



Informatica® Metadata Command Center
November 2025

Introduction and Getting Started

© 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.

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: 2025-11-28

Table of Contents

Preface	5
Chapter 1: Welcome to Metadata Command Center.....	6
Using the metadata repository.	6
Audience.	7
Prerequisites.	7
Configure runtime environments.	7
Configure the firewall.	9
Understand access policies, roles, users, and user groups.	9
Chapter 2: Accessing Metadata Command Center.....	11
Log in.	11
Home page.	12
Explore.	14
Import predefined content.	15
Chapter 3: Manage access to assets.....	16
Key concepts.	17
Roles, users, and user groups.	17
Access policies.	18
Asset groups.	18
Asset privileges in Administrator.	19
Feature privileges in Administrator.	20
Predefined user roles.	23
Data Access Owner role.	23
Governance Administrator role.	24
Governance Owner role.	27
Governance User role.	28
Predefined access policies.	29
Use cases.	34
Use case: Control access to unpublished glossary changes.	34
Use Case: Cross-unit glossary collaboration	35
Chapter 4: Notifications.....	36
Chapter 5: Editing your user profile.....	37
Chapter 6: Editing your user settings.....	38
Chapter 7: Informatica resources.....	39
Informatica Intelligent Cloud Services web site.	39

Informatica Intelligent Cloud Services Communities.	39
Informatica Intelligent Cloud Services Marketplace.	39
Informatica Intelligent Cloud Services Trust Center.	40
Informatica Product Availability Matrices.	40
Informatica Documentation.	40
Informatica Knowledge Base.	40
Informatica Global Customer Support.	41
Index.	42

Preface

Read *Introduction and Getting Started* to understand Metadata Command Center. Learn how to configure runtime environments and firewalls, and get familiar with the Metadata Command Center home page. You can also learn about roles, users, permissions, and privileges in Metadata Command Center.

CHAPTER 1

Welcome to Metadata Command Center

Metadata Command Center is a metadata management application for the Cloud platform and a one-stop solution for administrators, data stewards, model developers and evaluators. With Metadata Command Center, you can extract, store, and enrich metadata from diverse source systems in your organization.

You can use this service to perform the following tasks:

- Extract metadata from sources such as databases, data integration sources, data lakes, and data warehouses.
- Perform data profiling to determine column statistics, patterns, and data types.
- Classify data elements based on the metadata and data facts.
- Discover relationships among assets.
- Enrich your technical assets with custom attributes.
- Define workflows to create or modify assets.

Using the metadata repository

After you use Metadata Command Center to extract metadata from the source systems in your organization, you can use other services in Informatica Intelligent Cloud Services™ to access the metadata repository.

If you use other services like Data Governance and Catalog, you can leverage the metadata repository to perform the following tasks:

- Build an inventory of assets.
- Understand the relationships between data assets.
- Govern the data according to the requirements of your business.
- Interpret data on which profiling and classification are applied to make effective business decisions.

Audience

The audience for Metadata Command Center can be the following roles:

- **Governance Administrator:** As a governance administrator, you typically perform administration tasks such as catalog source configuration, job monitoring, and more.
- **Data Steward:** As a data steward, you define data classifications, create lookup tables, and extend the default business and technical assets.
- **Data Scientist:** As a data scientist, you develop machine learning models, train and evaluate the models, and participate in data labeling.

Prerequisites

Before you start using Metadata Command Center, the Informatica Intelligent Cloud Services organization administrator must set up the runtime environment and provide you access to Metadata Command Center.

Install a separate Secure Agent for each sub-organization. Sub-organizations can't share a Secure Agent with the main organization. Capabilities don't run as expected in a sub-organization that uses a shared Secure Agent.

For more information about features that the organization administrator can enable, see [“Feature privileges in Administrator” on page 20](#). For more information about assigning feature privileges to users, see *User Administration* in the Cloud Common Services help.

Configure runtime environments

A runtime environment is the execution platform where you run Metadata Command Center tasks.

A runtime environment can consist of one or more Secure Agents or a Serverless runtime environment. A Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. The runtime environment that your organization uses depends on your licenses and the Informatica Intelligent Cloud Services that your organization uses.

If you configured a runtime environment on a Linux server, verify that the `fontconfig` package is installed on the server. If the package is not installed, download and install it manually and restart the Secure Agent machine.

You can set up runtime environments in the following ways:

Use the Informatica Cloud Hosted Agent.

When you use the Informatica Cloud Hosted Agent, you run tasks within the Informatica Cloud hosting facility. Informatica maintains the Hosted Agent runtime environment and agents.

Create one or more Secure Agent groups.

You can install one or more Secure Agents to run within your network or in a cloud computing services environment such as Amazon Web Services (AWS), Google Cloud, Microsoft Azure, or Oracle Cloud Infrastructure. You can install one Secure Agent on each physical or virtual machine.

Note: If you installed the Secure Agent in a cloud computing services environment, ensure that the runtime environment used for metadata extraction is hosted on AWS, Google Cloud, or Microsoft Azure.

When you install a Secure Agent, it is added to its own group by default. You can add multiple agents to one Secure Agent group.

When you configure a connection or some types of tasks, you specify the runtime environment to use. The runtime environment determines which agent runs the tasks at run time. If the runtime environment is the Hosted Agent, the Hosted Agent runs the tasks. If the runtime environment is a Secure Agent group, any available agent in the group can run the tasks.

Secure Agent services

Secure Agent services are pluggable microservices that the Secure Agent uses for data processing. The runtime environment for Metadata Command Center includes the Metadata Foundation Application service and the Metadata Platform Service.

For information on how to configure Secure Agent services, see *Secure Agent Services* in the *Administrator* help.

The runtime environment for Metadata Command Center allows runtime continuity. You can upgrade the Secure Agent services without interrupting running jobs or application payload processes. The upgrade process installs a new version of the services, updates connector packages, and applies configuration changes. To minimize downtime, the services continue to run and restart after existing jobs complete. The updated services run jobs that start after the upgrade process completes.

Metadata Foundation Application (MFA)

The Metadata Foundation Application (MFA) service enables you to extract metadata from source systems configured in your organization, and uploads the extracted metadata to the cloud environment through the Secure Agent. After you download the Secure Agent to your runtime environment and enable the Data Governance and Catalog service, the MFA packages are pushed to the on-premises system where the Secure Agent runs.

You can optimize the performance of the Metadata Foundation Application service by configuring some of its service properties. For more information about configuring Metadata Foundation Application, see *Metadata Foundation Application properties* in the *Administrator* help.

Metadata Platform Service (MPS)

The Metadata Platform Service (MPS) enables you to perform profiling activities for the jobs that you run in Metadata Command Center. Profiling fails if there is no active Metadata Platform Service present in the runtime environment of Metadata Command Center.

