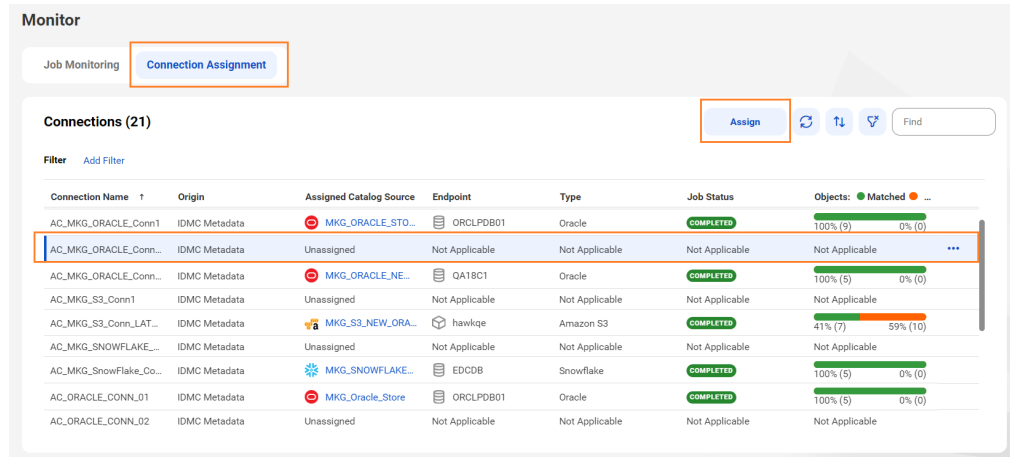
**Important:** The first job that runs is a connectionless scan and might result in a partial or incomplete lineage. To perform a connection-aware scan, after the first job completes, perform connection assignment, and either run the mapping task again in Data Integration or retry the mapping task job in Metadata Command Center or perform realtime connection assignment if the same reference catalog source connection applies for multiple mapping tasks.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab. On the **Catalog Sources** panel, select the required catalog source and click the **Assign Connections** tab.

The **Assign Connections** tab displays a list of assigned and unassigned connections along with details for each connection. Use filters to view the connections based on the connection names. Click the **Add Filter** menu to add filters.

2. Select the connection of the reference catalog source that you want to assign to objects in endpoint catalog sources and click **Assign**.

The following image shows the **Connection Assignment** tab with the **Assign** button and the list of connections:



**Note:** You can find the connection name on the **Hierarchy** tab of the mapping task in Data Governance and Catalog. The connection name is prefixed to the reference catalog source name.

The **Assign Connection** dialog box appears with a list of objects of the endpoint catalog sources.

3. Select one or more endpoint objects to assign to the selected connection and click **Assign**.

You can filter the list in the **Assign Connection** dialog box by name, type, or endpoint.

The following table lists the types of reference source systems that you can connect to and the class type that the endpoint objects must belong to:

Reference source system	Endpoint object class type
Amazon Redshift	Database
Amazon S3	Bucket
Google BigQuery	Database
IBM Db2 for LUW	Database
Microsoft Azure Blob Storage	Container
JDBC	Database
Microsoft Azure Data Lake Storage Gen2	Container
Microsoft Azure Synapse Data Warehouse	Database
Oracle	Database
Microsoft SQL Server	Database
PostgreSQL	Database
SFTP File System	File System

Reference source system	Endpoint object class type
Snowflake	Database
Teradata Database	Database

When you click **Assign**, Metadata Command Center creates links between matching objects in the connected catalog sources, and it calculates the percentage of matched and unmatched objects. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog.

The following image shows the **Assign Connection** dialog box:

**Assign Connection: AC\_MKG\_ORACLE\_Conn\_LATEST\_01** ✕

Select catalog sources to assign to the selected connection.

**Catalog Sources (16)** 1 Selected ↕ 🔍

Filter Type: Oracle ✕ [Add Filter](#)

<input type="checkbox"/>	Name	Class Type	Endpoint ↑	Type	<input checked="" type="checkbox"/> Case Sensitive ?
<input type="checkbox"/>	CDGCORA1	Schema	DEC_PATCH_O...	Oracle	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	QA18C1	Database	DEC_PATCH_O...	Oracle	<input checked="" type="checkbox"/>
<input type="checkbox"/>	QA18C1	Database	MKG_ORACLE...	Oracle	<input checked="" type="checkbox"/>
<input type="checkbox"/>	CDGCORA1	Schema	MKG_ORACLE...	Oracle	<input checked="" type="checkbox"/>
<input type="checkbox"/>	QA18C1	Database	MKG_ORACLE...	Oracle	<input checked="" type="checkbox"/>
<input type="checkbox"/>	CDGCORA1	Schema	MKG_ORACLE...	Oracle	<input checked="" type="checkbox"/>
<input type="checkbox"/>	CDGCORA1	Schema	MKG_ORACLE...	Oracle	<input checked="" type="checkbox"/>

? Assign Cancel

4. After connection assignment, perform any of the following tasks:

- Run the mapping task again in Data Integration.  
After the mapping task completes, a new mapping task job runs in Metadata Command Center. After the new mapping task job completes, a new mapping task instance appears on the **Relationships** tab of the mapping task in Data Governance and Catalog.

**Note:** The previous mapping task instance run on connectionless scan remains in the catalog.

- Retry the mapping task job in Metadata Command Center.  
On the **IDMC Metadata** tab of the **Monitor** page, hover the mouse over the mapping task job and click **Retry** from the **Action** menu.

After the new mapping task job completes, a new mapping task instance appears on the **Relationships** tab of the mapping task in Data Governance and Catalog.

**Note:** The previous mapping task instance run on connectionless scan remains in the catalog.

- Realtime connection assignment. If the reference catalog source connection used in a mapping task is assigned to an endpoint object, the subsequent mapping task jobs which have the same connection runs connection-aware scans.

After the mapping task job completes, a mapping task instance appears on the **Relationships** tab of the mapping task in Data Governance and Catalog. For the subsequent mapping task jobs, only one mapping task instance is generated.

To view the complete lineage of the mapping task, click the **Lineage** tab of the mapping task instance.

## Updating synchronized metadata in the catalog

You might need to update synchronized metadata for different reasons. For example, you might want to change the filter path to include different metadata. You might also need to update the synchronized metadata if the metadata in the filter path has changed. For example, assets are added, moved, or deleted from the path.

