Informatica® Intelligent Cloud Services
August 2024

Organization Administration

Table of Contents

Preface

Use *Organization Administration* to learn how to set up and maintain your Informatica Intelligent Cloud Services℠ organization and sub-organizations. Learn how to manage licenses and monitor license usage, configure source control, configure object permissions, create schedules, manage bundles, monitor events, and troubleshoot security issues.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

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 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 mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.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 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 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.

CHAPTER 1

Introducing Administrator

Administrator provides organization management capabilities across Informatica Intelligent Cloud Services.

Use Administrator to manage the following aspects of your organization:

Organization and sub-organizations

Configure settings for your organization and sub-organizations such as password requirements, trusted IP addresses, connection properties storage, time zone and email notification settings for Data Integration tasks, CLAIRE™ recommendation preferences, and Enterprise Data Catalog settings. Create and manage sub-organizations.

For information about organizations and sub-organizations, see Chapter 2, "Organizations" on page 11.

Licenses

View your organization's licenses and manage sub-organization licenses.

For information about licenses, see Chapter 10, "Licenses" on page 84.

Metering

View metering information such as job limits, usage, and Informatica processing unit (IPU) balances.

For information about metering, see Chapter 3, "Metering" on page 29.

Ecosystem and SAML single sign-on

Configure single-sign on settings for Microsoft Azure. Enable single sign-on capability for a SAML third-party identity provider.

For information about Microsoft Azure single sign-on settings and information about enabling and configuring SAML single sign-on, see *User Administration*.

General and security settings

Enable source control for projects, folders, and assets. Configure upgrade error handling and upgrade restart schedules for some Secure Agent services. Configure custom branding settings for a parent organization to apply to sub-organizations. Enable and disable the use of customer managed encryption keys for your organization. Configure your organization to retrieve connection credentials from an external secrets manager.

For more information about general and security settings, see Chapter 4, " General and security settings" on page 46.

Users, user groups, and user roles

Create and configure individual user accounts to allow access to your organization. Create groups of users that can perform the same tasks. Create and configure roles to define the privileges for your users and user groups.

For information about users, user groups, and user roles, see *User Administration*.

Permissions

Configure the access rights that users and user groups have for objects such as Secure Agents, Secure Agent groups, connections, and schedules.

For information about permissions and configuring permissions, see .

Runtime environments

Download and install Secure Agents. Create and configure Secure Agent groups.

For information about Secure Agents, Secure Agent groups, and downloading and installing a Secure Agent, see *Runtime Environments*.

Serverless runtime environments

Use a runtime environment that Data Integration manages to reduce maintenance overhead.

Note: To use a serverless runtime environment, you must have a private cloud on the AWS cloud platform.

For information about serverless runtime environments, see *Runtime Environments*.

Secure Agent services

Configure settings for the microservices that the Secure Agent uses for data processing such as the Elastic Server, CIH Processor, Data Integration Server, EDC Search Agent, and Process Server.

For information about Secure Agent services and their configuration, see *Secure Agent Services*.

Advanced clusters

Manage the ephemeral clusters that your organization can use to process data integration jobs.

For information about advanced clusters, see *Advanced Clusters*.

Schedules

Create schedules to run tasks or taskflows at specified times or at regular intervals. Define a blackout period in which no scheduled tasks or jobs in your organization can run.

For information about schedules and organization blackout periods, see .

Add-on bundles

Install, copy, upgrade, and uninstall sets of related mappings, mapping tasks, mapplets, and Visio templates that Data Integration users can use in data integration projects.

For information about managing add-on bundles, see .

Data services repository

Download out-of-the-box data services that process industry-standard messages and use them to create custom data services to process custom messages.

For information about the data services repository, see *Data Services Repository*.

Event monitoring

Monitor events for the assets, licenses, users, and Secure Agents in your organization through the asset and security logs.

For information about asset and security logs, see .

File transfer

Configure your organization's file server to securely send and receive files from a business partner's remote server. Configure a connection, and then send the files to your partners using the Informatica Intelligent Cloud Services REST API.

For information about file servers and file transfer, see *File Transfer*.

Note: Some of the functionality that's mentioned in the help might not be available due to your organization's Informatica Intelligent Cloud Services license agreement.

CHAPTER 2

Organizations

An organization is a secure area within the Informatica Intelligent Cloud Services repository that stores your licenses, user accounts, data integration assets such as mappings and tasks, and information about jobs and security. You might have access to one or more organizations.

By default, the organization that you create when you start your free trial is a production organization.

Based on your licenses, you might also have access to the following organizations:

Sub-organizations

If you have the appropriate license, administrators in the production organization can create one or more sub-organizations. Sub-organizations are child organizations of the production organization. They are automatically linked to the parent organization.

Each sub-organization has its own set of assets, connections, runtime environments, and users. However, the parent organization can share runtime environments and add-on connectors with a sub-organization. Administrators in the parent organization can switch to a sub-organization unless the sub-organization forbids this.

You cannot create any other organizations from a sub-organization.

Additional production organizations and sandbox organizations

If you have the appropriate license, administrators in the production organization can create additional production organizations and sandbox organizations.

These organizations are automatically linked to the production organization for IPU usage, but they are otherwise completely independent organizations. They do not share assets, connections, runtime environments, or users with the production organization. Administrators in the production organization cannot switch into an additional production organization or a sandbox organization.

If the production organization has the license to create sub-organizations, administrators in the additional production organizations and sandbox organizations can create sub-organizations for their organizations.

The administrator of an organization maintains the organization and its sub-organizations. Log in to Informatica Intelligent Cloud Services as an administrator to set up your organization, create and manage schedules, and monitor activities related to assets and security.

Setting up an organization

When you set up an organization, you configure the organization properties, sub-organizations, additional organizations, licenses, runtime environments, and user accounts.

To set up your company's organization, perform the following steps:

1. Configure organization properties such as the organization name and address, authentication information, and notification email addresses.
2. Verify that your organization has the appropriate licenses.
3. Optionally, create one or more sub-organizations and configure licenses for the sub-organizations.
4. Optionally, create additional production organizations and sandbox organizations.
5. Configure runtime environments and Secure Agents.
6. Set up users, user groups, and roles.

You might also need to download and install non-native connectors for your organization. For example, if users in your organization create tasks that read data from Teradata tables, you need to download and install the add-on connector for Teradata. For more information about downloading and installing add-on connectors, see *Connections*.

Organization settings

Configure settings for your organization or sub-organizations on the **Organization** page. To access the **Organization** page, in Administrator, select **Organization**.

The following image shows the **Organization Settings** page:

You can configure the following settings:

- General properties such as organization name, description, number of employees, and address information.
- Authentication information and connection properties storage.
- Connection credentials and where they are stored.
- Fingerprint authentication enforcement.
- Data Integration service properties such as the time zone and default addresses for email notifications.
- CLAIRE™ recommendation preferences. If enabled, CLAIRE provides design time recommendations based on collected metadata.
- Enterprise Data Catalog integration properties such as the URL of the Enterprise Data Catalog Service, runtime environment that reads data from Enterprise Data Catalog, and Enterprise Data Catalog user name and password.

Organization general properties

You can configure general properties for your organization and sub-organizations. General properties include information such as the organization name, ID, description, address, and number of employees. History information for the organization is also displayed in the general properties.

The general properties include the following information:

Overview information

The following table describes the overview properties:

Property	Description
Name	Name of the organization. If you change the organization name, the new name appears on the **Organization** menu after you log out and log back in.
ID	ID assigned to your organization when it was created. You cannot change an organization ID.
Parent Organization ID	When you view a sub-organization, this property displays the ID assigned to the parent organization. You cannot change an organization ID.
Organization Status	When you view a sub-organization, this property indicates whether the sub-organization is enabled or disabled.
Environment Type	Environment type for the organization, either Production, QA, Development, or Sandbox. Informatica Intelligent Cloud Services sets the environment type in the following ways based on how you create the organization: - When you create your organization by starting your free trial, the environment type is Production. - When you create an additional production organization, the environment type is Production. - When you create a sandbox organization, the environment type is Sandbox. There is no difference in functionality among the environment types.

Property	Description
MDM Environment Type	MDM environment type for an organization to accurately govern and monitor the usage of the organization. The MDM environment type can be production, additional production, sandbox, partial sandbox, trial, partner, or provisional. Verify the MDM environment type whenever it changes. To update the MDM environment type, contact Informatica Global Customer Support.
Description	Optional description of the organization.
Number of Employees	Number of employees in the organization.
Deny parent organization access to this sub-organization	When this option is checked, users in the parent organization cannot switch from the parent organization to the sub-organization. Users in the parent organization with the appropriate privileges can make only the following changes to the sub-organization: - Enable and disable the sub-organization - Update the sub-organization licenses - Edit the sub-organization properties such as the organization description and CLAIRE recommendation preferences This option is displayed on the **Organization** page for sub-organizations. This option can be changed when an administrator in the sub-organization logs in to the sub-organization. This option is read-only when a parent organization administrator views the organization properties for the sub-organization. This option is unchecked by default.

Address information

Use the address properties to specify the street address, zip code, state, and country of the organization.

History information

The organization history information displays the date and time that the organization was created, the user who created the organization, the date and time that the organization was last updated, and the user who last updated the organization. Informatica Intelligent Cloud Services updates the history information when you make changes to the organization.

Authentication properties

You can configure authentication properties for your organization and sub-organizations. Authentication properties control password restrictions and IP address filtering.

Password restrictions are enforced when users create or change their passwords. If you change the password expiration date from "never" to a number of days, then users with passwords that are older than the number of days will be required to change their passwords the next time that they log in to Informatica Intelligent Cloud Services.

The following table describes the authentication properties:

Property	Description
Minimum Password Length	Minimum password length required for a valid password. Must be a number between 4 and 12 characters.
Minimum Character Mix	Minimum number of character types required for a valid password. Passwords can contain a mix of the following character sets: - Lowercase alphabetic characters - Uppercase alphabetic characters - Numeric characters - Special characters For example, if you set **Minimum Character Mix** to 1, then passwords must contain at least one of the character sets. If you set **Minimum Character Mix** to 2, then passwords must contain at least two of the character sets.
Password Reuse	Controls whether users can reuse passwords.
Password Expires	Determines how often users must reset their passwords.
Session Idle Timeout	Amount of time before a user's session times out due to inactivity. Informatica Intelligent Cloud Services displays a warning message to the user 60 seconds before the user is logged out. Default is 30 minutes.
Use Trusted IP Ranges	Enables IP address filtering. IP address filtering uses trusted IP address ranges in addition to account passwords to prevent unauthorized users from accessing your organization. When you enable IP address filtering, a user with a valid login must also have an IP address within the range of trusted IP addresses, or the user cannot log in to your organization. When you enable this option, you must also enter one or more trusted IP address ranges.
Allowed Trusted IP Ranges	The trusted ranges of IP addresses from which users can log in to access the organization. Informatica Intelligent Cloud Services supports IP address formats in IP version 4 (IPv4) and version 6 (IPv6). Fields for the trusted IP address range appear when you enable IP address filtering. To enter additional address ranges, click **+**. **Note:** If you enter an invalid IP address range, users cannot access your organization. Contact your network administrator for valid IP address ranges.

Connection properties storage

You can configure where to store the connection properties for your organization and sub-organizations. To specify where to store the connection properties, configure the **Connection Credentials** on the **Organization** page.

You can store connection properties in either of the following locations:

Informatica Cloud

When you store connection properties on the cloud, the connection properties are stored in the Informatica Intelligent Cloud Services repository and are always available. The connections are encrypted by the Informatica Intelligent Cloud Services key management service.

Informatica Intelligent Cloud Services backs up connection properties regularly as part of standard backup procedures.

Local Secure Agent

You might store connection properties with a local Secure Agent if you need the connection properties to reside within your firewall. When you enable this option, the properties for all connections that are listed on the **Connections** page are stored with the local agent.

Note: In organizations subject to FedRAMP, you can't store connection properties with a local Secure Agent.