You can optimize the performance of the Metadata Platform Service by configuring some of its service properties. For more information about configuring Metadata Platform Service, see *Metadata Platform Service properties* in the *Administrator* help.

To enable the Data Governance and Catalog service, your organization must have the appropriate license.

For more information about how to enable the Data Governance and Catalog service, see [“Enable the Data Governance and Catalog service” on page 8](#).

For more information about configuring and installing a Secure Agent, see *Runtime Environments* in the *Administrator* help.

Enable the Data Governance and Catalog service

After you install a Secure Agent, enable the Data Governance and Catalog service to run the Metadata Foundation Application and the Discovery Agent Application services.

1. In the Administrator, click **Runtime Environments**.

2. On the **Runtime Environments** page, find the runtime environment on which you want to enable the Data Governance and Catalog service.
3. Hover over the **Actions** icon for the runtime environment, and click **Enable or Disable Services, Connectors**.
4. Click **Data Governance and Catalog**.

Secure Agent recommendations

If you are using one or more Secure Agent services, monitor the CPU load on your local machine to ensure efficient performance of the Metadata Command Center services.

Consider the recommendations to efficiently manage the load of the local machine CPU where the Secure Agent services are installed.

The following table describes the recommendations to maintain the CPU load:

Condition	Resolution
If the CPU load for the profiling Secure Agent service is less than 20% and the Metadata Command Center Secure Agent service is less than 30%.	Continue using the existing Secure Agent services.
If the CPU load for the profiling Secure Agent service is more than 50%.	Add a new Secure Agent to run the Metadata Command Center services.
If the CPU load for the profiling Secure Agent service and the Metadata Command Center Secure Agent service is cumulatively more than 50%.	Add a new Secure Agent to run a new instance of the Metadata Command Center services.
If the CPU load for the Metadata Command Center Secure Agent service is more than 50%.	Add a new Secure Agent to run a new instance of the Metadata Command Center services.
If the CPU load for the Metadata Command Center Secure Agent service is less than 50%.	Continue using the existing Secure Agent service and monitor the CPU load. If the load is more than 50%, add a new Secure Agent to run a new instance of the Metadata Command Center services.

Configure the firewall

If your organization uses a Secure Agent and the Secure Agent is behind a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. To ensure that the Secure Agent can perform all necessary tasks through the firewall, enable the port that the Secure Agent uses.

For information about the list of approved IP addresses, see [POD Availability and Networking](#).

Understand access policies, roles, users, and user groups

To allow access to your organization and assets, create appropriate roles and user groups, and assign users to these roles and user groups in the Administrator. Also, create access policies in Metadata Command Center.

Access Policies

An access policy is a set of rules that you can use to control access to assets and define permissions on those assets in your organization. When you create access policies and set the correct permissions, they

define boundaries within which users can act. For example, you can create an access policy to grant data stewards permissions to create, read, update, and delete business terms in your organization. You can define multiple access policies to implement access control.

Roles

A role is a set of feature privileges and asset permissions that you can assign to users and user groups in the Administrator to manage assets. For example, your organization might require policies that use the Governance Administrator role to provide asset permissions to users, and the Governance User role to participate in approval workflows. In addition to the system-defined roles, the organization administrator can also assign custom roles to users or user groups. You can view the list of user roles that the administrator has configured for Metadata Command Center.

Users and user groups

Users receive secure access to assets in an organization. A user group is a group of users in which all members can perform the same tasks and have the same access permissions for assets. You can create and manage users and user groups in the Administrator. After the roles are defined, the organization administrator can assign specific users and user groups to the role. For example, the organization administrator might assign Peter and Natalie to the Governance Administrator role, and Jack to the Governance User role. When the users are assigned to the roles, Peter and Natalie have the permission to define asset permissions, but Jack can only view the assets. You can view the list of users and user groups that the administrator has configured for Metadata Command Center.

For more information about creating roles, users and user groups in Informatica Intelligent Cloud Services, see *User Administration* in the Cloud Common Services help.

CHAPTER 2

Accessing Metadata Command Center

You can access Metadata Command Center by logging in to Informatica Intelligent Cloud Services from a web browser.

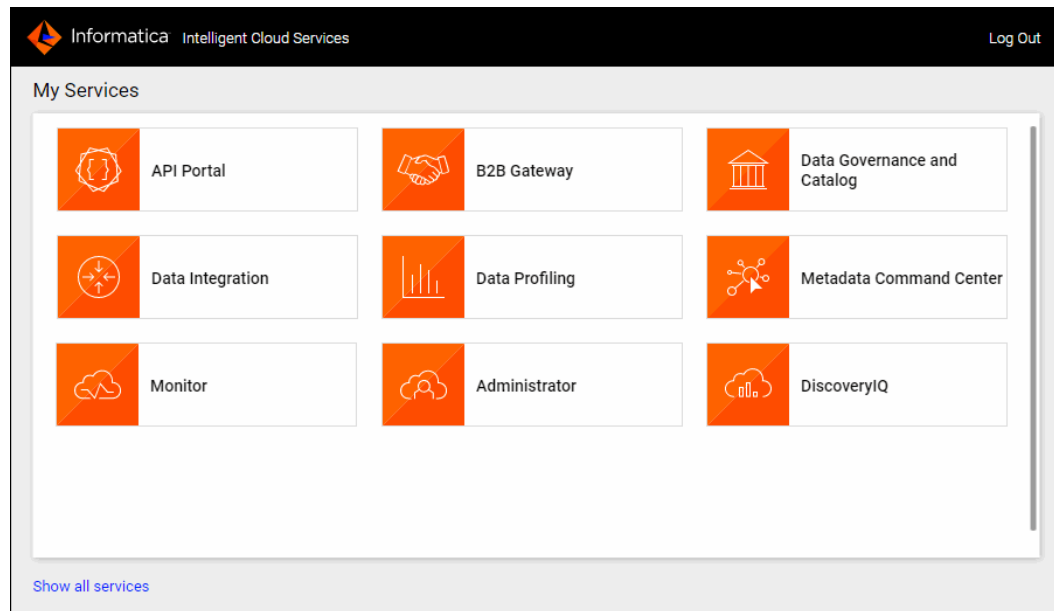
The home page of Metadata Command Center displays a dashboard of several key activities and tasks that you can monitor. Depending on your user role and privileges, you can perform various tasks to extract and create a repository of metadata. To run metadata tasks in compliance with the security protocols in your organization, you can download Secure Agent services to run the tasks in your local machine.

Log in

Log in to Metadata Command Center from the services displayed in the Informatica Intelligent Cloud Services page.