### Synchronizing updates when you modify a filter condition

When you modify a filter condition in your IDMC metadata configuration, Metadata Command Center starts a new IDMC Metadata Bulk Sync job. This job synchronizes metadata from Data Integration and Application Integration assets into the catalog, but doesn't remove previously synchronized assets that don't match the updated filter condition. To update the catalog to contain only assets that match an updated filter condition, wait for the IDMC Metadata Bulk Sync job to complete, and then disable IDMC metadata configuration. This starts an IDMC Metadata Purge job. When the purge job completes, enable IDMC metadata configuration. This starts a new IDMC Metadata Bulk Sync job. When the job completes, the catalog updates to contain only assets that match the updated filter condition.

**Note:** You don't need to disable and enable IDMC metadata configuration when you add a new filter condition.

### Synchronizing updates when you add, move, or delete assets out of a filter path

If you add an asset to a path specified in an IDMC metadata filter condition, the asset gets synchronized with the catalog when the scheduled IDMC Metadata Realtime Sync job runs. This is because the IDMC Metadata Realtime Sync job synchronizes design-time metadata updates from the Data Integration and Application Integration assets into the catalog.

After you configure IDMC metadata, if you move assets from a project not included in the filter condition to a project included in the filter condition, the asset doesn't get synchronized with the catalog. For example, if you apply a filter condition with the path as Project1/Folder1/\* and save the IDMC metadata configuration, then all assets under the Project1/Folder1 path will be available in the catalog. Now, if you move an asset, Asset2, from another path to the Project1/Folder1 path, then Asset2 won't be available in the catalog. To update the catalog to include Asset2, rerun the completed mapping and data synchronization tasks.

To rerun a task on the **IDMC Metadata** tab of the **Monitor** page, hover the mouse over the task and click **Retry** from the **Action** menu.

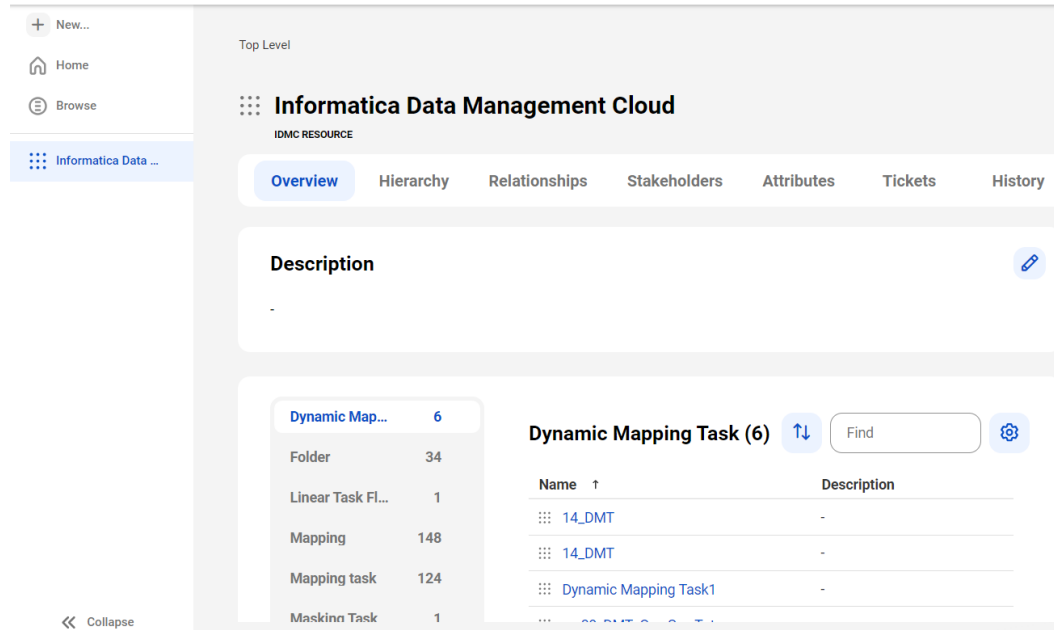
If you delete an asset from a path specified in an IDMC metadata filter condition, the asset gets deleted from the catalog when the scheduled IDMC Metadata Realtime Sync job runs.

## Viewing assets

After metadata synchronization is complete, you can view the details about the synchronized assets in Data Governance and Catalog.

The Data Integration and Application Integration assets appear under the **Informatica Data Management Cloud** source, and these assets are represented as technical assets. You can view the catalog source as a hierarchy which corresponds to the hierarchy defined in Data Integration and Application Integration. Expand each technical asset to see its components.

The following image shows the **Overview** tab of the **Informatica Data Management Cloud** source:



**Note:** You can export IDMC metadata assets to a Microsoft Excel file in Data Governance and Catalog. You can also update the asset description and re-import the file on the **New Import** page in Data Governance and Catalog.

For more information about how to export and re-import assets, see *Working with Assets* and *Bulk Import Assets* in the Data Governance and Catalog help.

## View lineage for mappings

After you run mappings, you can view lineage of the mapping assets.

You can view lineage through the execution instance of a task. A task can include multiple execution instances based on the parameter values used during execution. You can also view lineage from the source or target of the execution instance.

**Note:** You can view lineage of mapping tasks at the mapping task instance level.

To view lineage of mapping assets, perform the following steps:

1. Click the **Relationships** tab of the mapping asset. The following image shows the **Relationships** tab:

The screenshot shows the 'Relationships' tab for the mapping task 'MT\_SQL\_2\_Gen2'. The interface includes a top navigation bar with tabs: Overview, Hierarchy, Relationships (selected), Stakeholders, Attributes, Tickets, and History. Below the tabs, there is a summary bar showing '3 All', '1 Mapping', '1 Mapping task instance', and '1 Folder'. A search bar with a 'Find' button is also present. The main content area is a table with three columns: 'Name', 'Type', and 'How It Is Related'.