If you choose this option, you can store connection properties with one Secure Agent. Connection properties are stored in the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data
```

When you store properties with a local Secure Agent, the Secure Agent must be running so that tasks can run and users can work with connections. Back up connection properties regularly to prevent loss of data. A best practice is to back up connection properties after you change the location or the encryption key for connection properties.

The connections are encrypted by the Informatica Intelligent Cloud Services key management service. Informatica Intelligent Cloud Services uses CBC (Cipher Block Chaining) mode 256 AES encryption to store the connections.

If you use an external secrets manager like AWS Secrets Manager or Azure Key Vault to store sensitive connection credentials, you need to set the connection credential storage to **Informatica Cloud**. When you do this, sensitive credentials are retrieved from the secrets manager and other connection properties are stored in the Informatica Intelligent Cloud Services repository. You can't use a secrets manager if you store connection credentials on a local Secure Agent. For more information about secrets manager configuration, see .

You can change where you want to store connection properties. When you do this, Informatica Intelligent Cloud Services moves the connection properties to the appropriate location. For example, your license expires, so you configure the organization to store connections on the cloud. Informatica Intelligent Cloud Services moves the connection properties from the local Secure Agent to Informatica Intelligent Cloud Services.

Fingerprint authentication properties

You can enforce a fingerprint authentication every time the Secure Agent starts. An authentication failure can trigger an email alert but allow normal operations, or it can disallow agent startup.

To set the authentication mode, configure the options in **Fingerprint Authentication** on the **Organization** page.

You can configure these levels of authentication enforcement:

No enforcement, no notifications

Disable fingerprint enforcement and don't specify an email address.

No authentication check is performed when the Secure Agent starts up. This is the default.

Report violations only

Disable fingerprint enforcement and specify an email address. The email format is checked, but the validity of the email address isn't verified. Be sure to allow emails from the address "admin@informaticacloud.com".

An authentication check is performed during Secure Agent start up. Any fingerprint mismatch triggers a notification to the email recipient, but the agent starts up normally.

Enforce authentication match

Set fingerprint enforcement to **On** and specify an email address. The email format is checked, but the validity of the email address isn't verified. Be sure to allow emails from the address "admin@informaticacloud.com".

Any fingerprint mismatch triggers a notification to the email recipient and the Secure Agent log in is prevented from starting up.

Note: An email address is required if enforcement is turned on.

A fingerprint is created the first time a Secure Agent starts up, using device attributes from the agent's host machine. The data is anonymized and hashed to produce a unique fingerprint. When switching from no enforcement to any other level of enforcement, the Secure Agent generates a fingerprint the first time it starts up.

If you reinstall the Secure Agent on the same machine, the fingerprint doesn't change.

The following table summarizes what happens when fingerprint enforcement prevents the Secure Agent from starting up:

Action	Message
Error is logged to agentcore.log	"Internal error. Agent <Secure Agent ID> fingerprint is not matching with the previous stored value for request <Request ID>."
Email notification is sent (if an email address was specified)	"There was a fingerprint mismatch while logging in agent with name <Secure Agent name> for Organization <Organization ID>. The agent was last active on <Date in UTC>."

Data Integration service properties

Data Integration service properties are used by Data Integration. Configure these properties to set the time zone and default email addresses for job notifications.

You can set the following Data Integration service properties:

Jobs properties

The following table describes the jobs properties:

Property	Description
Schedule Offset	A small amount of time that is added to schedule start times to help prevent server overload at standard schedule start times. An organization has a single schedule offset that is applied to all schedules. The schedule offset does not affect the start time of manually started tasks or taskflows. You cannot change the schedule offset.
	Even though it is not displayed in the schedule details, the schedule offset for your organization is added to the time range configured for all schedules. This ensures that scheduled tasks run as often as expected. For example, you configure a schedule to run every hour from 8:00 a.m. to 12:00 p.m., and the schedule offset for your organization is 15 seconds. Your schedule runs at 8:00:15, 9:00:15, 10:00:15, 11:00:15, and 12:00:15.
Time Zone	Time zone used to display job execution time stamps in email notifications.

Default email notifications properties

Configure the default email notifications properties to set the default email addresses to use for job failure, warning, and success messages. Enter one or more valid email addresses. Separate email addresses with a comma (,) or semicolon (;).

You can also set email notification properties at the task level. When you set email notifications in a task or taskflow, Informatica Intelligent Cloud Services sends email to the addresses in the task or taskflow instead of the addresses configured for the organization.

CLAIRE preferences

You can configure CLAIRE preferences for your organization to enable or disable CLAIRE GPT and CLAIRE recommendations for mappings.

You can configure the following settings:

CLAIRE generative AI services

Enable CLAIRE generative AI services to allow the users in your organization to use CLAIRE GPT to discover, analyze, and explore data through natural language prompts.

By default, CLAIRE generative AI services are disabled. You can enable or disable them for your organization at any time.

For more information about CLAIRE GPT, see the CLAIRE GPT help.

CLAIRE recommendations

Enable CLAIRE recommendations to allow in-product recommendations for mapping design based on analysis of metadata from your organization's assets and assets from other Informatica Intelligent Cloud Services organizations. The metadata collected and processed by the CLAIRE engine is anonymous.

By default, CLAIRE recommendations are enabled. When you disable CLAIRE recommendations, recommendations are disabled for all users within your organization. You can enable or disable recommendations for your organization at any time.

Enable and disable CLAIRE recommendations for sub-organizations from within the sub-organization.

When you enable CLAIRE recommendations, Data Integration users can disable recommendations for individual mappings in the mapping designer.

If your organization uses Advanced Integration, enabling CLAIRE recommendations enables the following features:

- CLAIRE-powered configurations, CLAIRE insights, and CLAIRE recommendations for advanced clusters
- CLAIRE-powered runtime strategies and CLAIRE Tuning for mapping tasks that are based on mappings in advanced mode
- CLAIRE recommendations for jobs that run mappings in advanced mode

Enterprise Data Catalog integration properties

If your organization uses data catalog discovery in Data Integration, you can configure Enterprise Data Catalog integration properties for your organization and sub-organizations. Configure Enterprise Data

Catalog integration properties so that users can use catalog assets in mappings, synchronization tasks, and file ingestion and replication tasks.

The Enterprise Data Catalog integration properties that you configure for the organization apply to the data catalog searches that all users in the organization perform. If your organization includes sub-organizations, you can configure different Enterprise Data Catalog integration properties for the parent organization and for each sub-organization.

The following table describes the Enterprise Data Catalog integration properties:

Property	Description
Catalog URL	URL of the Enterprise Data Catalog Service. Use the following format: `http://<fully qualified host name>:<port>` Do not append `/ldmcatalog` at the end of the URL.
Runtime environment	Name of the Secure Agent group that is used to read data from Enterprise Data Catalog. The agents in the group that you select must be able to communicate with Enterprise Data Catalog. Therefore, the Enterprise Data Catalog host must be in the same network as the agent machines or it must have the appropriate ports open for communication.
User name	Enterprise Data Catalog user account that the Secure Agent uses to access Enterprise Data Catalog. This user account must have privileges to view and search for objects in Enterprise Data Catalog and to perform functions using the Enterprise Data Catalog REST API.
Password	Password for the Enterprise Data Catalog user account.
Show the data catalog	Shows and hides the **Data Catalog** page in Data Integration.

Sub-organizations

If your organization has the appropriate license, you can create one or more sub-organizations within your organization. Create sub-organizations to represent different business environments within your company. For example, you might create sub-organizations to represent different clients or different departments in your organization.

You can create a sub-organization from the production organization, from an additional production organization, or from a sandbox organization.

When you create a sub-organization, the organization that you use to create a sub-organization becomes the parent organization. Each sub-organization can have only one parent, and it cannot contain another sub-organization.

Note: Sub-organizations must reside in the same POD (point of deployment) as the parent organization. In a CI/CD (continuous integration/continuous deployment) -oriented approach, all sub-organizations receive feature releases simultaneously, potentially resulting in issues and downtime during the same maintenance window.

Your organization's license controls the number of sub-organizations that you can create. To increase this number, contact Informatica Global Customer Support.

Creating sub-organizations provides the following advantages:

You can manage sub-organization licenses individually or you can automatically synchronize them with the parent organization licenses.

Each sub-organization inherits all feature, connector, and custom licenses from the parent organization except for the license to create sub-organizations and bundle licenses.

Based on your organization's licenses, you can manage sub-organization licenses in the either of the following ways:

- Manage the licenses for your sub-organizations individually. The administrators for the parent organization can disable, enable, and modify the expiration dates for the licenses for each sub-organization. Changes to one sub-organization do not affect other sub-organizations.
- Automatically synchronize sub-organizations licenses with the parent license.

You can manage users and assets separately.

Each sub-organization has its own set of users and assets.

Users whom you create in a sub-organization are unique to the sub-organization. They cannot log in to the parent organization or to other sub-organizations. Only administrators in the parent organization and users in the parent organization that have sub-organization access privileges can access the parent organization and all sub-organizations.

Assets such as mappings and tasks are also unique within an organization. Assets are not shared among sub-organizations or between the parent organization and any sub-organization. If you want to migrate an asset between organizations, export the asset from one organization and import it into a different organization.

You can share runtime environments.

Administrators in the parent organization can share Secure Agent groups with the sub-organizations. When you share Secure Agent groups, users in the sub-organizations can run jobs on the Secure Agents within the group.

Users of a parent organization or sub-organization can use only a Secure Agent that belongs to that organization or sub-organization. Users of a sub-organization cannot use a Secure Agent that belongs to the parent organization.

Note: Share a Secure Agent group when all agents in the group run only the Data Integration Server service. You cannot run other agent services' jobs on a shared Secure Agent group.

For more information about shared Secure Agent groups, see *Runtime Environments*.

You can share resources using bundles.

The Bundle Deployment feature lets you push bundles seamlessly from your parent organization to your sub-organizations. This ensures a smooth and efficient distribution of resources and features across your organizational structure.

For more information about bundles, see Chapter 7, "Bundle management" on page 77.

You can view aggregated IPU consumption metrics.

IPU (Informatica Processing Unit) consumption metrics for each sub-organization are aggregated and rolled up to their respective parent organization. This consolidation gives you a clear overview of how your resources are utilized. The consumption data is consolidated and rolled up within the organizational hierarchy until it reaches the main production organization.

You can switch between organizations without logging in to each one.

Users in the parent organization that have privileges to view sub-organizations can switch between organizations without logging out and logging back in to Informatica Intelligent Cloud Services.

Sub-organizations example

To observe CI/CD best practices, you want to create separate sub-organizations to represent different areas of your business, such as development, testing, and production. To achieve this, you first create separate parent organizations for development, testing, and production. Each parent organization should ideally be on a different POD, to safeguard against outages if a POD or organization becomes unavailable. Under each parent organization, you create sub-organizations that represent different clients or departments.

The following diagram shows the recommended hierarchy:
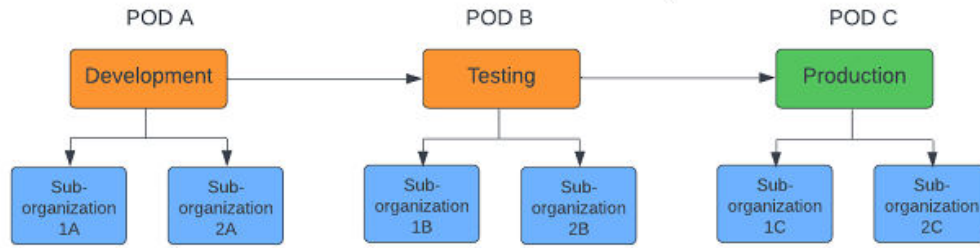
Using this hierarchy ensures a step-by-step flow of updates and improvements between environments, beginning with Development, moving to Testing, and concluding in Production. Isolating the environments in this way reduces the chances of unintended changes impacting other workflow stages.