When you log in to Informatica Intelligent Cloud Services, the **My Services** page displays the services that your organization is licensed to use, and common services that are available under the same license, such as Administrator. If your organization has trial licenses for additional services, the page displays those services.

The following image shows an example of the **My Services** page:

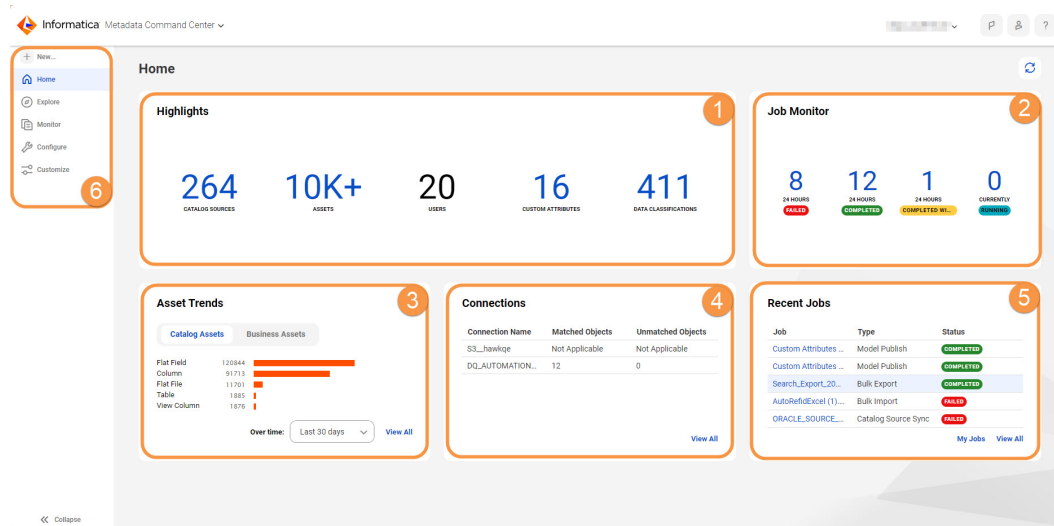


To use Metadata Command Center, click the **Metadata Command Center** box.

Home page

The Metadata Command Center home page presents a dashboard of various jobs, connections, and assets. The dashboard provides a view that you can use to quickly see the status of the activities and trends.

The following image is a sample of the dashboard and its panels:



1. Highlights

Get a quick view of your most important data in Metadata Command Center. This panel displays the following data:

- **Catalog Sources:** Number of catalog sources that you configured
- **Assets:** Number of assets
- **Users:** Number of users that you configured
- **Custom Attributes:** Number of custom attributes that you created for your assets
- **Data Classifications:** Number of data classification expressions that you created

2. Job Monitor

See the status of jobs in Metadata Command Center.

The panel displays the following job statuses:

Column	Description
Failed	The number of jobs that failed in the last 24 hours. Click the number to see the list of all the jobs that failed.
Completed	The number of jobs that completed in the last 24 hours. Click the number to see the list of all the jobs that completed successfully.
Running	The number of jobs in progress that started before the last 24 hours. Click the number to see the list of all the jobs that are running.
Completed with errors	The number of jobs that completed with errors in the last 24 hours. Click the number to see the list of all the jobs that have completed with errors.

3. Asset Trends

Get a graphical view of the growth of the catalog and business assets in Metadata Command Center. This panel displays the following information:

- **Catalog Assets:** View the top catalog asset types that are extracted from the catalog sources over the specified period of time.
- **Business Assets:** Select this tab to view the growth of assets based on the metadata extracted from the catalog sources over the specified period of time.
- **View All:** Click **View All** to see all catalog and business assets in Data Governance and Catalog.
- **Over time:** From this list, select a value to view assets growth data for the last 7 days, last 30 days, or last year.

4. Connections

See the connections from catalog sources that have been assigned or unassigned to the database schema.

The panel title displays the following information about the connections:

- **Matched Objects:** The percentage of objects that matched between the connected catalog sources.
- **Unmatched Objects:** The percentage of objects that did not match between the connected catalog sources.

5. Recent Jobs

See the status of recent jobs that you started or are triggered by your activities.

The panel displays the following properties for the job:

Column	Description
Job	Name of the job Click any job name to open the job in a new page and view complete details of that job.
Type	Type of the job
Status	Completion status of the job

To go to the **Monitor** page and see the complete list of jobs that are triggered by all users in the tenant, click **View All**. For a complete list of jobs that you started, click **My Jobs**.

6. Navigation Bar

Navigate to the various components of the Metadata Command Center application to perform different actions.

The navigation bar displays the following menu:

Navigation Page	Description
New	Create a new asset type.
Home	View the dashboard to see snapshots of recent jobs, asset trends, and assigned or unassigned connections. Also, view highlights of catalog sources, assets, users, and custom attributes.
Explore	Browse for asset types.
Monitor	See the details and completion status of jobs. For more information about the status of jobs, see the <i>Administration</i> help.
Configure	Specify reference ID and manage workflows for working with assets. For more information about configuring reference IDs and workflows, see the <i>Administration</i> help.
Customize	Manage custom attributes and modify page display layouts for assets. Create and manage custom catalog source types and metadata models for a custom catalog source. For more information about performing these tasks, see the <i>Administration</i> help.


Explore

The **Explore** page lets you browse assets by asset type in Metadata Command Center.

Use this page to find and work with the following assets:

- Catalog sources
- Data classifications
- Relationship inference models


- Lookup tables
- Workflows

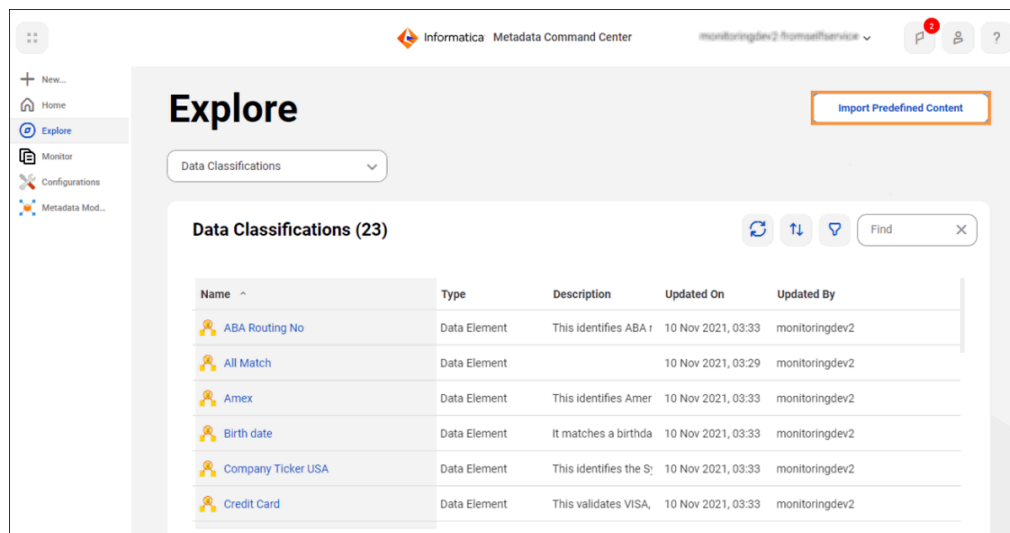
You can view, edit and update assets based on a particular type by clicking the  icon. For each asset, you can view basic details, such as, name, description, and type. For more details about each asset, click the asset to view the complete configuration details.