Name	Type	How It Is Related
M_SQL_to_ADLS_Gen2	Mapping	MT_SQL_2_Gen2 Depends On M_SQL_to_ADLS_Gen2
MT_SQL_2_Gen2(803e80a7)	Mapping task instance	MT_SQL_2_Gen2(803e80a7) is an instance of MT_SQL_2_Gen2
Execute_mapping01	Folder	Execute_mapping01 is a parent of MT_SQL_2_Gen2

2. Click the mapping task instance. The mapping task instance page appears.
3. Click the **Lineage** tab to view the lineage of the mapping asset. The following image shows the **Lineage**

The screenshot shows the 'Lineage' tab for the mapping task instance 'MT\_SQL\_2\_Gen2(803e80a7)'. The interface includes a top navigation bar with tabs: Overview, Hierarchy, Lineage (selected), Relationships, Stakeholders, Attributes, Tickets, and History. Below the tabs, there is a summary bar showing 'Data Set Level' and 'Overlay Selected: Certification'. A search bar with a 'Find Assets' button is also present. The main content area is a diagram showing the lineage of the mapping task instance. The diagram consists of three main components: 'MKG\_SQL\_Store' (containing 'MKG\_SCHEMA' and 'ALLDATATYPES'), 'Informatica Data Management' (containing 'MT\_SQL\_2\_Gen2' and 'MT\_SQL\_2\_Gen2(803e80a7)'), and 'MKG\_ADLS\_Gen2\_Store' (containing 'EZE' and 'ORGANIZATION\_202011271...'). Arrows indicate the flow of data from 'MKG\_SQL\_Store' to 'MT\_SQL\_2\_Gen2(803e80a7)' and then to 'MKG\_ADLS\_Gen2\_Store'.

tab:

**Note:** You can view the complete lineage of mapping assets that use parameter files along with a list of user-defined parameters and their associated values.

## CHAPTER 17

# Notifications

Configure notifications to alert users in your organization each time the data quality score in a rule occurrence changes between two consecutive runs. Users will receive in-app and email notifications for data quality score changes in scorecard rule occurrences, automated rule occurrences, and rule occurrences within Data Governance and Catalog.

When users create a rule occurrence or update a generated rule occurrence, they can assign a high, medium, or low criticality level to the rule occurrence. If they don't define any criticality level, then they will not receive any notifications for the data quality score changes.

You can specify the data quality configuration settings. You can define downward and upward score thresholds for which the users want to see the notifications. For example, if you set the downward and upward threshold values as 5 for a medium criticality level, the users will get notified if there is a 5% change in the data quality score between two consecutive runs of a rule occurrence with the criticality defined as **Medium**.

Users can also receive notifications if there is an update to the data quality scores through API or bulk import. To enable the notifications, you need to configure the data quality settings on the **Notifications** tab in Metadata Command Center.

## Configuring data quality notifications

Configure the data quality notification settings to enable data quality score change notifications between two consecutive runs.

1. On the **Configure** page, go to the **Notifications** tab.

The screenshot shows the 'Configure' page with the 'Notifications' tab selected. The 'Notification Settings' section is visible, with a 'Save' button and a 'Cancel' button. The settings are as follows:

Criticality	Downwards Change	Upwards Change
<input checked="" type="checkbox"/> Criticality: High	-5	5
<input checked="" type="checkbox"/> Criticality: Medium	-5	5
<input checked="" type="checkbox"/> Criticality: Low	-5	5

At the bottom, there is a 'Reset Values' link.



2. Under the **Notification Settings** tab, select **Data Quality Score Change** as **Yes**. Users can enable the criticality levels as **High**, **Medium**, or **Low** for which they want to receive notifications.
3. Specify the downward and upward score change threshold values for each data quality rule occurrence, and click **Save**.

The score change values that you specify represent the thresholds for which the users are notified. The values are calculated in percentage.

You have configured data quality score change notifications.

## CHAPTER 18

# Usage analytics

Usage analytics help track and report the impact of catalog and governance activities on users and assets in Data Governance and Catalog and Metadata Command Center. Several predefined metrics drive usage analysis and provide data on usage trends across various services and operations.

In Data Governance and Catalog, the metric data is focused and visualized through widgets on dashboards. Thus, the usage analytics dashboards provide a unified experience for viewing specific operation and service data.

Metrics such as **New Users**, **Assets by Lifecycle**, and **Assets with Stakeholders** help capture associated data and provide insights on a number of trends in your organization. You can also filter the data that appears on a widget. For example, on a widget for assets and stakeholder relationships, you can filter the data to view analytics for a specific asset type such as all technical assets with stakeholders.

You can enable usage analytics on the **Configure** page in Metadata Command Center. Usage Analytics starts collecting metric data only after the configuration is saved.

## Configuring usage analytics

Enable or disable usage analytics in Metadata Command Center. Enable usage analytics to generate the usage analytics dashboards in Data Governance and Catalog.

1. In Metadata Command Center, go to the **Configure** page.
2. On the **Usage Analytics** tab, enable usage analytics.

The configuration options for usage analytics appear.

**Configure**

Reference IDs Workflows IDMC Metadata Lineage **Usage Analytics** Notifications

Enable Usage Analytics: ☒ You have started capturing data now. Disabling usage analytics deletes captured metric data. Save Cancel

Mark Metrics as Restricted

Metrics (9)

Name	Description	Metric Type	Application	<input type="checkbox"/> Restricted Display
New Users	Number of new users	User Adoption	Data Governance and Catalog	<input type="checkbox"/>
Assets by Lifecycle	Number of assets for each lifecycle	Assets	Data Governance and Catalog	<input type="checkbox"/>
Assets within Asset Groups	Number of assets within asset groups	Assets	Data Governance and Catalog	<input type="checkbox"/>
Assets with Stakeholders	Number of assets linked to stakeholders	Assets	Data Governance and Catalog	<input type="checkbox"/>
Average Task Resolution Time	Average time to resolve tasks	Assets	Data Governance and Catalog	<input type="checkbox"/>
Average Ticket Resolution Time	Average time to resolve tickets	Assets	Data Governance and Catalog	<input type="checkbox"/>
Data Classifications with Sensitivity	Number of data elements classified for sensitivity	Assets	Data Governance and Catalog	<input type="checkbox"/>
Deleted Users	Number of deleted users	User Adoption	Data Governance and Catalog	<input type="checkbox"/>
User Activities	Number of user activities performed	User Adoption	Data Governance and Catalog	<input type="checkbox"/>

3. Select the metrics you want to restrict from display.  
Restricted metrics are visible only to users who have the **View Restricted Metrics** privilege.
4. Click **Save**.  
**Caution:** When you disable usage analytics, Metadata Command Center starts a job to purge the metric data and deactivates the usage analytics dashboards.

## Privileges for usage analytics dashboards

How you interact with usage analytics dashboards depends on the privileges you're assigned.

For access to usage analytics dashboards, administrators can assign additional privileges to user roles in Administrator.

The following table explains the Metadata Command Center and Data Governance and Catalog feature privileges that an administrator must assign to you for usage analytics dashboards:

Feature	Description
Manage Usage Analytics	Allows users to enable and disable usage analytics.
View Usage Metrics	Allows users to view metric data, to edit widgets on usage analytics dashboards, and to clone and share usage analytics dashboards.
View Restricted Metrics	Allows users to view restricted metric data on usage analytics dashboards.