For OEMs (original equipment manufacturers), the sub-organizations can represent individual clients. The structure allows the OEM to maintain control and oversee licensing, while allowing the individual clients to manage their development, testing, and production processes.

For corporations, the sub-organizations can represent different departmental divisions. This structure simplifies administrative monitoring and allows the parent organization to access assets, processes, and other resources set up by the departments.

Adding a sub-organization

To add a sub-organization, you can either create a new sub-organization or link existing organizations.

You can add a sub-organization in either of the following ways:

Create a sub-organization.

Log in to the organization that you want to be the parent organization and create a sub-organization. The new sub-organization is automatically linked to the parent organization.

Link existing organizations.

The organization that you link from becomes the parent organization and the organization that you link to becomes a sub-organization.

Creating a sub-organization

The administrator of a parent organization can create a sub-organization.

To create a sub-organization, you must be a native user with the Admin role or a native user with the "Suborg - create" and "Suborgs - view" privileges.

To create a sub-organization:

1. Log in to the organization that you want to be the parent organization.

2. Open Administrator and select **Organization**.

3. Open the **Sub-Organizations** tab and click **New Sub-Organization**.

4. Enter the properties for the sub-organization and click **Save**.

After you create a sub-organization, verify the licenses, and configure runtime environments, user accounts, and connections so that other people can use it.

Linking organizations

You can create a sub-organization by linking existing organizations. The organization that you link from becomes the parent organization and the organization that you link to becomes a sub-organization.

Before you link an organization, you need the organization ID for the organization that you want to link. You can find this information on the **Organization** page.

Note: If you link a sub-organization that has a license that the parent organization does not have, then the sub-organization loses the license.

You can link an organization if all of the following conditions apply:

- You have a user account with the organization.

- The organization is not the parent of another organization or a sub-organization of another organization.

- You are the administrator of the parent organization, and the parent organization has the license to create sub-organizations.

- The organization that you want to link as a sub-organization does not have the license to create sub-organizations.

You can later unlink the organizations.

To link organizations:

1. Log in to the organization that you want to be the parent organization.

2. Open Administrator and select **Organization**.

3. Open the **Sub-Organizations** tab and click **Link Sub-Organization**.

4. In the **Link Sub-Organization** dialog box, enter the following information:

   - The organization ID for the organization you want to link.

   - The user name and password of an administrator in the organization that you want to set up as a sub-organization.

5. Click **Link Sub-Organization** to link the organization.

   The organization displays on the **Sub-Organizations** page.

Removing a sub-organization

To remove a sub-organization, you can unlink organizations or delete the sub-organization.

You can remove a sub-organization in either of the following ways:

Unlink an existing sub-organization from its parent organization.

An unlinked sub-organization becomes a stand-alone organization. You can link it to a different parent organization or re-link it to the original parent organization. If you obtain the license to create sub-organizations for the unlinked organization, you can make it the parent organization for a different sub-organization.

Delete the sub-organization.

When you delete a sub-organization, you delete all of the assets and data associated with the sub-organization. If you have a usage-based license, after deletion, the sub-organization continues to consume IPUs in the current billing period. For more information, see "IPU usage for disabled and deleted sub-organizations" on page 35.

Unlinking a sub-organization

You can unlink a sub-organization from your parent organization. After you unlink an organization, update the unlinked organization with the required licenses unless you plan to link it to a different parent organization.

You can unlink a sub-organization if all of the following conditions apply:

- You have an administrator account with the sub-organization you want to unlink.
- You are an administrator of the parent organization, and the parent organization has the license to create sub-organizations.
- No asset in the sub-organization that you want to unlink uses a shared Secure Agent group as the runtime environment. If any asset in the sub-organization uses a shared Secure Agent group as the runtime environment, update the asset to use a different runtime environment before you unlink the sub-organization.

  Note: This condition does not apply to Application Ingestion and Replication and Database Ingestion and Replication because Application Ingestion and Replication and Database Ingestion and Replication do not support shared runtime environments.

To unlink a sub-organization:

1. Log in to the parent organization.
2. Open Administrator and select **Organization**.
3. Open the **Sub-Organizations** tab.
4. Expand the Actions menu for the sub-organization that you want to unlink and select **Unlink**.
5. In the **Unlink** dialog box, enter the user name and password of a user in the sub-organization with the Admin role.
6. Click **Unlink**.

   The sub-organization is no longer linked to the parent organization.

Deleting a sub-organization

You can delete a sub-organization. When you delete a sub-organization, you delete all of the associated data. If you have a usage-based license, the sub-organization's metering information is retained in the parent organization.

You can delete a sub-organization if you are the administrator of the parent organization.

1. Log in to the parent organization.
2. Open Administrator and select **Organization**.
3. Open the **Sub-Organizations** tab.
4. Expand the Actions menu for the sub-organization that you want to unlink and select **Delete**.

   Note: Contact Informatica Global Customer Support to complete the deletion process.

   If you have a usage-based license, the sub-organization continues to consume IPUs until the end of billing period in which the deletion was completed. For more information, see "IPU usage for disabled and deleted sub-organizations" on page 35.

Disabling or enabling a sub-organization

If you are the administrator for a parent organization, you can disable or enable a sub-organization.

When you create a sub-organization, the sub-organization is enabled by default. You might want to disable a sub-organization if you have a separate license agreement with the sub-organization and the license agreement expires. You can re-enable the sub-organization after you disable it.

You can disable or enable a sub-organization even if the sub-organization administrator blocks parent organization access to the sub-organization.

You can perform the following actions:

Disable a sub-organization

When you disable a sub-organization, the organization exists, but sub-organization users cannot log in to the sub-organization or access it through the REST API. Scheduled jobs in the sub-organization do not run.

If you have a usage-based license and you disable a sub-organization, it continues to consume IPUs. For more information, see "IPU usage for disabled and deleted sub-organizations" on page 35.

Enable a sub-organization

When you enable a sub-organization, sub-organization users can log in to the sub-organization and access assets and perform tasks based on their user roles. Users with the appropriate privileges can access the sub-organization through the REST API. Scheduled jobs resume according to their schedules.

Disable or enable a sub-organization on the **Sub-Organizations** tab of the **Organizations** page. In the **Actions** menu for the sub-organization, select **Disable** or **Enable**.

Switching to a different organization

If you are an administrator in a parent organization or a user in a parent organization that has privileges to view sub-organizations, you can switch among organizations. You do not have to log out and log back in to Informatica Intelligent Cloud Services.

Note: If you switch from a parent organization to a sub-organization, you can't perform the following operations in the sub-organization:

- Create or import data transfer tasks
- Create or import dynamic mapping tasks
- Create, validate, publish, and run taskflows
- Export and import taskflows

To switch to a different organization:

▶   From the **Organization** menu in the upper right corner, select the organization that you want to view.

Denying parent organization access to a sub-organization

If you are the administrator for a sub-organization, you can deny parent organization access to the sub-organization.

When you deny access to the sub-organization, users in the parent organization cannot switch from the parent organization to the sub-organization. Users in the parent organization with the appropriate privileges can make only the following changes to the sub-organization:

- Enable and disable the sub-organization

- Update the sub-organization licenses
- Edit the sub-organization properties such as the organization description and CLAIRE recommendation preferences

To deny parent organization access to the sub-organization, log in to the sub-organization as an administrator. On the **Organization** page, enable the **Deny parent organization access to this sub-organization** option.

Add-on connectors in sub-organizations

To use an add-on connector in a sub-organization, you must install the connector in the parent organization. You cannot install add-on connectors in a sub-organization.

Sub-organizations inherit all connector licenses from the parent organization. If a sub-organization should not use a specific connector, disable the connector license for the sub-organization. For more information about editing and disabling licenses for a sub-organization, see <u>"Editing sub-organization licenses" on page 86</u>.

Exporting and importing assets in sub-organizations

Export and import assets in a sub-organization in the following ways:

- Log in to the sub-organization and export or import assets from within the sub-organization.
- Parent organization administrators can log in to the parent organization, switch to the sub-organization, and import or export Data Integration assets.

    Note: This condition does not apply to taskflows and Application Integration assets.

Sub-organization capability and service support matrix

The capability of sub-organizations vary based on the Informatica service.

The following table summarizes the capabilities for each service:

Service	Capabilities				
	Licensing	Metering	Bundles	Shared Agent	Asset Access
Cloud Data Integration (CDI)	Organization has appropriate license to create sub-organizations.	Legacy Meter must be present in the parent organization.	Available	Supported	Not supported
Cloud Application Integration (CAI)	Organization has appropriate license to create sub-organizations.	Legacy Meter must be present in the parent organization.	Available	Not supported	Not supported
Cloud Data Governance & Catalog (CDGC)	Organization has appropriate license to create sub-organizations.	Legacy Meter must be present in the parent organization.	Not available	Not supported	Not supported

Master Data Management (MDM)	Organization has appropriate license to create sub-organizations.	Legacy Meter must be present in the parent organization.	Not available	Not supported	Supported
Cloud Data Quality (CDQ)	Organization has appropriate license to create sub-organizations.	Legacy Meter must be present in the parent organization.	Available	Supported	Not supported

Additional production organizations and sandbox organizations

If your organization has the appropriate license, you can create additional production organizations and sandbox organizations from the production organization. Create these organizations when you need separate organizations for different assets and users, but you want to manage all IPU usage from the production organization. Additional production organizations and sandbox organizations are automatically linked to the production organization.

You can create the following types of organizations:

Additional production organization

This is a separate production organization. It functions in the same way as the production organization, except that you cannot create additional production organizations or sandbox organizations from an additional production organization.

Sandbox organization

This is an organization that is typically used for asset development and testing. There is no difference in functionality between a sandbox organization and an additional production organization.

Additional production organizations and sandbox organizations are completely independent of the production organization and each other. They do not share assets, connections, runtime environments, or users. However, you can export and import assets between them.

The additional production organizations and sandbox organizations that you create inherit all licenses and editions from the production organization. If the production organization has the license to create sub-organizations, administrators in the additional production organizations and sandbox organizations can create sub-organizations for their organizations.

Additional production organizations and sandbox organizations appear on the **Additional Organizations** tab of the **Organization** page in the production organization. The **Additional Organizations** tab is shown in the following image:
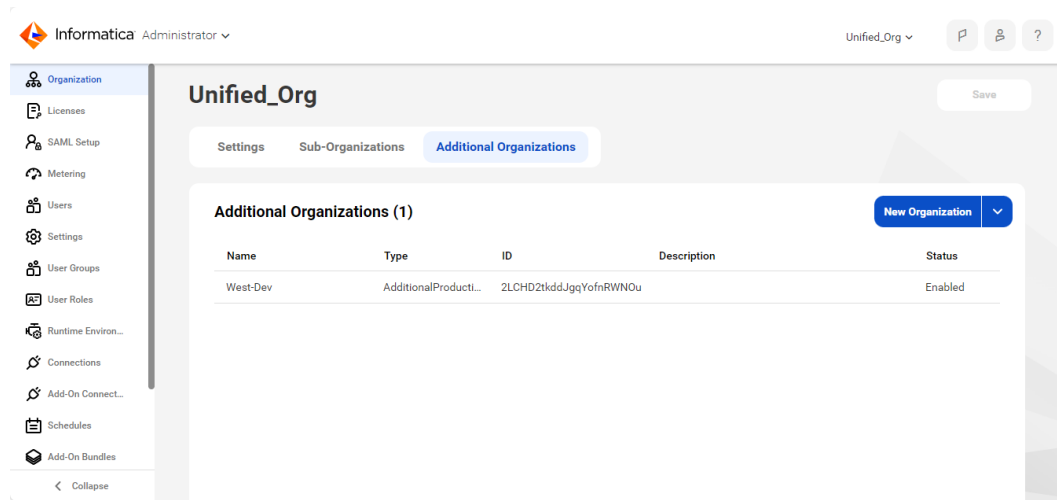
When you create an additional production organization or a sandbox organization, you must enter the organization name and a user name for the organization administrator. You can log in to the new organization using this user account and add other users and assets.

After you create an additional production organization or a sandbox organization, you cannot disable or delete it, and you cannot unlink it from the production organization. If you need to do this, contact Informatica Global Customer Support.

Creating an additional organization

Create an additional production organization or a sandbox organization on the **Additional Organizations** tab of the **Organization** page.

Note: Creating additional production organizations or sandbox organizations can incur additional IPU charges for your organization.

To create an additional organization, you must be a native user with the Admin role or a native user with the "AdditionalOrg creation" and "AdditionalOrg view" privileges.