Import predefined content

Metadata Command Center provides predefined data classifications, lookup tables, and a relationship inference model. You can import these predefined assets and use them in data classification and relationship discovery capabilities.

To import predefined assets, perform the following steps:

1. In Metadata Command Center, go to the **Explore** page.
2. Click the  icon on the top of the page and select **Data Classifications**, **Relationship Inference Model** or **Lookup Tables**.
3. On any of these pages, click **Import Predefined Content**.



4. On the confirmation dialog box, click **Yes**.
This triggers a job to import and install the predefined assets. You can track the status of the job on the **Monitor** page. For more information about monitoring jobs, see the *Administration* help.
5. After the job is successful, you can view the imported assets on the **Explore** page by browsing asset types.

You can use the imported data classifications directly in catalog sources. Use the imported lookup tables in inclusion rules while creating data classifications. For more information about each of these assets, see the *Administration* help.

CHAPTER 3

Manage access to assets

As your organization's data rapidly evolves, a robust and centralized mechanism to control access to assets becomes crucial to effectively manage the assets in your organization. Metadata access control is the practice of managing the level of user access to assets in your organization through a set of rules called access policies.

With metadata access control, you can view and perform actions on specific assets or groups of assets only if your organization administrator has explicitly granted access and permissions to you through access policies. This ensures that with appropriate permissions the right users have access to the right assets.

The following concepts apply as you implement metadata access control in your organization:

- Roles, users, and user groups. See ["Roles, users, and user groups" on page 17](#).
- Access policies. See ["Access policies" on page 18](#).
- Asset groups. See ["Asset groups" on page 18](#).

How it works

The organization administrator can implement access control in your organization through a combination of privileges in Administrator and access policies in Metadata Command Center. Let us look at the tasks that the administrator performs to enforce metadata access control.

In Administrator,

1. Create users, user roles, and user groups.
2. Assign users and user groups to user roles.
3. Grant minimum asset and feature privileges to user roles.

In Metadata Command Center,

1. Extend the Administrator user role definitions and create access policies to determine the level of access that users have on assets. Optionally, use asset groups or attribute groups in access policies to control access to a group of assets or to certain attributes of assets.
2. Publish the access policies to enforce metadata access control.

In Data Governance and Catalog,

1. Users interact with assets based on the permissions and level of access defined in access policies.
2. If using asset groups, assign asset groups to assets to enforce access control over the assets.
3. Assign a user as the stakeholder of the asset to grant asset permissions that are unique to the stakeholder.

Key concepts

To understand how your administrators can manage access to assets using metadata access control, you need a basic understanding of the following key concepts.

Roles, users, and user groups

To use Data Governance and Catalog, the organization administrator must create the users, user groups, and user roles in Administrator for your organization.

A user is an individual Informatica Intelligent Cloud Services account that can perform tasks and access assets based on the roles that are assigned to the user. You can assign roles directly to the user or to a group that the user is a member of. Administrators can create user accounts for the organization in Administrator.

A user group is a group of users who can perform tasks and access assets based on the roles that you assign to the group. Administrators can create user groups for the organization in Administrator.

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. Data Governance and Catalog provides three predefined user roles that you can assign to users and user groups in Administrator. See ["Predefined user roles" on page 23](#). To create custom roles, you can create a new role or clone an existing custom role in the Administrator.

With metadata access control, there are two types of roles that administrators can use to grant different types of access to users.

User roles

A user role defines the permissions and privileges for different types of assets and features. 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.

The user roles that the organization administrator creates for your organization appear on the **Users** tab on the **Access Control** page in Metadata Command Center. You can use the user roles in access policies to grant users access and permissions for different types of assets.

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. 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. In Metadata Command Center, you can create stakeholder roles from user roles and use them in access policies to grant users granular access to assets. If a stakeholder is assigned to an asset, the level of access and permissions for users who are not stakeholders of the asset are determined by the stakeholder role policies configured with the non-stakeholder option.

View user roles, stakeholder roles, and stakeholders on the **Users** tab on the **Access Control** page in Metadata Command Center.

For information about using user roles, user groups, and stakeholder roles in access policies, see the *Administration* help in Metadata Command Center.

Access policies

Access policies are sets of rules that the administrator creates in Metadata Command Center to define permissions and control the level of access to the assets in the organization.

Access policies are an extension of the asset and feature privileges that are granted to your user role through Administrator. Along with the asset and feature privileges that are assigned to the user roles in Administrator, your organization administrator must create and assign access policies in Metadata Command Center that determine whether users can read, create, update, delete or manage access for the assets. Administrators can use predefined policies or define custom policies specific to their organization in Metadata Command Center. Predefined policies are associated with predefined user roles defined in Administrator. See [“Predefined user roles” on page 23](#).

Administrators can grant access to assets, asset groups, or individual attributes of an asset using the following types of access policies:

- 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 in Metadata Command Center. A stakeholder role policy grant asset permissions that are unique to the stakeholder of the asset.
- User group policy. Defines the access level of users who are assigned a user group in Administrator. You can also use this access policy to control the access level to all users in the organization.

For information about managing access policies, see the *Administration* help in Metadata Command Center.