## Usage analytics dashboards

Usage analytics dashboards serve as a centralized view of various asset and user trends from Data Governance and Catalog and Metadata Command Center. Over a period of time, the dashboards provide a picture of the activity in your organization.

To activate the dashboards, an administrator enables usage analytics on the **Configure** page in Metadata Command Center. Administrators can grant dashboard access through privileges to Data Governance and Catalog users and user groups.

Usage analytics dashboards contain widgets that display a range of metrics. The predefined metrics configured for these widgets vary depending on the dashboard type. When you configure a widget, you can select the metric that you want to visualize for a specific usage trend.

You can customize usage analytics dashboards by cloning the dashboards. On the cloned dashboards, you can add and configure widgets to show metric data for specific asset and user operations such as user count, asset curation trends, and login trends.

You can manage and access the following system-generated usage analytics dashboards from the **Manage Dashboards** menu in Data Governance and Catalog:

- Asset Dashboard
- User Adoption Dashboard

In Metadata Command Center, administrators can control the metrics that are visible to users. When you select a metric to restrict from display, the widget configured with that metric is only visible to users who have the **View Restricted Metrics** privilege.

The following table lists the metrics that administrators can restrict from display in Metadata Command Center:

Metric	Metric Type	Description
Assets by Lifecycle	Asset	Number of assets for each lifecycle
Assets within Asset Groups	Asset	Number of assets within asset groups
Assets with Stakeholders	Asset	Number of assets linked to stakeholders
Average Task Resolution Time	Asset	Average time to resolve tasks
Average Ticket Resolution Time	Asset	Average time to resolve tickets
Data Classifications with Sensitivity	Asset	Number of data elements classified for sensitivity
Deleted Users	User Adoption	Number of deleted users
User Activities	User Adoption	Number of user activities performed
New Users	User Adoption	Number of new users

Consider the following rules and guidelines for usage analytics dashboards:

- Users who have dashboard privileges can share dashboards with other users, roles, and groups.
- Metric data is collected from the time of enablement. If you disable usage analytics, a job is initiated to purge the collected metric data and deactivate the dashboards.
- A scheduled job to collect metric data runs daily. Dashboard data updates only after the job completes each day.
- You can use date filters to access metric data for the last 90 days and view data for a custom date or time range. For certain filters, such as **Last Week**, **Last Month**, and **Last 12 Months**, no data is displayed if the filters refer to periods before data collection.
- You can view differences in values on summary widgets for various time ranges. From the **Time Range** filter, select a date filter or set a custom time range to view differences in values.

For more information about usage analytics dashboards, see the *Asset Discovery* module in Data Governance and Catalog.

# CHAPTER 19

## Jobs

Monitor jobs and task flows that are currently in progress, have completed, or have failed in Metadata Command Center to ensure that background jobs and task flows are running as expected.

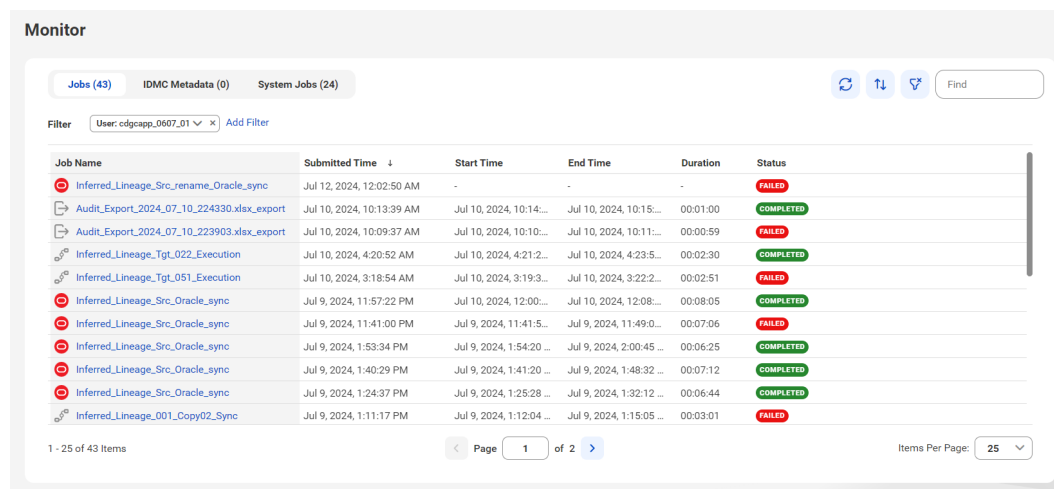
**Note:** When Metadata Command Center upgrades to the November 2021 release, all the previous job execution logs in your tenant are removed from the **Monitor** page. The list of newly executed jobs appears on this page.

To view running and completed jobs, ensure that you define appropriate roles, and select the **Manage Jobs** feature for that role when configuring privileges for the Metadata Command Center service in Informatica Intelligent Cloud Services Administrator. For more information about feature privileges that the organization administrator can configure for user roles, see the *Introduction and Getting Started* help.

### Job history and retention period

System and IDMC metadata jobs have a retention period of 30 days and user jobs have a retention period of 90 days. All jobs older than their retention periods are automatically deleted from the **Monitor** page.

You can monitor the status of jobs for technical assets, the bulk import of business assets, and synchronization for the pushdown of data access assets. The following image shows an example of a **Monitor** page in Metadata Command Center:



The screenshot shows the 'Monitor' page in Metadata Command Center. At the top, there are tabs for 'Jobs (43)', 'IDMC Metadata (0)', and 'System Jobs (24)'. Below the tabs is a filter bar with a dropdown menu set to 'User: edgoapp\_0607\_01' and an 'Add Filter' button. To the right of the filter bar are icons for refresh, sort, and find. The main content is a table with the following columns: Job Name, Submitted Time, Start Time, End Time, Duration, and Status. The table lists 10 jobs, with statuses ranging from 'FAILED' to 'COMPLETED'. At the bottom of the table, there is a pagination bar showing '1 - 25 of 43 Items', a page selector for 'Page 1 of 2', and an 'Items Per Page' dropdown set to '25'.