To create an additional organization:

1. Log in to the production organization.
2. Open Administrator and select **Organization**.
3. Open the **Additional Organizations** tab.
4. Click **New Organization** and select **Additional Production Organization** or **Sandbox Organization**.
5. On the **New Organization** page, enter a user name for the administrator of the new organization and the organization name.

   The user name must be unique. It must be a valid email address, or it can contain only alphanumeric characters, hyphens, underscores, periods, and apostrophes.
6. Optionally, enter a description, the number of employees, and the address information.
7. Click **Save**.

The new organization appears on the **Additional Organizations** tab, and the status is Enabled. Informatica Intelligent Cloud Services sends a welcome email for the new organization administrator to your email address.

8. Log out of the production organization.

9. Click the Confirm Account link in the welcome email, and follow the prompts to activate the account for the new organization administrator.

When you finish activating the account, Informatica Intelligent Cloud Services logs you in to the new organization.

After you log in to the new organization, you can add other users and create runtime environments, connections, and assets.

CHAPTER 3

Metering

You can view metering information for your organization and sub-organizations. View metering information on the **Metering** page.

The information on the **Metering** page depends on your organization's license agreement:

- If you have a usage-based license, the **Metering** page displays a dashboard that includes the number of Informatica processing units (IPUs) that you have purchased, have consumed, and have remaining in the current billing cycle. You can also view meters that show the number of IPUs that you have used for each service.

- If you have feature-based licenses, the **Metering** page displays the amounts of computing resources that your organization uses and has remaining. The page also displays the usage limits set through your organization's licenses. The page doesn't mention IPUs since IPUs do not apply to feature-based licenses. The **Metering** page displays information as a dashboard or as a table, based on your licenses.

Informatica processing unit metrics

If your organization has the Intelligent Cloud Data Management feature, your license is based on Informatica Intelligent Cloud Services usage.

An Informatica processing unit (IPU) is a unit of credit used to pre-pay for using Informatica Intelligent Cloud Services scalars such as Compute Units and Events Processed. You can monitor your IPU balance and usage on the **Metering** page.

The following image shows the metering dashboard for an account that's set up for monthly billing periods:
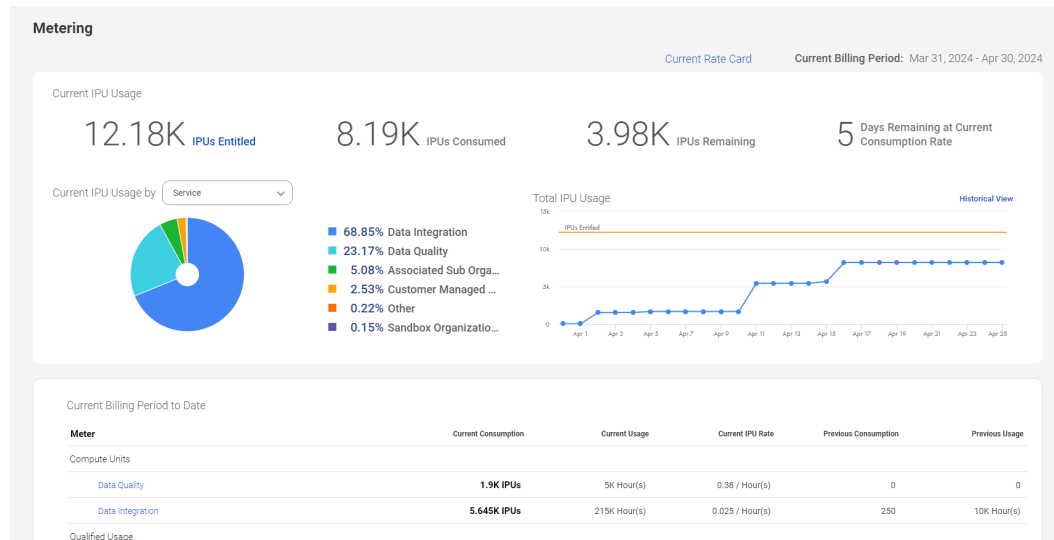
Users with the Admin role receive notification through email when the organization crosses the 25, 50, 75, 95, and 100% IPU consumption thresholds.

Viewing IPU metrics

View IPU metrics on the **Metering** page. The **Metering** page displays IPU information in a dashboard view.

The dashboard shows IPU usage for the organization that you're logged in to and linked organizations such as sub-organizations, additional production organizations, and sandbox organizations.

IPU billing periods

IPU billing periods can be on a monthly or annual basis. The **Metering** page for monthly billing is slightly different from the page for annual billing.

Monthly billing basis

If your billing period is on a monthly basis, you can view IPU information by billing periods. The metering dashboard includes the following panels:

Current IPU Usage

The **Current IPU Usage** panel includes the following information:

- The total number of IPUs entitled, consumed, and remaining in the current billing period.
- An estimate of the number of days remaining before the IPU balance is depleted based on current usage.
- The IPU usage for the billing period. You can view usage by meter, project, or folder.
  If you view the usage by project or folder, you have the option to see historical consumption by asset location.
- A graph that shows the total IPU usage per day.

To view historical information on IPU consumption, click **Historical View** and select the number of billing periods to include.

Current Billing Period to Date

The **Current Billing Period to Date** panel includes the following information for most meters:

- The IPU rate.
- The IPUs consumed in the current billing period and the previous billing period.
- Usage based on scalars such as compute units, data volume, and rows processed for the current billing period and previous billing period.

To view the details for a meter, click on the meter name. The details page shows the current usage by IPU and scalar, an historical usage graph that shows IPU usage for the selected number of billing periods, and detailed usage information by date.

Annual billing basis

If your billing period is on an annual basis, you can view IPU information by billing periods or by reporting periods, which are monthly. The metering dashboard includes the following panels:

IPU Usage

The **IPU Usage** panel includes the following information:

- The total number of IPUs entitled, consumed, and remaining in the current billing period.
- The total number of IPUs consumed in the current reporting period. The reporting period is the current month.
- The IPU usage for the billing period or reporting period. You can view usage by meter, project, or folder.
  If you view the usage by project or folder, you have the option to see historical consumption by asset location.
- A graph that shows the total IPU usage per day for the billing period or reporting period.

To view historical information on IPU consumption, click **Historical View** and select the number of reporting periods to include.

Current Billing Period to Date

The **Current Billing Period to Date** panel includes the following information for most meters:

- The IPUs consumed in the current billing period.
- The IPUs consumed in the current reporting period and the previous reporting period.
- Usage based on scalars such as compute units, data volume, and rows processed for the current reporting period and previous reporting period.

To view the details for each meter, click the meter name. The details page shows the current usage by IPU and scalar, an historical usage graph that shows IPU and scalar usage for the selected number of reporting periods, and detailed IPU usage information by reporting period.

IPU metrics for multiple organizations

You can view IPU usage information for sub-organizations, sandbox organizations, and additional production organizations.

You can find the following information for organization meters on the metering dashboard in the **Current Billing Period to Date** panel:

Meter	Description
Sandbox Organizations	Displays total IPU usage and consumption by scalar for the sandbox organizations directly linked to the organization that you're logged in to. Includes a link to the details page, which shows details for each sandbox organization.
Sub Organizations	Displays total IPU usage and consumption by scalar for the sub-organizations directly linked to the organization that you're logged in to. Includes a link to the details page, which shows details for each sub-organization.
Additional Production Organizations	Displays total IPU usage and consumption by scalar for the additional production organizations directly linked to the organization that you're logged in to. Includes a link to the details page, which shows details for each additional production organization.
Associated Sub Organizations IPU Usage	When logged in to the production organization, displays total IPU usage for all sub-organizations of sandbox or additional production organizations, along with the rate of 6 IPUs per sub-organization.

For example, a production organization has two sandbox organizations and one additional production organization. The sandbox organizations and the additional production organization each have a sub-organization.

When you log in to the production organization, you can find the following metering information:

- IPU usage, consumption by scalar, and detailed metering data for the production organization.
- Total IPU usage and consumption by scalar for the two sandbox organizations and detailed metering data for each sandbox organization.
- IPU usage, consumption by scalar, and detailed metering data for the additional production organization.
- Total IPU usage for the sandbox organizations' and additional production organization's sub-organizations.

When you log in to one of the sandbox organizations, you can find the following metering information:

- IPU usage, consumption by scalar, and detailed metering data for the sandbox organization.
- IPU usage, consumption by scalar, and detailed metering data for the sandbox organization's sub-organization.

Note: A lag of up to 10 minutes might occur before a linked organization's first IPU usage of the day is reflected on the production organization's **Metering** page.

IPU scalars

IPUs are based on scalar values. Appropriate scalars are used for each service.

For example, Data Integration usage is measured by Compute Units, and Cloud Integration Hub usage is measured by Events Processed.

The following table lists the primary scalars and their unit of measure:

Scalar value	Unit of measure	Description
API Calls	Million API calls	Number of custom API calls.
Compute Units	Hour	Processing capacity used or consumed.
Data Volume	Gigabyte	Volume of data transferred, transformed, or incorporated.
Events Processed	Event	Inbound and outbound instances of data accessing an intermediate storage layer.
Queries	Thousand queries	Number of queries submitted.
Records Stored	Record	Number of records stored. The value resets at the end of the billing period, rather than resetting daily.
Rows Processed	Million rows	Number of rows processed from underlying database logs.
Taskflow Runs	Runs	Number of taskflow runs.
Objects Processed	Thousand objects	Number of objects processed during assessment and conversion of PowerCenter assets to Cloud Data Integration assets.
Organizations	Number	Number of additional production organizations, sub-organizations, and sandbox organizations. If you delete a sub-organization, this number includes the deleted sub-organization until the next billing period starts.
Qualified Usage	Qualified IPUs	Percentage of total IPUs used in your organizations that have enabled customer managed keys. The value resets at the end of the billing period, rather than resetting daily.

IPU meters

IPU meters are the services and features included with Intelligent Cloud Data Management.

The following table lists the IPU meters and applicable scalars:

Meter	Scalar value
Advanced Data Integration	Compute Units
Advanced Data Integration with Advanced Serverless	Compute Units
Advanced Data Quality	Compute Units
Advanced Data Quality with Advanced Serverless	Compute Units
Advanced Pushdown Optimization	Rows Processed
API Management	API Calls
Application Integration	Compute Units

Meter	Scalar value
Application Integration with Advanced Serverless	Compute Units
B2B Gateway	Compute Units
Cloud Data Integration for PowerCenter	Compute Units
Cloud Data Integration for PowerCenter - Change Data Capture	Rows Processed
Cloud Data Integration for PowerCenter - Push Down Optimization	Rows Processed
Customer Managed Keys	Qualified Usage
Data Governance and Catalog	Compute Units
Data Governance and Catalog - 10,000 records per scalar unit for governance records - 100,000 records per scalar unit for catalog records	Records Stored
Data Integration	Compute Units
Data Integration with Advanced Serverless	Compute Units
Data Marketplace: 10,000 records per scalar unit	Records Stored
Data Masking	Compute Units
Data Quality	Compute Units
Data Quality with Advanced Serverless	Compute Units
Industry Solutions	Compute Units
INFACore	Compute Units
Integration Hub	Events Processed
Mass Ingestion Application (for Application Ingestion and Replication)	Data Volume
Mass Ingestion Applications - Change Data Capture (for Application Ingestion and Replication)	Rows Processed
Mass Ingestion Database (for Database Ingestion and Replication)	Data Volume
Mass Ingestion Database - Change Data Capture (for Database Ingestion and Replication)	Rows Processed
Mass Ingestion Files (for File Ingestion and Replication)	Data Volume
Mass Ingestion Streaming (for Streaming Ingestion and Replication)	Data Volume
MDM Data Ingestion and Replication (for Streaming Ingestion and Replication)	Data Volume
Model Serve	Compute Units
PC2CDI Modernization Service Assessment	Objects Processed

Meter	Scalar value
PC2CDI Modernization Service Conversion	Objects Processed
Additional Production Organizations	Organizations
Sandbox Organizations	Organizations
Sub Organizations	Organizations
Taskflow Runs	Taskflow Runs
Associated Sub Organizations IPU Usage	Organizations

IPU usage by asset location

The **IPU Usage by Asset Metadata** page shows the IPU usage data broken down by asset location.

You can view the usage data by project or by folder and choose a date range to view.

When you log in to the production organization, you can also see the usage by assets in sub-organizations of sandbox and additional production organizations. To view the project and folder data for a sub-organization, log in to that sub-organization.

IPU usage for disabled and deleted sub-organizations

Sub-organizations are counted in the Organizations scalar value for the Sub-organizations meter. Sub-organizations also consume IPUs based on other meters and scalar values.

Note the following rules regarding IPU consumption for disabled and deleted sub-organizations:

Disabled sub-organizations

When you disable a sub-organization, the sub-organization continues to consume IPUs for meters that use the following scalars:

- Records stored
- Organizations
- Qualified Usage

Deleted sub-organizations

After Informatica Global Customer Support completes the deletion process for a sub-organization, the sub-organization consumes six IPUs in the current billing period and doesn't consume IPUs in subsequent billing periods. If you delete a sub-organization in Administrator but you don't open a ticket for Informatica Global Customer Support to complete the deletion process, then the sub-organization continues to be counted in the Organizations scalar value and continues to consume IPUs.

After a sub-organization is deleted, the parent organization's metering page continues to display the sub-organization's metering data in historical views.

IPU metrics reports

You can download a report that includes a summary of IPU usage, IPU usage by asset location, or a report that includes details for a particular meter.

You can download the following types of reports:

IPU usage summary report