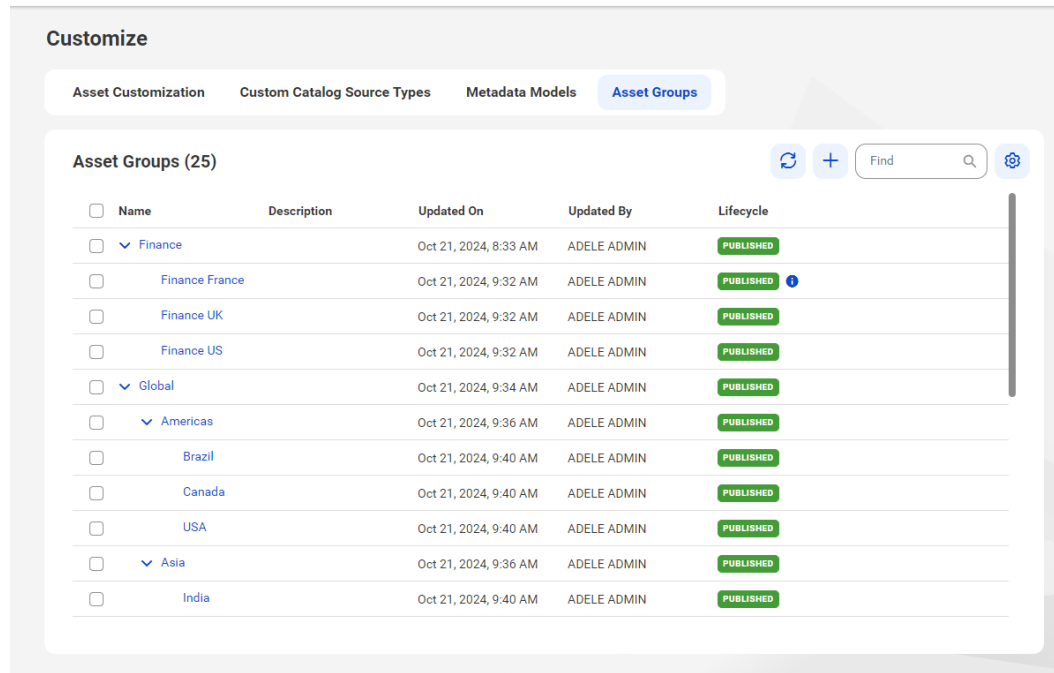
Asset groups

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:



Asset privileges in Administrator

An organization administrator can assign some asset privileges for the Metadata Command Center service to user roles in Administrator. To perform cataloging and governance tasks, the administrator must create and assign access policies to users in Metadata Command Center.

To assign asset privileges for user roles in Administrator, select the service, and select one or more privileges on the **Assets** tab for the service. For more information about assigning asset privileges to user roles, see *User Administration* in the Administrator help.

For information about creating access policies and assigning them to user roles, user groups, or stakeholder roles, see *Administration* in the Metadata Command Center help.

The following table explains the asset privileges that are available for the Metadata Command Center service in Administrator:

Asset	Description
Catalog Source Configuration	Asset privileges to create, update, delete, purge, and run a catalog source.
Custom Catalog Source Types	Asset privileges to create a custom catalog source type that represents the custom source system.
Custom Models	Asset privileges to create a custom model for custom metadata integration.

Feature privileges in Administrator

An organization administrator can assign privileges for some features of Data Governance and Catalog and Metadata Command Center to user roles in Administrator. To perform cataloging and governance tasks, the administrator must create and assign access policies to users in Metadata Command Center.

To assign feature privileges to user roles in Administrator, open a role, select the service, and select one or more features on the **Features** tab for a service. For more information about assigning feature privileges to user roles, see *User Administration* in the Administrator help.

For information about creating access policies and assigning them to user roles, user groups, or stakeholder roles, see *Administration* in the Metadata Command Center help.

Feature privileges for Metadata Command Center

The following table explains the feature privileges that are available for the Metadata Command Center service in Administrator:

Feature	Description
Access Metadata Command Center application	Grants access to Metadata Command Center. If disabled, users can't access Metadata Command Center.
Manage Custom Attributes	Allows users to manage asset relationships, predefined attributes, and custom attributes for asset types that appear in Data Governance and Catalog.
View Custom Attributes	Allows users to view attributes for asset types in Data Governance and Catalog.
Manage Data Classifications	Allows users to create and manage data classification inclusion rules.
View Data Classifications	Allows users to view data classifications in Data Governance and Catalog after you enable the capability and run the catalog source job in Metadata Command Center.
Manage Lookup Tables	Allows users to import and publish lookup tables that you can use in data classification.
View Lookup Tables	Allows users to view lookup tables in Metadata Command Center.
Monitor Jobs	Allows users to monitor jobs.
Manage Lineage Settings	Allows users to perform the following tasks: <ul style="list-style-type: none">- Assign or unassign connections to one or more catalog sources.- Link catalog sources to generate lineage.
View Lineage Settings	Allow users to view data lineage from the Lineage tab.
Manage Access Control	Allows users to create and manage stakeholder roles and access policies. Also allows users to share saved searches, dashboards, and set default dashboards for other users.
View Access Control	Allows users to view access policies.
Manage Asset Groups	Allows users to create, update, or delete asset groups.
View Asset Groups	Allows users to view asset groups.
Manage Workflows	Allows users to create or modify workflows.

Feature	Description
View Workflows	Allows users to view workflows.
Workflow Designer	Allows users to design new workflows.
Manage System Settings	Allows users to modify system settings.
View System Settings	Allow user to view the Reference IDs tab.
Manage Asset page customization	Allows users to create, update and delete the layout of pages and preview panes of assets. Also allows users to assign default layouts to other users based on their roles, user groups, or to all users in the organization.
View Asset page customization	Allows users to view the layout of pages.
Manage IDMC Metadata Settings	Allows users to synchronize metadata from Data Integration tasks and Application Integration objects with the catalog.
View IDMC Metadata Settings	Allow users to view IDMC metadata.
Manage Upgrade	Allows users to initiate upgrades to the latest version of Data Governance and Catalog.
Manage Usage Analytics	Allows users to enable and disable usage analytics.
Super Admin	Allows users access to unique administrator capabilities beyond the Governance Administrator role.

Feature privileges for Data Governance and Catalog

The following table explains the feature privileges that are available for the Data Governance and Catalog service in Administrator:

Feature	Description
Access Data Governance and Catalog application	Enable this feature to grant access to Data Governance and Catalog. If disabled, you cannot access Data Governance and Catalog to perform any governance tasks.
Export	Allows users the ability to export assets from Data Governance and Catalog.
Export Usage Metrics	This privilege is not in use.
Force Delete	Allows users the following privileges: <ul style="list-style-type: none"> - Delete assets with incoming relationships - Delete assets with all the child assets in the hierarchy through bulk import