Job Name	Submitted Time	Start Time	End Time	Duration	Status
Inferred_Lineage_Src_rename_Oracle_sync	Jul 12, 2024, 12:02:50 AM	-	-	-	FAILED
Audit_Export_2024_07_10_224330.xlsx_export	Jul 10, 2024, 10:13:39 AM	Jul 10, 2024, 10:14:...	Jul 10, 2024, 10:15:...	00:01:00	COMPLETED
Audit_Export_2024_07_10_223903.xlsx_export	Jul 10, 2024, 10:09:37 AM	Jul 10, 2024, 10:10:...	Jul 10, 2024, 10:11:...	00:00:59	FAILED
Inferred_Lineage_Tgt_022_Execution	Jul 10, 2024, 4:20:52 AM	Jul 10, 2024, 4:21:2...	Jul 10, 2024, 4:23:5...	00:02:30	COMPLETED
Inferred_Lineage_Tgt_051_Execution	Jul 10, 2024, 3:18:54 AM	Jul 10, 2024, 3:19:3...	Jul 10, 2024, 3:22:2...	00:02:51	FAILED
Inferred_Lineage_Src_Oracle_sync	Jul 9, 2024, 11:57:22 PM	Jul 10, 2024, 12:00:...	Jul 10, 2024, 12:08:...	00:08:05	COMPLETED
Inferred_Lineage_Src_Oracle_sync	Jul 9, 2024, 11:41:00 PM	Jul 9, 2024, 11:41:5...	Jul 9, 2024, 11:49:0...	00:07:06	FAILED
Inferred_Lineage_Src_Oracle_sync	Jul 9, 2024, 1:53:34 PM	Jul 9, 2024, 1:54:20 ...	Jul 9, 2024, 2:00:45 ...	00:06:25	COMPLETED
Inferred_Lineage_Src_Oracle_sync	Jul 9, 2024, 1:40:29 PM	Jul 9, 2024, 1:41:20 ...	Jul 9, 2024, 1:48:32 ...	00:07:12	COMPLETED
Inferred_Lineage_Src_Oracle_sync	Jul 9, 2024, 1:24:37 PM	Jul 9, 2024, 1:25:28 ...	Jul 9, 2024, 1:32:12 ...	00:06:44	COMPLETED
Inferred_Lineage_001_Copy02_Sync	Jul 9, 2024, 1:11:17 PM	Jul 9, 2024, 1:12:04 ...	Jul 9, 2024, 1:15:05 ...	00:03:01	FAILED

The **Jobs** tab on the **Monitor** page displays the list of all jobs and you can view the following details of the job on this page:

Field	Description
Job Name	Name of the job.
Submitted Time	The time at which the job was submitted.
Start Time	Date and time when the job was started.
End Time	Date and time when the job was completed.
Duration	Duration of the job. If the job is complete, the field displays the total time taken to complete the job. If the job is in progress, the field displays the elapsed time since the job started.
Status	Whether the job is completed or failed. If the job is in progress, the field displays the completion percentage.

You can perform the following actions on the **Monitor** page:

- Add or hide fields: Right-click any field name to add or remove fields if you want to see more or less information about the jobs. The Type and User fields for jobs are hidden by default.
- Filter jobs: Click the Filter icon and click **Add Field** to refine the list of jobs that appear on the page by their name, type, start time, end time, the user that started the job, or the status of the job. By default, the **Monitor** page displays all the jobs triggered by the user who is logged in. You can remove the User field from the filter to display the list of jobs triggered by all the users in your organization.
- Cancel an ongoing job: Hover the mouse over any ongoing job listed on this page, click the Action menu and select **Cancel Job**.
- Download or view job logs: Hover the mouse over any job listed on this page and click the Download Job Log icon to download the job log to your local computer. Or, click the View Job Log icon to view the logs for all the tasks in that job. If the job fails or completes with errors, click the View Job Log link to directly go to the **Logs** page to view all the tasks that failed or caused errors.
- View more details of the job: Click the job name to go to the **Overview** page for more details about the job.

You can monitor the status of the following types of jobs:

- [“Monitor jobs for technical assets” on page 162](#)
- [“Monitor the bulk import of business assets” on page 166](#)
- [“Monitor data access jobs” on page 168](#)

For information on IDMC metadata jobs, see [“Monitor IDMC metadata jobs” on page 149](#).

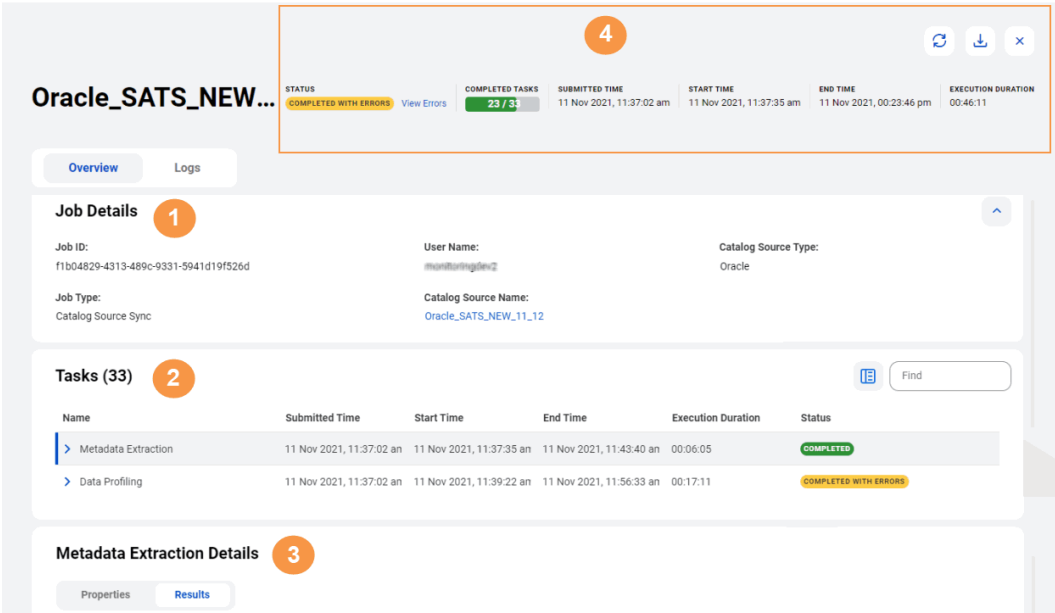
## Monitor jobs for technical assets

View the details of the jobs for technical assets on the **Monitor** page in Metadata Command Center.

Click the job name on the **Monitor** page to go to the **Overview** page for more details about the job, or navigate to the **Logs** page to view detailed logs for each task in the job.