The IPU usage summary report includes a summary of IPU usage for the production organization and its sub-organizations, additional production organizations, and sandbox organizations. The report includes data for the selected billing or reporting periods. The report includes the following data by month for each meter:

- Scalar utilization

- IPU consumption

- Organization ID and name

Download the IPU summary report from the **IPU Usage History** page.

IPU usage detail report

The IPU usage detail report includes IPU consumption in the selected billing or reporting periods by project or folder. In the production organization, the report also includes consumption by its sub-organizations, additional production organizations, and sandbox organizations. Download the IPU usage detail report from the **IPU Usage by Asset Metadata** page.

Table view report

The table view report includes the information that's currently shown in the table on an IPU meter's details page. Download a table view report from the overview tab of the IPU meter's details page.

Asset breakdown report

The asset breakdown report includes the information that's shown on an IPU meter's asset breakdown tab. Download an asset breakdown report from the asset breakdown tab of the IPU meter's details page.

Detailed service report

For some meters, you can download a report for an IPU meter that includes service details for a specific date range. Download a detailed service report from the overview tab of the IPU meter's details page.

To download a report, click the **Download** icon. The following image shows the **Download** icon on the **IPU Usage History** page:
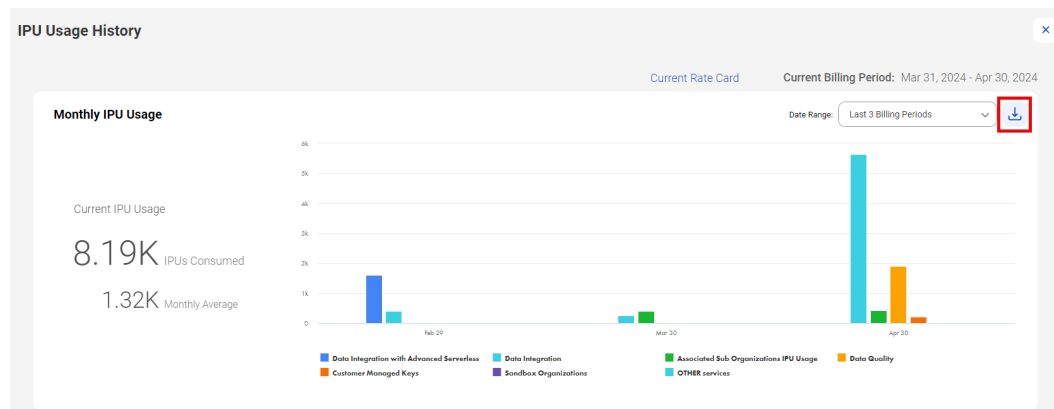
Downloading an IPU usage summary report

Download a summary report from the **IPU Usage History** page.

1. On the **Metering** page, click **Historical View**.
2. Select the billing periods that you want to include in the report, up to the last 13 billing periods.
3. Click the **Download** icon.
4. Click **Export**.

Downloading an IPU usage detail report

Download an IPU usage detail report from the **IPU Usage by Asset Metadata** page.

1. On the **Metering** page, view the **Current IPU Usage** chart by project or by folder.
2. Click **View Usage by Asset Metadata**.

    The **IPU Usage by Asset Metadata** page opens.
3. Select whether you want to view data by project or folder.
4. Select the billing periods that you want to include in the report, up to the last 13 billing periods.
5. Click the **Download** icon.

Downloading an IPU meter report

Download a report for a specific meter on the meter's details page. You can download a report that's based on the overview table or the asset breakdown table. For some meters, you can download a detailed service report.

1. On the **Metering** page, in the **Current Billing Period to Date** area, click the meter name.
2. Navigate to the overview tab or the asset breakdown tab based on the type of report you want to download.
3. Select the billing periods that you want to include in the report.
4. Click the **Download** icon.
5. If the option to download a detailed service report is available, the **Metering Usage Report** dialog box appears when you click the **Download** icon. Perform one of the following tasks:
    *   Select the table view report, and then click **Export**.
    *   Select the detailed service report, and then select the date range for the report and click **Export**.

Data Integration detailed reports

Data Integration detailed reports provide metering usage details for jobs that your organization ran within a specified time period.

Detailed reports for Data Integration can include the following fields:

Field	Description
Task ID	Unique ID to identify the task.
Task Name	Name of the job.

Field	Description
Task Object Name	Name of the object used in the job. Applicable to replication tasks and synchronization tasks.
Task Type	Type of task, for example mapping task or replication task.
Task Run ID	Run ID of the job.
Project Name	Project that contains the task.
Folder Name	Folder that contains the task. If the task is located directly under the project, this field is blank.
Org ID	Unique identifier for the organization.
Environment ID	Federated ID of the runtime environment.
Environment	Name of the runtime environment.
Cores Used	Number of cores used by the job.
Assigned SCU:	Requested serverless compute units. Applicable to serverless reports.
Start Time	Time when the job was started. Uses Coordinated Universal Time (UTC).
End Time	Time when the job was completed. Uses Coordinated Universal Time (UTC).
Status	Status of the job.
Metered Value	Processed rows for change data capture and advanced pushdown optimization reports. Consumed serverless compute units for serverless reports. Consumed compute hours for all other reports.
Audit Time	Time when the task reported for metering.
OBM Task Time(s)	Actual process time. Applicable to Salesforce OBMSG.

Feature-based license metrics

If your organization has feature-based licenses, the **Metering** page displays information based on your licenses.

The **Metering** page displays the following views depending on the licensed features:

Dashboard view

> If you have the appropriate licenses, the **Metering** page displays information in a dashboard view.

The Metrics Summary This Month area shows the total computing resources remaining for the month and each meter type. You can also display a table of all meters that apply to your organization, depending on your organization's editions.

The detail area for each meter type displays metering information for the month, including resource amounts remaining, average resource usage per day, and days of usage remaining. To see more detail for a meter type, you can display a detail chart that shows usage by organization or sub-organization, date range, and runtime environment.

License Metrics view

If you do not have the licenses required to see the dashboard view, the **Metering** page displays license metrics in a table. The table lists summary metrics for all meters that apply to your organization, which is determined by your organization's editions.

You can also navigate to the License Metrics view for all meters from the summary area in the dashboard view.

Note: Feature-based licensing is different from IPU-based licensing. IPUs are not used for feature-based licenses. If your organization uses IPUs, see .

Viewing license metrics

You can view a table of all meters used in your organization. For some meters, you can download a report that shows the metering usage. View the table and download the report from the License Metrics view of the **Metering** page.

To open the License Metrics view from the dashboard view, click **All Meters** in the Metrics Summary This Month area. If you do not have the licenses required to see the dashboard view, the License Metrics view is displayed when you open the **Metering** page.

The meters that appear in the License Metrics view are determined by the editions that your organization has. Your organization might also be assigned custom meters. Metering information might not be available for every edition.

If your organization has multiple editions or uses custom meters, a meter might be displayed multiple times with different limits. In this case, the least restrictive limit applies. For example, if one edition has a limit of 500 synchronization jobs per day and another edition has a limit of 100 synchronization jobs per day, the 500 job per day limit applies. The **In Effect** column indicates which limit applies.

The License Metrics view displays the following information for each meter:

Property	Description
Edition	Name of the edition that is associated with the meter.
Service	Service to which the meter applies.
Metering	Name of the meter. For example, the number of synchronization jobs per day, the number of rows processed by mapping jobs per month, or the total number of replication jobs. For Mass Ingestion, this column shows the ingestion type: File Ingestion and Replication, Application Ingestion and Replication, Database Ingestion and Replication, Application Ingestion and Replication - Change Data Capture, Database Ingestion and Replication - Change Data Capture, and Streaming Ingestion and Replication.

Property	Description
Limit	Numeric limit such as the maximum number of jobs or processed rows. The limit applies to the parent organization and to each sub-organization. For example, if the limit is 100 jobs per day, users in the parent organization can run 100 jobs per day, and users in each sub-organization can also run 100 jobs per day. If this field displays -1, there is no limit.
Used	The actual number units consumed, such as the number of jobs run or compute hours used, in the organization or sub-organization during the metering period.
Percent Used	The percentage of units consumed in the organization or sub-organization during the metering period.
In Effect	Indicates whether the meter is in effect for the organization or sub-organization.

Meter definitions

The meters that appear in the License Metrics view of the **Metering** page are determined by the editions that your organization has.

The following table describes the meters that might be in effect based on your editions:

Meter	Definition
Advanced Data Integration	Compute units measured in hours for mappings in advanced mode.
Advanced Data Integration with Advanced Serverless	Serverless compute units measured in hours for mappings in advanced mode.
Advanced Data Quality	Compute units measured in hours for data quality assets in mappings in advanced mode.
Advanced Data Quality with Advanced Serverless	Serverless compute units measured in hours for data quality assets in mappings in advanced mode.
CDI Rows Processed	Number of rows processed by mappings outside of advanced mode.
CDI-E Compute Hours	Deprecated. This meter has been replaced with the Advanced Data Integration meter.
Daily/monthly incoming API request maximum	Number of API access requests per day or per month.
Data Integration with Advanced Serverless	Serverless compute units measured in hours for mappings outside of advanced mode.
Data Quality	Compute units measured in hours for data quality assets in mappings outside of advanced mode.
Data Quality with Advanced Serverless	Serverless compute units measured in hours for data quality assets in mappings outside of advanced mode.

Meter	Definition
Mass Ingestion meters	For Mass Ingestion Applications, Mass Ingestion Databases, Mass Ingestion Files, and Mass Ingestion Streaming, the number of gigabytes (GBs) ingested by application ingestion and replication, database ingestion and replication, file ingestion and replication, or streaming ingestion and replication jobs per month. For Mass Ingestion Applications - Change Data Capture and Mass Ingestion Databases - Change Data Capture, the number of rows ingested. For MDM Data Ingestion and Replication, the number of gigabytes (GBs) ingested by streaming ingestion and replication tasks run by MDM users who publish real-time events from MDM SaaS.
Taskflow Runs	Number of taskflow runs per day or per month.
Number of PowerCenter jobs per day/month	Number of PowerCenter jobs per day or per month.
Number of mapping jobs per day/month	Number of mapping jobs per day or per month.*
Number of masking jobs per day/month	Number of masking jobs per day or per month.
Number of replication jobs per day/month	Number of replication jobs per day or per month.
Number of rows processed by PowerCenter jobs per day/month	Number of rows processed by PowerCenter jobs per day or per month.
Number of rows processed by mapping jobs per day/month	Number of rows processed by mapping jobs per day or per month.*
Number of rows processed by masking jobs per day/month	Number of rows processed by masking jobs per day or per month.
Number of rows processed by replication jobs per day/month	Number of rows processed by replication jobs per day or per month.
Number of rows processed by synchronization jobs per day/month	Number of rows processed by synchronization jobs per day or per month.
Number of state sync jobs per day	Number of state synchronization jobs per day. State synchronization jobs include the fetchState and loadState jobs that you run through the REST API.
Number of sub-organizations	Number of sub-organizations. If you delete any sub-organizations, this meter includes the deleted sub-organizations.
Number of synchronization jobs per day/month	Number of synchronization jobs per day or per month.
Number of user-management create requests	Number of user management creation requests. User management creation requests include requests to create users, user groups, and custom roles.
Serverless CDI Compute Hours	Deprecated. Serverless compute units measured in hours for mappings outside of advanced mode.

Meter	Definition
Serverless CDI-E Compute Hours	Deprecated. Serverless compute units measured in hours for mappings in advanced mode.
Total Serverless units used	Deprecated. Total number of serverless compute units used to run tasks.
Total compute hours used by elastic cluster nodes	Deprecated. This meter has been replaced with the Advanced Data Integration meter.
Total number of PowerCenter jobs	Total number of PowerCenter jobs.
Total number of agents	Total number of Secure Agents, including agents that are stopped. Does not include the Informatica Cloud Hosted Agent.
Total number of connections	Total number of connections.
Total number of folders	Total number of folders.
Total number of mapping jobs	Total number of mapping jobs.*
Total number of masking jobs	Total number of masking jobs.
Total number of projects	Total number of projects.
Total number of replication jobs	Total number of replication jobs.
Total number of rows processed by PowerCenter jobs	Total number of rows processed by PowerCenter jobs.
Total number of rows processed by mapping jobs	Total number of rows processed by mapping jobs.
Total number of rows processed by masking jobs	Total number of rows processed by masking jobs.
Total number of rows processed by replication jobs	Total number of rows processed by replication jobs.
Total number of rows processed by synchronization jobs	Total number of rows processed by synchronization jobs.
Total number of synchronization jobs	Total number of synchronization jobs.

Guidelines for Data Quality and Data Profiling assets

If you run a mapping outside of advanced mode in which a transformation reads a data quality asset, Informatica records transactions for the mapping in the Data Quality meter. If you run a mapping in advanced mode in which a transformation reads a data quality asset, Informatica records transactions for the mapping in the Data Quality Elastic meter.

If you run a profile on the Data Integration Server, Informatica records transactions for the profile in the Data Quality meter. If you run a profile on an advanced cluster, Informatica records transactions for the profile in the Data Quality Elastic meter.

You can preview the output data on a transformation in a mapping. If you preview the data on a transformation that reads a data quality asset, Informatica calculates the cost in the following ways:

- If the mapping that contains the transformation runs outside of advanced mode, it consumes Data Quality compute hours.
- If the mapping that contains the transformation runs in advanced mode, it consumes Data Quality Elastic compute hours.

Metering serverless compute units

When you view the total serverless compute units used, the meter is based on the number of serverless compute units that your organization uses to run tasks.

When the serverless runtime environment runs a task, the environment creates a virtual machine with resources based on the number of compute units that the task requests.

The minimum task duration is two minutes. If the task completes in less than two minutes, the serverless runtime environment consumes two minutes of compute units. After two minutes, compute units are consumed by the second.

If you cancel the job, the number of consumed compute units is the greater of the following values:

- The time that the job was running before it was canceled
- Two minutes

Guidelines for advanced clusters

To run a mapping in advanced mode, the serverless runtime environment creates an advanced cluster that contains one worker node with resources based on the number of serverless compute units that the task requests. If you run another task, the environment reuses idle worker nodes or adds worker nodes to the cluster to reserve additional resources.

Metering begins when the task starts running and ends when the task is complete. Metering doesn't include the time to compile the job or the time to start the cluster.

Metering doesn't take effect if the job fails before the cluster has been created, such as when the job fails to compile, the cluster fails to start, or you cancel the job before the cluster starts.
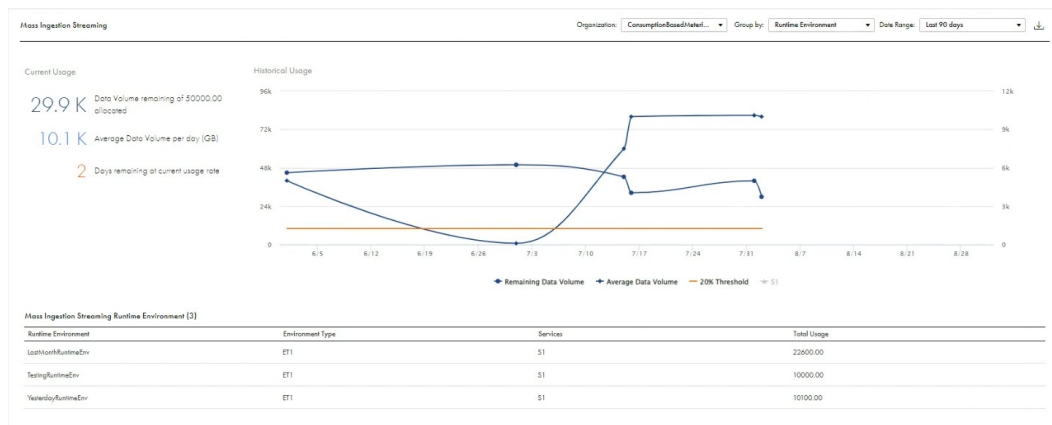
Viewing usage details

You can view detailed metering statistics. To view the detailed statistics, in the dashboard view of the **Metering** page, click **Detail Chart** for the relevant graph.

Detailed metering statistics are available for the following meters:

- Application Integration
- Application Integration with Advanced Serverless
- Catalog Records
- CDI-E Compute Hours
- Serverless CDI-E Compute Hours
- Serverless CDI Compute Hours
- Data Quality
- Data Quality Elastic
- Data Quality with Advanced Serverless

- Data Quality Elastic with Advanced Serverless

- Governance Records

- Mass Ingestion Application

- Mass Ingestion Applications - Change Data Capture

- Mass Ingestion Database

- Mass Ingestion Database - Change Data Capture

- Mass Ingestion Files

- Mass Ingestion Streaming

- MDM Data Ingestion and Replication

- PC2CDI Modernization Service Assessment

- PC2CDI Modernization Service Conversion

The following image shows an example of the details page that shows the total usage for each runtime environment in the last 90 days:

You can customize the view in the following ways:

- If your organization has sub-organizations, you can view usage details for the parent organization or for a sub-organization. You cannot view usage details for a deleted sub-organization.

- You can change the grouping. For example, you can group by runtime environment to see total usage for each runtime environment or you can view the full table to see usage by date.

- You can change the date range that defines the reporting period, such the current month, last month, last 90 days, or last 6 or 13 months.

Metering usage reports

If your organization uses Application Integration, the Data Ingestion and Replication service, advanced clusters, Cloud Data Integration for PowerCenter (CDI-PC) to modernize PowerCenter assets, or a serverless runtime environment, you can download a metering usage report.

A metering usage report contains the following information:

- For Application Integration, the report contains execution details of processes, app connections, and OData APIs. For an Application Integration advanced serverless runtime environment, the report contains execution details of processes and guides.

- For Application Ingestion and Replication and Database Ingestion and Replication, the report content depends on the load type of the ingestion and replication job. For jobs that perform initial loads, the report contains the volume of data ingested in GBs. For jobs that perform incremental loads, the report contains the number of records or rows processed. For jobs that perform combined initial and incremental loads, both reports are available.
- For File Ingestion and Replication, the report contains details about the volume of data ingested by file ingestion and replication tasks.
- For Streaming Ingestion and Replication, the report contains details about the volume of data ingested by streaming ingestion and replication jobs.
- For advanced clusters, the report contains details about the compute hours for cluster nodes.
- For Cloud Data Integration for PowerCenter (CDI-PC), the report contains details such as the date and time when assessment or conversion jobs were run, organization ID, job details, and the number of objects processed during assessment or conversion.
- For a serverless runtime environment, the report contains details about the number of serverless compute units that were requested and consumed to run tasks.

If your organization does not use Application Ingestion and Replication, Database Ingestion and Replication, File Ingestion and Replication, Streaming Ingestion and Replication, advanced clusters, or a serverless runtime environment, no metering usage reports are available.

Downloading a metering usage report from Detail Chart

Download a metering usage report from the Detail Chart view of the **Metering** page.

1. In Administrator, select **Metering**.
2. Click **Detail Chart** for the metering usage report you want to download.
3. Select the organization and the date range that you want to view.

   The report data adjusts accordingly.
4. Click the download icon.
5. Click **Export**.

CHAPTER 4

General and security settings

You can configure general and security settings on the **Settings** page.

Based on your organization's licenses, you can configure the following settings:

Source control settings

You can configure source control for your organization to enable version management for projects, folders, and assets. Configure a connection to the global source control repository for your organization. You can configure read/write or read-only access to the repository. You can also enable project-level source control so that users can link source control repositories to specific projects.

For more information, see "Source control configuration" on page 47.

Upgrade settings for Secure Agent services

If a service that supports rolling upgrades encounters an error during an upgrade, you can specify whether to continue or stop upgrading the service. For more information, see "Rolling upgrades for Secure Agent services" on page 54.

You can also configure a restart schedule for services that need to be restarted after minor upgrades. To configure a restart schedule, select the day of the week and the time to perform the upgrades. For more information, see "Restart schedule configuration for Secure Agent services" on page 56.

Custom branding settings

You can configure custom branding settings for your parent organization and apply them to your sub-organizations. You can also configure custom branding settings for each sub-organization based on your requirement. The custom branding settings include logo, color theme, and favicon.

When you configure the custom branding settings, Reference 360 service displays the logo and favicon that you provide.

For more information, see "Custom branding configuration" on page 56.

Customer managed encryption key settings

You can use your own master key to encrypt your organization's encryption keys instead of using Informatica's master key.

To create and use your own master key, first provision the key in your cloud provider's key management service and enable cross-account access with Informatica Intelligent Cloud Services. Then, enable the **Enable Customer Managed Keys** option on the **Security** tab and enter the key properties.

For more information, see "Customer managed encryption keys" on page 57.

Secrets manager configuration settings

You can configure your organization to retrieve sensitive connection credentials from an external secrets manager like AWS Secrets Manager or Azure Key Vault. To configure a secrets manager for your

organization, select the **Enable Secrets Manager** option on the **Security** tab and enter the connection details.

For more information, see "Secrets manager configuration" on page 61.

Source control configuration

You can configure source control for your organization to enable version management for projects, folders, and assets. When you configure source control, you can store versions of objects in a cloud-hosted or on-premises Git repository. Configure source control on the **Settings** page.

To use source control with Informatica Intelligent Cloud Services, you must have the appropriate licenses.

The following table lists the source control repositories that you can use:

Repository	Self-hosted	Cloud-hosted
Atlassian Bitbucket	Supported	Supported (see Note)
GitHub	Supported	Supported
GitLab	Supported	-
Microsoft Azure DevOps	-	Supported

Note: You can use cloud-hosted Bitbucket repositories for Data Integration assets.

When you configure source control for an organization, users can apply source control to objects. Objects are not checked in automatically. Users can apply source control to individual assets or to all assets in a project or folder. For more information about applying source control to projects, folders, and assets, see the help system for the appropriate Informatica Intelligent Cloud Services service.

When you configure source control, you configure the connection to a global source control repository for the organization. You can configure source control for your organization in the following ways:

Configure read/write access to the global source control repository.

When you configure read/write access, users in your organization can check in and check out objects, pull versions of objects, and revert objects to a previous version. Users must check out source-controlled objects to change them. Users check out objects exclusively, so one user cannot change an object that is checked out by another user. Users can change objects that are not source-controlled without checking them out.

You might want to configure read/write access for an organization in which you develop projects and assets.

Configure read-only access to the global source control repository.

When you configure read-only access, users in your organization can pull versions of source-controlled objects from the repository. However, users cannot check out or check in objects. Users can make changes to projects, folders, and assets in the organization without checking them out.

You might want to configure read-only access for a test or production organization so that users can test or run the latest versions of assets.

You can change the repository access type. However, to change from read/write to read-only, you must first ensure that no objects are checked out. Informatica Intelligent Cloud Services doesn't allow you to change the repository access type from read/write to read-only if any objects are checked out.

Warning: When you configure read-only access, users can overwrite source-controlled objects. For example, user John pulls the most recent version of a source-controlled mapping and changes it. If another user pulls any version of the mapping later, John's changes are lost. Configure object permissions and user privileges carefully to prevent users from accidentally overwriting source-controlled assets in your organization.

Enable project-level repositories

You can enable users to specify a branch in the global repository or a different repository for each project. Using different repository branches for your projects can enable parallel development and collaboration across teams in the organization.

You can change the repository URL. To do this, you must first unlink all source-controlled assets. Informatica Intelligent Cloud Services doesn't allow you to change the repository URL if any assets are source-controlled.

If you want to disable source control after you configure it, unlink all objects from source control and then disable source control for the organization.

You can unlink an object that's checked out by another user if you have the admin role or a user role with the Force Undo Checkout privilege.

Source control configuration for sub-organizations

Configure source control for a sub-organization on the **Settings** page in the sub-organization. As a best practice, each sub-organization should use its own source control repository. Additionally, the source control repository for a sub-organization should be different than the source control repository for the parent organization.

Maintain different source control repositories so that users in one organization do not accidentally overwrite or change assets in another organization.

If you want the parent organization administrator to be able to perform source control operations in the sub-organization, configure the Git user account for the parent organization administrator to have access to the sub-organization's source control repository.

Repository access using OAuth

If your source control repository is cloud-hosted, you can configure an organization to use OAuth authentication instead of personal access tokens to provide access to the repository. Configure OAuth authentication on the **Settings** page.

If you use a GitHub repository, you must have a GitHub access application installed on your repository that allows Informatica Intelligent Cloud Services to perform source control operations on the organization's GitHub repository. If you don't have this application installed on your repository, you can install it from the **Settings** page.

Working with an on-premises repository

If your source control repository is on-premises, the Secure Agent creates a local copy of the repository on the Secure Agent machine. The Secure Agent performs source control operations in the local repository and then pushes them to the remote repository.

When you use an on-premises repository, ensure that the Secure Agent machine has enough space for the local copy of the repository and for all subsequent version control operations.

The Secure Agent creates the local repository the first time that a user performs a source control operation, such as checking in an asset. When it creates the local repository, it copies the branch that stores Informatica Intelligent Cloud Services assets. It does not copy other branches. Each time a user performs a source control operation, the agent gets information about the changes from the remote repository to support the operation.

By default, the Secure Agent creates the local repository in the following directory on the Secure Agent machine:

```
<Secure Agent installation directory>/apps/GitRepoConnectApp/data/git_repository/<client URL>/<organization ID>/<branch>/<remote repository name>
```

You can change the local repository directory by editing the **git_local_repository_path** property for the GitRepoConnectApp service on the Secure Agent details page. For more information about changing the value of this property, see *Secure Agent Services*.

Enabling source control for an organization

To enable source control for an organization, configure the type of access and connection to the global source control repository on the **Settings** page. The settings that you configure vary based on the repository type.

1. On the **Settings** page in Administrator, click **Edit** in the Source Control area.
2. Enable the **Enable Source Control** option.
3. Optionally, enable the **Enable Project Level Source Control** option.

    When this option is enabled, users can specify a branch in the global repository or a different repository to use at the project level.
4. Configure the type of access to the source control repository:
    -   To configure read/write access, enable the **Allow Push to Git Repository** option.
    -   To configure read-only access, disable the **Allow Push to Git Repository** option.
5. To configure access to a cloud-hosted repository, enter the following information:

Option	Description
Platform	Platform type. Select **Cloud**.
Repository Type	Version control system that you use for the organization. You can use one of the following cloud-hosted systems: • GitHub • Microsoft Azure DevOps • Atlassian Bitbucket (for Data Integration)

Option	Description
Global Git Repository URL	Repository URL. For example: `https://github.com/MyGitUser/MyRepositoryName.git` The repository URL must use the HTTPS protocol. **Tip:** You can find the repository URL by selecting the clone option in the repository.
Global Git Branch Name	Name of the branch that stores the Informatica Intelligent Cloud Services objects. The branch that you specify must already exist in the repository. If you do not enter a branch name, Informatica Intelligent Cloud Services sets the branch name to "master" or "main," based on the name of the default branch in the remote repository.
Allow OAuth access to Git	Enable this option to use OAuth to access the repository. If you use a GitHub repository, a Git access application that authorizes Informatica Intelligent Cloud Services access must be installed on the organization's repository. To install the application, click **Install Git Access App at GitHub**.

6. To configure access to an on-premises repository, enter the following information:

Option	Description
Platform	Platform type. Select **On-Premise**.
Git Repository URL	Repository URL. For example: `https://gitlab.example.com/MyGitUser/MyRepositoryName.git` The repository URL must use the HTTPS protocol. **Tip:** You can find the repository URL by selecting the clone option in the repository.
Git Branch Name	Name of the branch that stores the Informatica Intelligent Cloud Services objects. The branch that you specify must already exist in the repository. If you do not enter a branch name, Informatica Intelligent Cloud Services sets the branch name to "master" or "main," based on the name of the default branch in the remote repository.
Runtime Environment	Runtime environment used to connect to the Git repository. The repository must be accessible by all agents in the runtime environment that you select.

You cannot configure OAuth access to an on-premises repository.

7. Click **Save**.

Informatica Intelligent Cloud Services prompts you for your source control credentials to verify the repository connection. Informatica Intelligent Cloud Services does not store this information.

If the connection is valid and you configure read/write access to the repository, Informatica Intelligent Cloud Services writes a small readme file to the repository to verify that it can push objects to the repository.

After you enable source control, all users that use source control must enter their source control credentials in their user settings. Users cannot see source control columns on the **Explore** page or perform source control actions until they enter their source control credentials. To enter source control credentials, click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window, and select **Settings**.

Changing the source control repository URL

To change the source control repository URL, you must first unlink all objects in the organization and then enter the new repository URL on the **Settings** page in Administrator. After you change the URL, all users that use source control must update their source control credentials in the user settings.

1. In each Informatica Intelligent Cloud Services service that uses the repository, unlink all objects from source control.
2. In Administrator, open the **Settings** page and click **Edit** in the Source Control area.
3. Verify that the **Enable Source Control** option is enabled.
4. Configure the type of access to the source control repository:
   - To configure read/write access, enable the **Allow Push to Git Repository** option.
   - To configure read-only access, disable the **Allow Push to Git Repository** option.
5. Verify the platform and name of the branch that stores the Informatica Intelligent Cloud Services objects. For a cloud-hosted repository, verify the OAuth access setting, as well.
6. Enter the new repository URL, for example:

   `https://github.com/MyGitUser/MyRepositoryName.git`

   Tip: You can find the repository URL in the following ways based on the repository type:

Repository	How to find URL
Atlassian Bitbucket (self- hosted and cloud-hosted)	Open the repository and select **Clone**.
GitHub (cloud-hosted)	Open the repository and select **Clone or download** > **Clone with HTTPS**.
GitHub Enterprise (self-hosted)	Open the repository and select **Code** > **Clone with HTTPS**.
GitLab Self-Managed	Open the repository and select **Clone** > **Clone with HTTPS**.
Microsoft Azure DevOps (cloud-hosted)	Open the repository and select **Clone**.

   The repository URL must use the HTTPS protocol.
7. Click **Save**.

   Informatica Intelligent Cloud Services prompts you for your source control credentials to verify the repository connection. Informatica Intelligent Cloud Services does not store this information.

   If the connection is valid and you configure read/write access to the repository, Informatica Intelligent Cloud Services writes a small readme file to the repository to verify that it can push objects to the repository.

After you change the source control repository URL, all users that use source control must update their source control credentials in the user settings. To update source control credentials, click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window, and select **Settings**.

Disabling source control for an organization

You can disable source control for an organization. Disabling source control breaks the link between your organization and the source control repository. It does not delete objects in the source control repository.

Before you can disable source control for a read-write organization, all assets must be unlinked.

1. In each Informatica Intelligent Cloud Services service that uses the repository, unlink all objects from source control.
2. In Administrator, disable source control:
   a. In Administrator, open the **Settings** page.
   b. Click **Edit** in the Source Control area.
   c. Disable the **Enable Source Control** option.
   d. Click **Save**.
3. Optionally, have users in the organization delete their source control credentials in their user settings:
   a. In the top right corner of the Informatica Intelligent Cloud Services window, click the **User** icon and select **Settings**.
   b. Clear the source control credentials.
   c. Click **Save**.

Configuring repository access

To work with source controlled objects, specify your repository credentials in Informatica Intelligent Cloud Services.

Your credentials can include a personal access token or app password, depending on the repository service that you use.

If your administrator has configured the organization's repository for OAuth access, you can enable OAuth access instead of providing a personal access token or app password.

Personal access tokens and app passwords must be configured to enable full control of private repositories. For information about generating personal access tokens, see the GitHub or Azure DevOps Git help. For information about generating app passwords, see the Bitbucket help.

In Informatica Intelligent Cloud Services, perform the following steps to configure access to the repository:

1. Click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window and then select **Settings**.
2. Perform one of the following tasks:
   - Enter your repository credentials.
   - Enable OAuth access to the repository. For GitHub and Azure DevOps Git repositories, if you have not already authorized access, a Git access app appears. Select to authorize access for Informatica Intelligent Cloud Services.
3. Click **Save**.

Source control best practices

To ensure that your organization configures and uses source control effectively, use the following guidelines as best practices.

Setup guidelines

Adhere to the following guidelines when you set up source control for your organization:

- Use different organizations for development, testing, staging, and production.

  When you maintain different organizations, you maintain isolation across environments so that changes in one environment do not affect other environments. For example, changes to assets in the testing environment are not accidentally deployed in the production environment.

- Configure development organizations with read/write access to the source control repository, and configure non-development organizations with read-only access to the source control repository.

  This ensures that only users in a development organization can make changes to assets. It also prevents users in a non-development environment from accidentally pushing changes to the source control repository.

- Ensure that only one development organization pushes to a particular source control repository.

  Maintaining separate repositories for development organizations ensures that users in one organization do not accidentally change or overwrite assets in a different organization. Maintaining separate repositories also avoids conflicting asset ID references from different organizations.

- When you enable source control for the organization, select an empty repository.

  Ensure that the repository does not contain a folder named "Explore" because Informatica Intelligent Cloud Services stores assets under the Explore folder in the Git repository.

- Do not share source control credentials among multiple Informatica Intelligent Cloud Services users.

  Separate credentials maintain security and make it easier to track which user made a particular change. Additionally, each user gets their own rate limit in GitHub.

Development guidelines

Adhere to the following guidelines as you develop and work with assets:

Guidelines for managing dependencies

Use the following guidelines to manage assets with dependencies:

- Create connections and runtime environments before you pull assets from the repository.

  When required connections and runtime environments exist in the target organization, you can run tasks immediately after you pull them from the repository.

- Ensure that reusable assets such as mappings and components are present in the repository before you use them.

  Informatica Intelligent Cloud Services does not allow you to save an asset such as a mapping task when the dependent mapping does not exist in the organization.

Guidelines for checking in and checking out assets

Use the following guidelines when you check in and check out assets:

- When you rename or move an asset, check out the asset's first-level dependent assets and include them in the same check-in.

  For example, if you want to rename a mapping that a mapping task uses, and the mapping task is used in a taskflow, check out the mapping and the mapping task. You don't need to check out the taskflow. After you rename the mapping, check in the mapping and the mapping task in one check-in action.

- Enter comments when you check in assets.

  When you check in assets, you might enter a release tag name in the **Summary** field and enter more descriptive comments in the **Description** field. When you do this, the **Git Summary** field in Informatica Intelligent Cloud Services shows the release tag that is associated with the asset.

- When you check in multiple assets at one time, limit the number of assets to 1000 or fewer.

  Checking in more than 1000 assets at one time can degrade performance between Informatica Intelligent Cloud Services and the Git repository service.

Undoing a checkout for another user

If you have the Admin role or your user role has the Force Undo Checkout feature privilege for the Administrator service, you can undo the checkout of an object that has been checked out by another user. You might need to undo the checkout of an object that has been checked out by another user if the user has checked out objects and goes on vacation or leaves the organization.

When you undo a checkout, the object reverts to the last version in the source control repository. The object's version history will not include a record of the checkout and undo checkout actions. If you think you might need the changed version later, make a copy of the object before you undo the checkout.

An undo action is not recursive. If you undo the checkout of a project or folder, the lock for the project or folder is released but the objects within the project or folder remain locked.

1. Open the service in which the user checked out the object.

2. On the **Explore** page, navigate to the object.

3. In the row that contains the object, click **Actions** and select **Undo Check Out**.

   The undo action releases the lock so that the object is available for checkout.

   Note: If an object was moved or renamed after it was checked out, undoing the checkout will restore the object's name and location to its name and location before it was checked out.

Rolling upgrades for Secure Agent services

Some Secure Agent Services support rolling upgrades. In a rolling upgrade, services that run on the agents within a Secure Agent group are upgraded sequentially. Therefore, while a service is being upgraded on one agent, the service remains available on other agents in the group.

The following Secure Agent service supports rolling upgrades:

- Process Server

Other services that run on the agents within a Secure Agent group are upgraded on each agent simultaneously. Therefore, they are unavailable while the agents in the group are being upgraded. They become available again when all agents in the group have been successfully upgraded.

Example