Feature	Description
Import	<p>Allows users the ability to download predefined templates and import business assets into Data Governance and Catalog. If you enable this privilege, you must additionally grant users the following asset privileges to import assets:</p> <ul style="list-style-type: none"> - Business assets. Create and update privilege - Technical assets. Update privilege
Manage Tickets	<p>Allows users the following privileges:</p> <ul style="list-style-type: none"> - Resolve or cancel tickets without being a stakeholder of the asset. - Receive notifications for manual tickets without being a stakeholder of the asset.
Manage Workflow Tasks	<p>Allows users the following privileges:</p> <ul style="list-style-type: none"> - View all the tasks on the Tasks Inbox page in Data Governance and Catalog. - Manage tasks in Data Governance and Catalog. - Assign and reassign tasks in Data Governance and Catalog,
Participate in Change Approvals	<p>Allows users the following privileges:</p> <ul style="list-style-type: none"> - Participate in workflow approvals in Data Governance and Catalog. <p>The role for which you grant this privilege appears in the Role in Metadata Command Center when a user creates or modifies a workflow task.</p> <ul style="list-style-type: none"> - Add stakeholders to assets in Data Governance and Catalog. - Configure workflows in Metadata Command Center.
Preview Data	<p>Allows user to view the latest preview of failed rows for data quality rule occurrences in Data Governance and Catalog.</p>
View Reference Data	<p>Allows users to view reference data on the Reference Data tab for business terms, metrics, manual data elements, and data elements.</p>
View Restricted Metrics	<p>Allow users to view restricted metric data on usage analytics dashboards.</p>
View Usage Metrics	<p>Allows users to view metric data, to edit widgets on usage analytics dashboards, and to clone and share usage analytics dashboards.</p>

Predefined user roles

As an organization administrator, you can assign predefined user roles to users and user groups in Administrator.

Predefined user roles are system-defined roles that define certain privileges to the services that your organization uses. Some asset and feature privileges are enabled by default for predefined user roles. You cannot modify, rename, or delete predefined roles.

Data Governance and Catalog provides the following predefined roles:

- [“Data Access Owner role” on page 23](#)
- [“Governance Administrator role” on page 24](#)
- [“Governance Owner role” on page 27](#)
- [“Governance User role” on page 28](#)

To extend the user role privileges provided in Administrator, you can assign the predefined access policies to user roles and stakeholder roles in Metadata Command Center. See [“Predefined access policies” on page 29](#).

Data Access Owner role

A user with the Data Access Owner role has the feature privileges assigned in Administrator to perform certain tasks in Data Governance and Catalog. In Metadata Command Center, a user with this role also automatically receives the default privileges to perform tasks on data access policies in Data Governance and Catalog.

Data Governance and Catalog

The following table lists the feature privileges that are enabled or disabled by default in Data Governance and Catalog for the Data Access Owner role:

Features	Status
Access Data Governance and Catalog Application	Enabled
Export	Disabled
Force Delete	Disabled
Import	Disabled
Manage Tickets	Disabled
Manage Workflow Tasks	Disabled
Participate in Change Approvals	Disabled
Preview Data	Disabled
View Reference Data	Enabled

Governance Administrator role

A user with the Governance Administrator role has asset and feature privileges assigned in Administrator that assist in working with features and assets in Metadata Command Center, Data Governance and Catalog and Data Marketplace. The Governance Administrator role also includes features and privileges that you need to configure and run Application Integration processes and Human Tasks services using custom workflows.

Metadata Command Center

The following table lists all the asset privileges that are enabled or disabled by default for the Governance Administrator role in Metadata Command Center:

Assets	Privileges enabled	Privileges disabled
Catalog Source Configurations	Create, read, update, delete, run, set permission	None
Custom Catalog Source Type	Create, read, update, delete	Run, set permission
Custom Models	Create, read, update, delete	Run, set permission

The following table lists the feature privileges that are enabled or disabled by default for the Governance Administrator role in Metadata Command Center:

Features	Status
Access Metadata Command Center Application	Enabled
Manage Access Control	Enabled
Manage Asset Groups	Enabled
Manage Asset Page Customization	Enabled
Manage Custom Attributes	Enabled
Manage Data Classifications	Enabled
Manage IDMC Metadata Settings	Enabled
Manage Lineage Settings	Enabled
Manage Lookup Table	Enabled
Manage System Settings	Enabled
Manage Upgrade	Disabled
Manage Workflows	Enabled
Monitor Jobs	Enabled
Super Admin	Disabled
View Access Control	Enabled

Features	Status
View Asset Groups	Enabled
View Asset Page Customization	Enabled
View Custom Attributes	Enabled
View Data Access Audit	Enabled Note: This privilege is for a future release.
View Data Access Management	Enabled
View Data Classifications	Enabled
View IDMC Metadata Settings	Enabled
View Lineage Settings	Enabled
View Lookup Table	Enabled
View System Settings	Enabled
View Workflows	Enabled
Workflow Designer	Enabled

Data Governance and Catalog

The following table lists the feature privileges that are enabled or disabled by default for the Governance Administrator role in Data Governance and Catalog:

Features	Status
Access Data Governance and Catalog Application	Enabled
Export	Enabled
Force Delete	Disabled
Import	Enabled
Manage Tickets	Disabled
Manage Workflow Tasks	Enabled
Participate in Change Approvals	Enabled
Preview Data	Enabled
View Reference Data	Enabled

Data Marketplace

The following table lists the feature privileges that are enabled or disabled by default for the Governance Administrator role in Data Marketplace:

Features	Status
Access Data Marketplace	Enabled
Approve or Reject Orders	Disabled
Cancel Your Orders And Data Collection Requests	Enabled
Complete or Reject Data Collection Requests	Disabled
Configure And Manage Data Marketplace	Disabled
Fulfill Or Reject Orders	Disabled
View Set up page	Disabled
Withdraw Consumer Accesses	Disabled

Application Integration

The following table lists the asset privileges that are enabled or disabled by default for the Governance Administrator role in Application Integration:

Assets	Privileges enabled	Privileges disabled
Application Integration Assets	Create, read, update, delete, run, set permission	None

The following table lists the feature privileges that are enabled or disabled by default for the Governance Administrator role in Application Integration:

Features	Status
Administration	Enabled
Console Administration	Enabled
Data Viewer	Enabled
Development	Enabled
Monitoring	Enabled
Publish Application Integration Assets	Enabled

Features	Status
View Application Integration Console	Enabled
View Application Integration Designer	Enabled

Human Tasks

The following table lists the asset privileges that are enabled or disabled by default for the Governance Administrator role in Human Tasks:

Assets	Privileges enabled	Privileges disabled
Human Task Assets	Create, read, update, delete, run, set permission	None

The following table lists the feature privileges that are enabled or disabled by default for the Governance Administrator role in Human Tasks:

Features	Status
Development	Enabled
View Human Task Application	Enabled
View Tasks	Enabled

Governance Owner role

A user with the Governance Owner role has the privileges assigned in Administrator to perform certain tasks and manage assets in Data Governance and Catalog and Data Marketplace.