### Overview

The **Overview** page lets you monitor the job completion status, the execution duration of the job, the status of the individual tasks associated with the job, and more. The jobs for technical assets include the catalog source sync job, catalog source delete job, catalog source purge job, the lookup table import job and other details. The following image shows an example of a catalog source job **Overview** page and its panels:



### 1. Job Details

Expand or collapse the **Job Details** section to view the primary details about your job. This panel displays the following data:

Job Detail	Description
Job ID	The unique ID of the job.
Job Type	The type of job for technical assets.
User Name	The name of the user that triggered the job.

### 2. Tasks

View or download tasks associated with the job. The tasks are displayed in a hierarchical manner, with the parent tasks containing subtasks. The parent tasks are usually capability-level tasks, such as Metadata Extraction, Data Profiling, Data Classification, and Glossary Association.

You can hover the mouse over any parent task and click Download Task Log to download logs, View Task Log to view logs, or Retry Task to retry a task that has completed with errors. You cannot download or view logs for subtasks. When you search for a task in the **Tasks** panel, the search result always

displays the parent task along with the subtask that is searched. The **Tasks** panel displays the following details of the parent tasks and their subtasks:

Task Detail	Description
Name	The name of the parent task or the subtask.
Submitted Time	The time at which the task was submitted.
Start Time	The time at which the task started.
End Time	The time at which the task ended.
Execution Duration	The amount of time that the task takes to execute.
Status	The status of the task. It could be Completed, Completed with Errors, Running or Failed.

### 3. Task Details

Select a parent task in the **Tasks** panel to view the following information about the selected task in the **Task Details** panel:

- **Properties.** Depending on the type of the selected task, the **Properties** tab displays information such as the runtime environment and the secure agent name on which the task has executed.
- **Results.** Depending on the type of the selected task, the **Results** tab displays the statistics of the assets collected or generated as a result of the executed task. For example, a metadata extraction task displays the number of columns, tables, views, database, and other assets that the catalog source extracts.

You can download hierarchical logs and debug logs for metadata extraction tasks associated with catalog source jobs. Click **Debug Logs** to download the ZIP file. The contents of the ZIP file vary based on the type of the catalog source.

The reports folder in the ZIP file contains hierarchical logs with the following information:

- **Summary.** Displays a summary of the log levels with the count of log messages. The log levels are categorized as *Information, Warning, Error, Debug, or Fatal*.
- **Hierarchy.** Displays the extracted metadata in a hierarchical structure. For example, database is followed by schema, which in turn nests views.
- **Logs.** Displays the detailed log messages of the metadata extraction task.

You can also download hierarchical logs directly as an Excel file on the **Results** tab.

**Note:**

- You can download debug logs for all catalog sources that use a Secure Agent service as the runtime environment.
- You can download debug logs for only the last 10 scan runs. Previous debug logs are deleted.

You can click the values of assets generated in the **Results** tab to open the **Logs** page to view logs for the following parent tasks:

- Data Profiling
- Data Classification
- Glossary Association
- Import Predefined Content



#### 4. Menu

The menu on the top of the **Overview** page displays the following information about the job:

Job Detail	Description
Status	The status of the job. It could be Completed, Completed with Errors, Running or Failed. If the job fails or completes with errors, click the <b>View Errors</b> link that appears next to the status to go to the <b>Logs</b> page to view at a glance all the tasks that failed or caused errors.
Completed Tasks	The progress bar that shows the completion status of the tasks in the job.
Submitted Time	The time at which the job was submitted.
Start Time	The time at which the job started.
End Time	The time at which the job ended.
Execution Duration	The total amount of time that the job takes to execute, including the execution of the tasks associated with the job.

You can click the Download Job Log icon to download logs for the entire job. You can download logs for jobs regardless of the status of the job.

#### Logs

The **Logs** page for a job displays detailed log for each task that was executed in the job. The following image shows an example **Logs** page of a catalog source sync job:

The screenshot shows the Oracle\_SATS\_NE... Logs page. At the top, there is a header with job details: STATUS (COMPLETED WITH ERRORS), COMPLETED TASKS (23 / 34), SUBMITTED TIME (11 Nov 2021, 11:37:02 am), START TIME (11 Nov 2021, 11:37:35 am), END TIME (11 Nov 2021, 00:23:46 pm), and EXECUTION DURATION (00:46:11). Below the header, there are tabs for Overview and Logs. The Logs tab is selected, showing a list of 5343 logs. The logs are displayed in a table with columns: Timestamp, Task Name, Level, Service Name, and Message. The first few rows show logs with Level 'INFORMATION' and Task Name 'Not Applicable' or 'Metadata Extraction'. At the bottom, there is a pagination bar showing '1 - 100 of 5343 Items' and a 'Page 1 of 54' indicator.

You can perform the following actions on the **Logs** page:

- Click the Filter icon on this page and click **Add Filter** to filter task logs by the task name or level. The level represents the level of the log and is categorized as **Information**, **Warning**, **Error**, **Debug**, or **Fatal**.
- View all the errors at a glance for a job that fails or completes with errors. To do this, filter the logs by level and select the level as **Error** and **Fatal**.
- Click the Download Job Log icon on the top of the page to download the log for the entire job to your local computer.

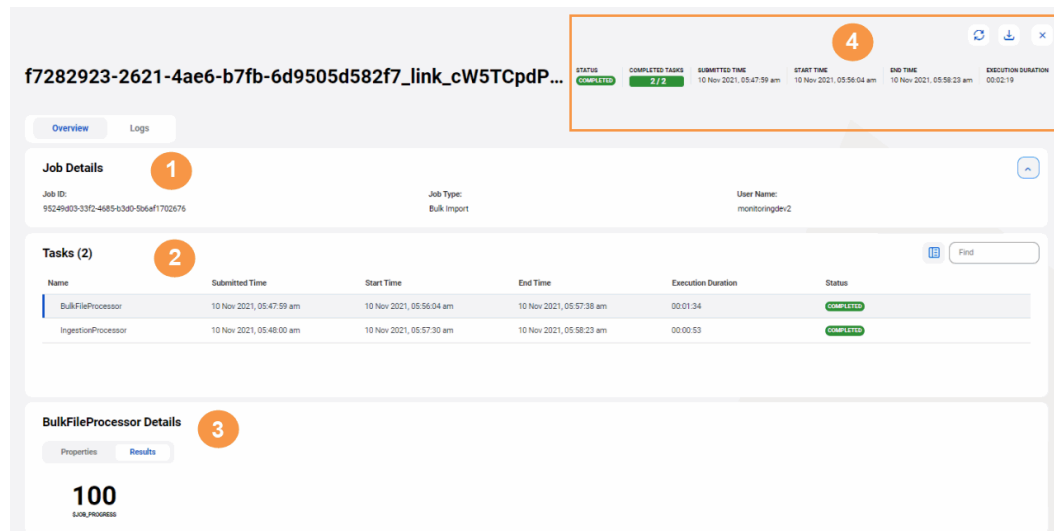
# Monitor the bulk import of business assets

View details of the bulk import jobs for business assets on the **Monitor** page in Metadata Command Center.

Click the job name on the **Monitor** page to go to the **Overview** page for more details about the job, or navigate to the **Logs** page to view detailed logs for each task in the job.

## Overview

The **Overview** page lets you monitor the job completion status, the execution duration of the job, the status of the individual tasks associated with the job, and more. The following image shows an example of a catalog source job **Overview** page and its panels:



### 1. Job Details

Expand or collapse the **Job Details** section to view the primary details about your job. This panel displays the following data:

Job Detail	Description
Job ID	The unique ID of the job.
Job Type	The type of job for business assets.
User Name	The name of the user that triggered the job.

### 2. Tasks

View the tasks associated with the job for bulk import of business assets. The tasks appear in a single level hierarchy.

You can hover the mouse over the parent task and click the Download Task Log icon or the View Task Log icon to download or view the logs for that task. You cannot download or view logs for subtasks. When you search for a task in the **Tasks** panel, the search result always displays the parent task along with the task that is searched. The **Tasks** panel displays the following details of the parent tasks and their subtasks:

The **Tasks** panel displays the following details of the tasks:

Task Detail	Description
Name	The name of the parent task or the subtask.
Submitted Time	The time at which the task was submitted.
Start Time	The time at which the task started.
End Time	The time at which the task ended.
Execution Duration	The amount of time that the task takes to execute.
Status	The status of the task. It could be Completed, Completed with Errors, Running or Failed.

### 3. Task Details

Select a parent task in the **Tasks** panel to view the following information about the selected task in the **Task Details** panel:

- **Properties:** Depending on the type of the selected task, the **Properties** tab displays the properties of the job.
- **Results:** Depending on the type of the selected task, the **Results** tab displays the statistics of the assets collected or generated as a result of the executed task.

### 4. Menu

The menu on the top of the **Overview** page displays the following information about the job:

Job Detail	Description
Status	The status of the job. It could be Completed, Completed with Errors, Running or Failed. If the job fails or completes with errors, click the <b>View Errors</b> link that appears next to the status to go to the <b>Logs</b> page to view at a glance all the tasks that failed or caused errors.
Completed Tasks	The progress bar that shows the completion status of the tasks in the job.
Submitted Time	The time at which the job was submitted.
Start Time	The time at which the job started.
End Time	The time at which the job ended.
Execution Duration	The total amount of time that the job takes to execute, including the execution of the tasks associated with the job.

You can click the Download Job Log icon to download logs for the entire job. You can download logs for jobs regardless of the status of the job.

### Logs

The **Logs** page for a job displays detailed log for each task that was executed in the job. The following image shows an example **Logs** page of a bulk import job:

**01\_Domain**

STATUS: **COMPLETED** | COMPLETED TASKS: **3 / 3** | SUBMITTED TIME: 10 Nov 2021, 02:45:36 am | START TIME: 10 Nov 2021, 02:45:52 am | END TIME: 10 Nov 2021, 03:12:34 am | EXECUTION DURATION: 00:26:42

Overview **Logs**

**Logs (44)**

Filter [Add Filter](#)

Timestamp	Task Name	Level	Service Name	Message
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-lifecycle...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-lifecycle...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-lifecycle...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-lifecycle...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-manage...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>
Jan 2, 2023, 04:20:...	Not Applicable	INFORMATION	ccgf-orchestration-manage...	Job: DQScorePropagator with type: DQScor... <a href="#">Show More</a>

You can perform the following actions on the **Logs** page:

- Click the Filter icon on this page and click **Add Filter** to filter task logs by the task name or level. The level represents the level of the log and is categorized as **Information**, **Warning**, **Error**, **Debug**, or **Fatal**.
- View all the errors at a glance for a job that fails or completes with errors. To do this, filter the logs by level and select the level as **Error** and **Fatal**.
- Click the Download Job Log icon on the top of the page to download the log for the entire job to your local computer.

# Monitor data access jobs

View the details of data access synchronization and agent jobs on the **System Jobs** tab on the **Monitor** page in Metadata Command Center. Data access synchronization jobs identify changes in data access policies that have a pushdown enforcement method. This prepares the changes for the Secure Agent to push to your cloud data platform. Data access agent jobs identify the actions pushed to your cloud data platform.

To view detailed logs for each task in the job, click the job name on the **System Jobs** tab on the **Monitor** page. The **Overview** page displays more details about the job and its tasks. Download the **Job Monitor Logs** to view detailed logs for each task in the job.

## Overview

The **Overview** page lets you monitor the job completion status, the execution duration of the job, the status of the individual tasks associated with the job, and more.

For more information about pushdown enforcement of data access policies, see *Pushdown enforcement method prerequisites* in the *Data Access Management* help.

# Data Access Sync Job

STATUS

COMPLETED WITH ERRORS

View Errors

COMPLETED TASKS

0 / 1

SUBMITTED TIME

Jul 7, 2025, 2:11:31 PM

START TIME

Jul 7, 2025, 2:11:58 PM

END TIME

Jul 7, 2025, 2:12:05 PM

RUN DURATION

00:00:07

Overview

Logs

Job Details

Job ID:

7819649f-0c82-4da9-b787-1628ffb5c6f

User Name:

Job Type:

Data Access Sync

Trace ID:

cdam-sync-72453af3-1a49-46ee-9623-129bde061ffb

Tasks (1)

Find

Name	Submitted Time	Start Time	End Time	Run Duration	Status	Type
Data Access Sync Task	Feb 17, 2025, 2:...	Feb 17, 2025, 2:...	Feb 17, 2025, 2:...	00:00:07	SKIPPED	Data Access Sync

Data Access Sync Task Details

Properties

Results

No data to display

Expand the **Job Details** panel to view the primary details about your job.

Job Detail	Description
Job ID	Unique ID of the job.
Job Type	Type of job for data access assets.
User Name	Name of the user that triggered the job. This is a system-generated user name.
Trace ID	Unique ID for the data access synchronization job. Informatica Global Customer Support uses this for in-depth troubleshooting.

View or download tasks associated with the job.

The following table describes the task details:

Task Detail	Description
Name	Name of the task.
Submitted Time	Time at which the task was submitted.