Data Governance and Catalog

The following table lists the feature privileges that are enabled or disabled by default in Data Governance and Catalog for the Governance Owner role:

Features	Status
Access Data Governance and Catalog Application	Enabled
Export	Enabled
Force Delete	Disabled
Import	Enabled
Manage Tickets	Disabled
Manage Workflow Tasks	Disabled

Features	Status
Participate in Change Approvals	Enabled
Preview Data	Enabled
View Reference Data	Enabled

Data Marketplace

The following table lists the feature privileges that are enabled or disabled by default in Data Marketplace for the Governance Owner role:

Features	Status
Access Data Marketplace	Enabled
Approve or Reject Orders	Disabled
Cancel Your Orders And Data Collection Requests	Enabled
Complete or Reject Data Collection Requests	Disabled
Configure And Manage Data Marketplace	Disabled
Fulfill Or Reject Orders	Disabled
View Set up page	Disabled
Withdraw Consumer Accesses	Disabled

Governance User role

A user with the Governance User role is assigned specific privileges in Administrator that assist in working with features and assets in Data Governance and Catalog and Data Marketplace.

Data Governance and Catalog

The following table lists the feature privileges that are enabled by default for the Governance User role in Data Governance and Catalog:

Features	Status
Access Data Governance and Catalog Application	Enabled
Export	Enabled
Force Delete	Disabled
Import	Disabled
Manage Tickets	Disabled

Features	Status
Manage Workflow Tasks	Disabled
Participate in Change Approvals	Disabled
Preview Data	Disabled
View Reference Data	Enabled

Data Marketplace

The following table lists the feature privileges that are enabled by default for the Governance User role in Data Marketplace:

Features	Status
Access Data Marketplace	Enabled
Approve or Reject Orders	Disabled
Cancel Your Orders And Data Collection Requests	Enabled
Complete or Reject Data Collection Requests	Disabled
Configure And Manage Data Marketplace	Disabled
Fulfill Or Reject Orders	Disabled
View Set up page	Disabled
Withdraw Consumer Accesses	Disabled

Predefined access policies

Predefined access policies provide an extension of the access privileges that the organization administrator provides through user roles in Administrator. To perform cataloging and governance tasks, the administrator must assign the predefined access policies to user roles and stakeholder roles in Metadata Command Center.

The predefined access policies have a set of predefined rules that grants different levels of access to users based on the user roles or stakeholder roles assigned to the users. You cannot modify the predefined access policies but you can disable and clone them to create custom access policies that are specific to your organization.

To view all the predefined access policies, go to the **Access Policies** tab on the **Access Control** page in Metadata Command Center, and apply the filter on **Category**.

The following table lists the predefined access policies that are enabled and disabled by default:

Access Policy	Description	Type	Status
Data Access Owner	Defines permissions on data access controls for a user with the Data Access Owner user role.	User Role Policy	Enabled
Data Access Stakeholder	Defines permissions on data access controls for a stakeholder with the Data Access Owner user role.	Stakeholder Role Policy	Enabled
Data Marketplace Data Collection Owner Stakeholder	Defines the permissions that a user will have as a stakeholder with Data Marketplace Data Collection Owner stakeholder role on a data collection. When in effect, the policy allows a user to manage a data collection and the assets within it.	Stakeholder Role Policy	Enabled
Data Marketplace Data Collection Technical Owner Stakeholder	Defines the permissions that a user will have as a stakeholder with Data Marketplace Data Collection Technical Owner stakeholder role on a data collection. When in effect, the policy allows a user to manage the assets and deliveries of a data collection.	Stakeholder Role Policy	Enabled
Non-Stakeholder Policy for Marketplace Assets	Grants read permission on Data Marketplace assets to users who are not stakeholders of Data Marketplace assets.	Stakeholder Role Policy	Enabled
Data Marketplace Delivery Template Owner Stakeholder	Defines the permissions that a user will have as a stakeholder with Data Marketplace Data Collection Delivery Template Owner stakeholder role on a delivery template. When in effect, the policy allows a user to manage a delivery template.	Stakeholder Role Policy	Enabled

Access Policy	Description	Type	Status
Data Marketplace Category Owner Stakeholder	Defines the permissions that a user will have as a stakeholder with Data Marketplace Category Owner stakeholder role on a category. When in effect, the policy allows a user to manage a category and the assets within it.	Stakeholder Role Policy	Enabled
Governance Owner Stakeholder	Defines the permissions that a user will have as a stakeholder with Governance Owner stakeholder role on business and technical asset types. When in effect, the policy allows a user to manage business and technical assets.	Stakeholder Role Policy	Enabled
Governance Administrator Stakeholder	Defines the permissions that a user will have as a stakeholder with Governance Administrator stakeholder role on business and technical asset types. When in effect, the policy allows a user to manage business and technical assets.	Stakeholder Role Policy	Enabled
Non Stakeholder policy for Business and Technical assets	Grants read permission to non-stakeholders on business and technical asset types.	Stakeholder Role Policy	Enabled
Data Marketplace Delivery Template Owner	Grants permissions to the Data Marketplace Delivery Template Owner user role to manage delivery templates in Data Marketplace. Also grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled

Access Policy	Description	Type	Status
Data Marketplace User	Grants permission to the Data Marketplace User role to view and consume data collections in Data Marketplace. In addition, grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled
Data Marketplace Technical Administrator	Grants permissions to the Data Marketplace Technical Administrator user role to perform technical administrative tasks such as managing delivery options, specifying the general terms of use and customizing the appearance of Data Marketplace. In addition, grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled
Data Marketplace Category Owner	Grants permissions to the Data Marketplace Category Owner user role to manage categories and the data within them. In addition, grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled
Admin	Grants read permissions to the Admin user role on business and technical asset types and limited permissions on marketplace asset types.	User Role Policy	Enabled

Access Policy	Description	Type	Status
Data Marketplace Administrator	Grants all permission to the Data Marketplace Administrator user role on all Data Marketplace assets. In addition, grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled
Governance Administrator	Grants all permissions to the Governance Administrator user role on business and technical asset types and limited permission on marketplace asset types. Provides the ability to manage catalog source configuration in Metadata Command Center.	User Role Policy	Enabled
Governance User	Grants read permission to the Governance User role on business and technical asset types and limited permissions on marketplace asset types.	User Role Policy	Enabled
Governance Owner	Grants all permissions to the Governance Owner user role on business and technical asset types and limited permissions on marketplace asset types.	User Role Policy	Enabled
Data Marketplace Data Collection Technical Owner	Grants permission to the Data Marketplace Data Collection Technical Owner user role to manage deliveries of data collections. Also grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled

Access Policy	Description	Type	Status
Data Marketplace Data Collection Owner	Grants permissions to the Data Marketplace Data Collection Owner user role to manage data collections and the data within them. Also grants read permission on business and technical assets in Data Governance and Catalog.	User Role Policy	Enabled
Super Admin	Grants the manage access permission to the Governance Administrator user role to manage stakeholders on business and technical asset types.	User Role Policy	Disabled
No Asset Group	Grants all permissions to users on assets that do not belong to asset groups. Other user role or stakeholder role policies can restrict permissions granted by this policy.	User Group Policy	Enabled

Use cases

The following use cases illustrate how you can use metadata access control to effectively manage access to the assets in your organization:

- [“Use case: Control access to unpublished glossary changes” on page 34](#)
- [“Use Case: Cross-unit glossary collaboration ” on page 35](#)

Use case: Control access to unpublished glossary changes

HypoStores is a popular online shopping retail company that offers a wide range of products, from clothing to electronics. *HypoStores* uses Data Governance and Catalog to manage its data assets effectively.

Problem statement

The *HypoStores* business is growing, and the website team needs to keep the business glossary updated with product categories, pricing models, and promotional terms. The glossary stewards collaborate with stakeholders to update and finalize the glossary definitions. In the meantime, they want to make sure that only the glossary stewards have access to the unpublished changes. Otherwise, confidential information might be leaked.

Solution

HypoStores can use attribute groups in access policies to explicitly grant glossary stewards in their organization access to assets that contain unpublished or draft changes. Users other than glossary stewards

With access control in Data Governance and Catalog, the organization administrator can perform a few simple steps:

1. In Administrator, define a user role called *Glossary Steward* and assign this role to users who manage glossary assets in the organization.
2. In Metadata Command Center, create and publish a user role-based access policy for the *Glossary Steward* role. The access policy can contain the following rules:
 - Grant data stewards permissions to create, read, update, and manage access on business asset types. This grants data stewards permissions to all lifecycle statuses of business assets.
 - Grant read permission on the **Unpublished Changes** attribute group for all business asset types.

After the access policy is published in Metadata Command Center, users with the *Glossary Steward* role can access the unpublished changes or the draft version of the business assets in Data Governance and Catalog.

Use Case: Cross-unit glossary collaboration

Acme Inc. is a finance company that provides loans, credit and other financial services. *Acme Inc.* uses Data Governance and Catalog for compliance, data quality, and collaboration.

Problem Statement

The company has three separate business units that want to work together on a common enterprise glossary. While they need to collaborate on the common glossary, each unit has its own assets that must stay private and separate from the others for security, legal, and operational reasons.

Solution

Acme Inc. can use asset groups to segregate assets based on the business units that use them, ensuring that only the employees of a particular business unit can interact with the business unit's assets.

With metadata access control in Data Governance and Catalog, *Acme Inc.* can segregate assets using asset groups while ensuring collaboration among employees in a few simple steps:

1. In Metadata Command Center, create an asset group called *Acme Inc.*
2. Under the *Acme Inc* asset group, create three child asset groups that correspond to the business units. For example, create: *Acme France*, *Acme UK*, and *Acme India*.
3. Assign each child asset group to the corresponding assets from each business unit and assign the parent asset group to common glossary assets that all users can collaborate on.
4. Use these asset groups in access policies to grant different levels of user access for each asset group. Each asset group can have the following rules:
 - Grant read permission to data stewards to view all technical and business assets that belong to the asset group.
 - Grant read permission to business users to view all business assets that belong to the asset group.
 - Grant read permissions to all users to view glossary assets that are assigned to the *Acme Inc* asset group.

After the access policies are published and the assets are assigned to asset groups, only users that are part of each asset group will have permission to interact with the assets in those groups. All users can collaborate on the glossary assets that belong to the parent asset group.

CHAPTER 4

Notifications

You receive notifications in Informatica Intelligent Cloud Services for certain events, including job status updates, license expiration, and workflow progress. You can manage how you receive notifications.

The Notifications icon on the toolbar displays the number of unread notifications. You can click the icon to view the latest unread notifications in the notifications tray. In some services, you can filter the tray to display only notifications from the current service.

You can also view and manage notifications on the **Notifications** page. To access the **Notifications** page, select **View All Unread** from the Actions menu in the notifications tray. On the **Notifications** page, you can filter notifications by service, category, subcategory, status, and date received.

CHAPTER 5

Editing your user profile

Your user profile contains the details of your Informatica Intelligent Cloud Services user account.

You can update the following information in your profile:

- First and last name
- Job title
- Email address
- Phone number
- Time zone (used in the job execution time stamps on the **All Jobs**, **Running Jobs**, **My Jobs**, **Import/Export Logs**, and **My Import/Export Logs** pages)
- Password
- Security question and answer

Note: If you use SAML to sign on to Informatica Intelligent Cloud Services and your organization administrator has enabled SAML group and role mapping on the **SAML Setup** page in Administrator, you can only update the time zone. The other attributes are updated directly from your enterprise directory each time you log into Informatica Intelligent Cloud Services.

1. Click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window and then select **Profile**.
2. On the **Profile** page, add or edit personal information such as your name, job title, phone number, and time zone.
3. To update your email address, click **Update Email**.
Informatica Intelligent Cloud Services sends a verification email to your new email address. The email contains a link that is valid for 24 hours. When you click the link in the email, the new address is verified, and it appears in your profile. If the link expires, you can resend the verification email.
4. Optionally, change your password or security question.
5. Click **Save**.

CHAPTER 6

Editing your user settings

In your user settings, you can configure how you receive email notifications and you can set source code credentials.

To access user settings, click the **User** icon on the toolbar and then select **Settings**. The user settings page includes the following sections:

Notification Settings

The **Notification Settings** section lists categories of events that trigger notifications, such as changes in an asset's stakeholders and new comments on an asset. By default, you receive an email notification each time an event occurs. You can disable all email notifications, disable event notifications by category and subcategory, and for some categories you can choose to receive an email summarizing events at an interval that you specify.

For more information, see *User Administration* in the Administrator help.

Source Code Control Credentials

In the **Source Code Control Credentials** section, you can configure repository credentials that allow you to work with source controlled objects.

For more information, see *Organization Administration* in the Administrator help.

CHAPTER 7

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 Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and maplets:

<https://marketplace.informatica.com/>

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.

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.

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>.

INDEX

C

Cloud Application Integration community
URL [39](#)
Cloud Developer community
URL [39](#)

D

Data Integration community
URL [39](#)

E

email addresses
for notification [37](#)

F

features
assign privileges [20](#)

I

Informatica Global Customer Support
contact information [41](#)
Informatica Intelligent Cloud Services
web site [39](#)

M

maintenance outages [40](#)

P

passwords
changing [37](#)
privileges
for features [20](#)
profiles
editing [37](#)

S

security questions
editing [37](#)
status
Informatica Intelligent Cloud Services [40](#)
system status [40](#)

T

time zones
changing user profile [37](#)
trust site
description [40](#)

U

upgrade notifications [40](#)
user profiles
editing [37](#)

W

web site [39](#)