Task Detail	Description
Start Time	Time at which the task started.
End Time	Time at which the task ended.
Run Duration	Amount of time that the task takes to execute.
Status	<p>Status of the task. It could be any of the following statuses:</p> <ul style="list-style-type: none"> <li>- Success</li> <li>- Completed</li> <li>- Skipped</li> <li>- Running</li> <li>- Failed</li> </ul> <p><b>Note:</b> A status of Skipped indicates the process ignored the task. This occurs when there were no changes to data access policies, users, or data access assets to protect. A skipped task results in a job status of Completed with Errors.</p>
Type	Type of task for the data access synchronization job.

### 3. Task Details

Select a task in the **Task Details** panel to view the following information about the selected task in the **Audit Export Details** panel:

- **Properties.** This tab displays additional information about the task and any error messages.
- **Results.** This tab appears blank because data access synchronization and data access agent jobs don't use it.

### 4. Menu

The menu on the top of the **Overview** page displays information about the job.

The following table describes the overview details:

Job Detail	Description
Status	<p>Status of the job. It could be any of the following statuses:</p> <ul style="list-style-type: none"> <li>- Success</li> <li>- Completed</li> <li>- Completed with Errors</li> <li>- Running</li> <li>- Failed</li> </ul> <p>If the job fails or completes with errors, click the <b>View Errors</b> link that appears next to the status to go to the <b>Logs</b> page. Adjust the filter to include the "Information" and "Debug" levels.</p>
Completed Tasks	Progress bar that shows the completion status of the tasks in the job.
Submitted Time	Time at which the job was submitted.
Start Time	Time at which the job started.

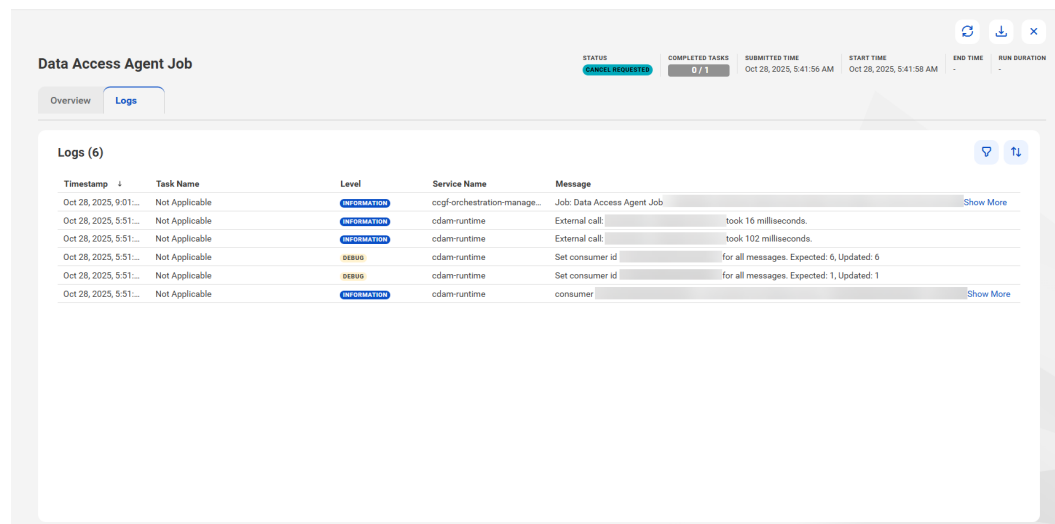
Job Detail	Description
End Time	Time at which the job ended.
Run Duration	Total amount of time that the job takes to run, including the running of the tasks associated with the job.

You can click the **Refresh** icon to refresh the page. Click the **Download Job Logs** icon to download logs for the entire job as a CSV file. You can download logs for jobs regardless of the job status.

## Logs

The **Logs** page displays a detailed log for each task that was run in the job.

The following image shows an example of a data access synchronization job **Logs** page and its panels:



You can perform the following actions on the **Logs** page:

- Filter task logs by the task name, level, or message ID, click the **Filter** icon. To do this, click **Add Filter**. The level represents the level of the log and is categorized as Information, Warning, Error, Debug, or Fatal.
- View all the errors at a glance for a job that fails. To do this, filter the logs by level and include all levels.

## CHAPTER 20

# Upgrade an organization to the latest version

You can upgrade your organization to the latest version of Metadata Command Center, Data Governance and Catalog, and Data Marketplace after Informatica makes the version available on the Point of Deployment (POD) that you connect to.

To upgrade, you can either run the upgrade immediately or schedule it to run at a convenient date and time.

**Note:** To upgrade, you must be the organization administrator or have the Manage Upgrade privilege for your user role.

If you don't initiate or schedule the upgrade, Informatica upgrades your organization six weeks after the version is made available on the POD. For more information about the upgrade window, see *Intelligent Data Management Cloud Release Readiness* in the Administration help.

When an upgrade is available, a notification banner appears in Metadata Command Center. Click the banner to open a confirmation dialog box. You can click the links on the confirmation dialog box to view information on the new features and enhancements that the latest version contains. Click **Manage Upgrade** to upgrade.

You can choose to upgrade immediately or schedule it for a date earlier than the default scheduled date.

If you choose to upgrade immediately, the upgrade starts right away and might take up to two hours for a major release and up to five minutes for a standard release. Ensure that all jobs are complete before you upgrade. Pending jobs prevent the upgrade from starting. During the upgrade, you can't create, update, or delete assets. Save your work to prevent data loss.

If you choose to schedule the upgrade, specify the date and time at which you want to run the upgrade. For example, you can choose a date and time when the upgrade time causes minimal impact.

To find the dates on which Informatica makes the latest version available on each POD, visit the Informatica Community page:

<https://network.informatica.com/s/event-landing>



## CHAPTER 21

# Informatica Resources

In addition to the online help, you can find information about Informatica Intelligent Cloud Services using the following resources.

## Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at <http://www.informatica.com/cloud>. This site contains information about Informatica Cloud integration services.

## Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

<https://network.informatica.com/community/informatica-network/products/cloud-integration>

Developers can learn more and share tips at the Cloud Developer community:

<https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers>

## Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at <https://www.informatica.com/trust-center.html>.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The [Informatica Intelligent Cloud Services Status](#) page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can

subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the [Informatica Intelligent Cloud Services Status](#) page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

## Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit <https://docs.informatica.com>.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

## Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit <https://search.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

## Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at <https://www.informatica.com/services-and-training/support-services/contact-us.html>.