Your organization uses the following runtime environments:

- Secure Agent group A:

    Agent A1 runs Data Integration Server and Process Server.

    Agent A2 runs Data Integration Server, Mass Ingestion, and Process Server.

- Secure Agent group B:

    Agent B1 runs Data Integration Server, Mass Ingestion, and Process Server.

    Agent B2 runs Data Integration Server, Mass Ingestion, and Process Server.

When your organization is upgraded, Secure Agent groups A and B are upgraded simultaneously. Within each Secure Agent group, Process Server is upgraded sequentially. Therefore, while Process Server is being upgraded on agents A1 and B1, it remains up and running on agents A2 and B2. When the upgrade finishes on agents A1 and B1, Process Server is upgraded on agents A2 and B2.

Data Integration Server and Mass Ingestion do not support rolling upgrades. In groups A and B, Data Integration Server is upgraded on each agent simultaneously. In group B, Mass Ingestion is upgraded on agents B1 and B2 simultaneously.

Rolling upgrade error handling

If a service that supports rolling upgrades encounters an error during an upgrade, you can specify whether to continue or stop upgrading the service. Configure the error handling behavior on the **Settings** page.

You can select either of the following options:

In case of error, flag error and continue with upgrade

  If an error occurs while a service is being upgraded, the service stops with an error on the agent in which it encountered the error. The upgrade then continues on the other agents within the group.

  Warning: If you enable this option and the error occurs on all agents in the group, the service stops running on the Secure Agent group. This can cause job interruptions.

In case of error, stop upgrade

  If an error occurs while a service is being upgraded, the service stops with an error on the agent in which it encountered the error. Upgrade of the service stops for all other agents in the group that have not already been upgraded. The agents that have not been upgraded continue to run the previous version of the service.

  This is the default option.

To configure the error handling behavior, click **Edit** in the Upgrade Settings for Secure Agent Services area, select the appropriate option, and click **Save**.

Restart schedule configuration for Secure Agent services

Some Secure Agent services such as Process Server might need to be restarted after they are upgraded. You can configure a restart schedule for some of these services after a minor upgrade such as a monthly upgrade or a patch release. Configure the restart schedule on the **Settings** page.

When you configure a restart schedule, you select the day of the week and time in which to restart the services. For example, you might schedule the restarts for Sundays at 00:00 GMT.

You can configure a restart schedule for the Process Server service. To configure the restart schedule, perform the following steps:

1. In Administrator, select **Settings**.
2. Click **Edit** in the **Upgrade Settings for Secure Agent Services** area.
3. Select a day and time.
4. Click **Save**.

If you do not configure a restart schedule, by default, the Process Server service is automatically restarted 7 days after your Point of Deployment (POD) is upgraded.

Custom branding configuration

You can customize the branding configuration to use a custom logo, color theme, and favicon instead of the Informatica defaults. Configure custom branding on the **Settings** page.

Custom branding settings are applied to the following services:

- Data Governance and Catalog
- Data Marketplace
- Metadata Command Center
- MDM - Customer 360 SaaS
- MDM - Product 360 SaaS
- MDM - Reference 360
- MDM - Supplier 360 SaaS
- Multidomain MDM SaaS

To customize branding configuration, you must have the appropriate license.

Logo and favicon guidelines

Use the following guidelines when you upload a logo and favicon for your organization:

- The file size for logo and favicon images must be less than 1 MB.
- The maximum size of logo images must be 80 x 325 pixels. The recommended size is 48 x 325 pixels.
- When you upload a logo image, the image is placed within the outlined region. Use the zoom control option to resize the image so that the image fits in the outlined region.
- The maximum size of favicon images must be 196 x 196 pixels. The recommended size is 32 x 32 pixels.

- Use the PNG, JPG, and GIF format for the custom logo and the PNG format for the favicon.

Configuring custom branding for an organization

You can upload a logo and a favicon, and select a color theme on the **Settings** page.

1. On the **Settings** page in Administrator, click **Edit** in the **Custom Branding** area.
2. Select **Enable Custom Branding**.
3. If you want the sub-organizations to inherit the branding configuration from the parent organization, select **Sub-Organizations inherits custom branding**.
4. To update a logo image, click **Upload** and select the logo file. For more information about the logo guidelines, see "Logo and favicon guidelines" on page 56.
5. To update a favicon image, click **Upload** and select the favicon file. For more information about the favicon guidelines, see "Logo and favicon guidelines" on page 56.
6. Select the color theme to match the logo and favicon. You can also create a theme.
7. Preview and verify the changes in the Preview section before applying the custom branding settings.
8. Click **Save**.

Customer managed encryption keys

You can use your own master key to encrypt your organization's encryption keys.

By default, Informatica Intelligent Cloud Services protects your organization's sensitive data in the cloud using organization-specific encryption keys that are generated and stored in the Informatica Intelligent Cloud Services key management service (KMS). To prevent malicious access, the keys are encrypted using a master key that is stored in the cloud provider's KMS. The master key is provisioned in Informatica's KMS account and varies by POD.

If you prefer, you can create a customer managed key (CMK). When you create a CMK, you control access to it. However, you'll need to grant Informatica Intelligent Cloud Services access to the CMK so that it can encrypt and decrypt your organization's sensitive data.

Creating a CMK offers the following benefits:

- You can restrict and control any access to your data.
- You can restrict the decryption of your data in the event of a data breach.
- You create and hold the key material in your KMS. The key is never exposed to your cloud service provider.
- You maintain full control of the key throughout its lifecycle. You can revoke access or delete the key at any time.

The following image shows how Informatica Intelligent Cloud Services interfaces with your CMK:
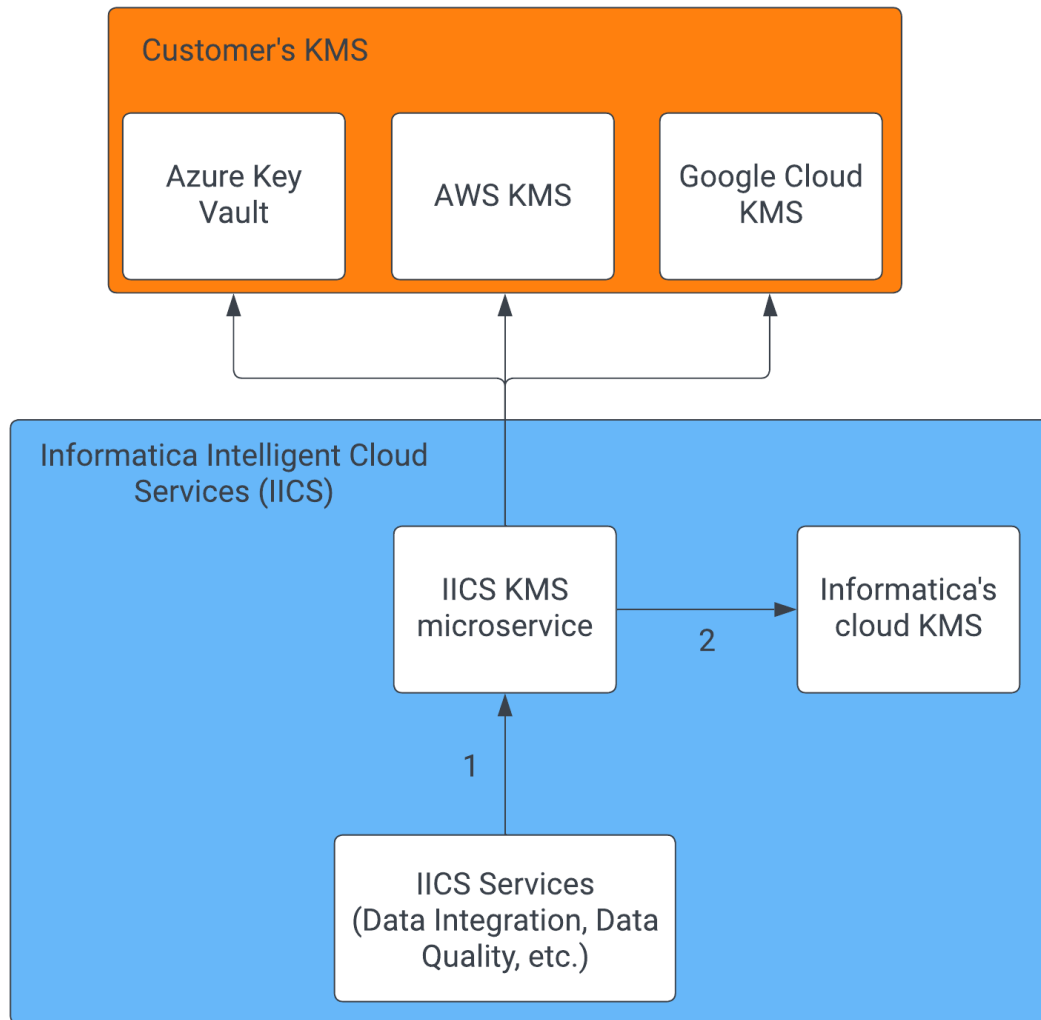
1. Informatica Intelligent Cloud Services interfaces with the Informatica Intelligent Cloud Services KMS agnostically.
2. Non-customer managed keys go to Informatica's cloud KMS.

You can create and enable a CMK when you use the following cloud providers' key management services:

- Amazon Web Services

- Microsoft Azure

- Google Cloud

Note: When you create a CMK, your KMS and Informatica Intelligent Cloud Services POD must use the same cloud provider. For example, if your Informatica Intelligent Cloud Services POD is USW1 on AWS, then you must store your CMK in AWS KMS. You can't store it in Google Cloud KMS or Azure Key Vault.

Creating and enabling a customer managed key

To create and enable a customer managed key, provision the key in your KMS and then enable customer managed keys in Administrator.

Note: The steps you perform to create and enable a CMK vary based on your cloud provider. For specific instructions, see the following H2L articles:

- [Enable Customer Managed Keys for your Organization on Amazon Web Services](#)
- [Enable Customer Managed Keys for your Organization on Microsoft Azure](#)
- [Enable Customer Managed Keys for your Organization on Google Cloud](#)

In general, you perform the following steps:

1. In your cloud KMS, provision the key and enable cross-account access with Informatica Intelligent Cloud Services.

2. In Administrator, open the **Security** tab on the **Settings** page, enable the **Enable Customer Managed Keys** option, and enter the key properties.

   Note: To perform this step, you must log in to Informatica Intelligent Cloud Services with a user account that has both the Admin and Key Admin roles.

   You can test the key after you configure the key properties. It can take up to 24 hours for the key to become active.

After you create and enable a CMK, you can revoke it at any time by disabling the **Enable Customer Managed Keys** option on the **Security** tab. When you do this, you'll go back to using Informatica's master key.

Frequently asked questions about customer managed keys

I can't see the **Security** tab on the **Settings** page even though my organization has the appropriate license. Why not?

Log in to Informatica Intelligent Cloud Services with a user account that has both the Admin and Key Admin roles. If you don't have both roles, you can't see the **Security** tab.

For more information about user roles, see *User Administration*.

When I clicked **Test Managed Key** in on the **Settings** page, the test failed. What should I do?

If you get an error when testing the key, perform the following checks:

- In Administrator, verify that the key settings on the **Settings** page match the settings for the CMK in your cloud KMS.
- In your cloud KMS, verify that the status of the CMK is active.
- In your cloud KMS, verify that the permissions on the CMK allow Informatica cryptographic access to the key.

If you continue to encounter errors, contact Informatica Global Customer Support.

What happens if the CMK is rotated in my KMS?

You can rotate the key in your cloud KMS manually or on a schedule. Rotating a key creates a new version of the key. The old version of the key remains in your cloud KMS and is used for decryption only.

Informatica Intelligent Cloud Services detects key rotation in Azure Key Vault and Google Cloud KMS. When the CMK is rotated, Informatica Intelligent Cloud Services decrypts your organization's keys using the old CMK and then encrypts them using the new CMK.

Informatica Intelligent Cloud Services cannot detect key rotation in AWS KMS. If you use AWS KMS, you'll need to disable customer managed keys in Informatica Intelligent Cloud Services and reenable it. To do this, perform the following steps:

1. On the **Settings** page in Administrator, click the **Security** tab and note the **Key ARN** and **Role ARN**.

2. Disable the **Enable Customer Managed Keys** option.

3. Enable the **Enable Customer Managed Keys** option, reenter the key ARN and role ARN, and click the save icon.

What if I need to update the CMK in my KMS?

If you need to update the CMK, first provision a new CMK in your cloud KMS. Then update the key details on the **Settings** page in Administrator.

Note: Be sure to keep the old version of the CMK in your cloud KMS active until you update the key details in Administrator.

You can delete the old version of the CMK in your cloud KMS after you update the key details on the **Settings** page.

What if I want Informatica to manage key encryption?

If you want Informatica to manage key encryption, you can disable the **Enable Customer Managed Keys** option on the **Settings** page in Administrator:
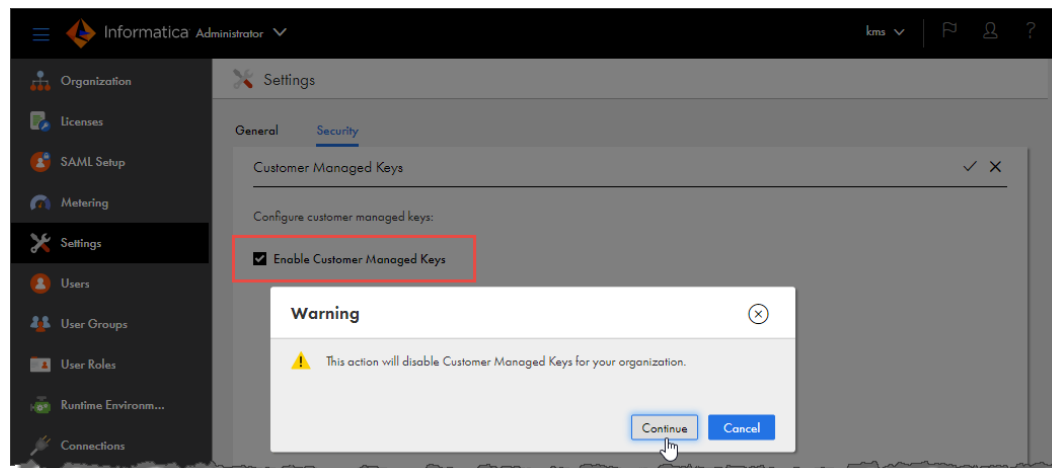
When you do this, be sure to keep the current version of the CMK in your cloud KMS active. If the CMK is not active, disabling customer managed keys fails.

When you disable this option, your organization's encryption keys are once again encrypted using encryption keys that are managed by Informatica. It can take up to 10 minutes for the Informatica encryption keys to become active.

You can disable or delete the CMK in your cloud KMS after you disable the **Enable Customer Managed Keys** option in Administrator.

What if I want to temporarily revoke Informatica's access to the CMK?

If you want to temporarily revoke Informatica's access to the CMK, you can disable the key in your cloud KMS.

When you disable the CMK, Informatica Intelligent Cloud Services can no longer unencrypt your organization's encrypted data, and any jobs that use the data will fail until you reactivate the CMK in your cloud KMS.

How do I replace the CMK if I suspect it has been compromised?

If you want to replace the CMK, you can delete the key in your cloud KMS and create a new one.

Warning: Deleting the CMK in your cloud KMS results in permanent loss to any encrypted data in Informatica Intelligent Cloud Services and causes the jobs that use the data to fail.

If you need to replace the CMK, perform the following steps so that you don't lose access to the encrypted data and jobs don't fail:

1. In Administrator, open the **Settings** page, click the **Security** tab, and disable the **Enable Customer Managed Keys** option.
2. In your cloud KMS, delete the CMK.
3. In your cloud KMS, create a new CMK.
4. On the **Settings** page in Administrator, re-enable the **Enable Customer Managed Keys** option and enter the details for the new CMK.

Can I delete the CMK if I don't want Informatica to access any of my encrypted data?

Warning: Deleting the CMK in your cloud KMS results in permanent loss to any encrypted data in Informatica Intelligent Cloud Services and causes the jobs that use the data to fail.

If you're sure that you want Informatica to forgo all access to your encrypted data in Informatica Intelligent Cloud Services, you can delete the CMK in your cloud KMS.

Secrets manager configuration

You can configure your organization to retrieve sensitive connection credentials from an external secrets manager instead of storing the credentials in the Informatica Intelligent Cloud Services repository. A secrets manager is also called a secret vault or a key vault.

Using a secrets manager offers the following benefits:

- You retain complete control of your sensitive connection credentials like passwords, OAuth tokens, and API shared secrets.
- You can manage secrets across multiple environments instead of on a per-application basis.
- You can rotate secrets on your schedule without affecting your connections, mappings, or tasks in Informatica Intelligent Cloud Services.

When you enable your organization to use a secrets manager, your Secure Agents can dynamically access sensitive connection credentials from the secrets manager. You can configure one secrets manager for each organization or sub-organization.

You can use one of the following secrets managers:

- AWS Secrets Manager
- Azure Key Vault
- HashiCorp Vault (HCP cloud-hosted)

If you use AWS Secrets Manager, the Secure Agent can access it using either role-based authentication or an access key.

Configure a secrets manager for your organization or sub-organization on the on the **Security** tab of the **Settings** page, as shown in the following image:
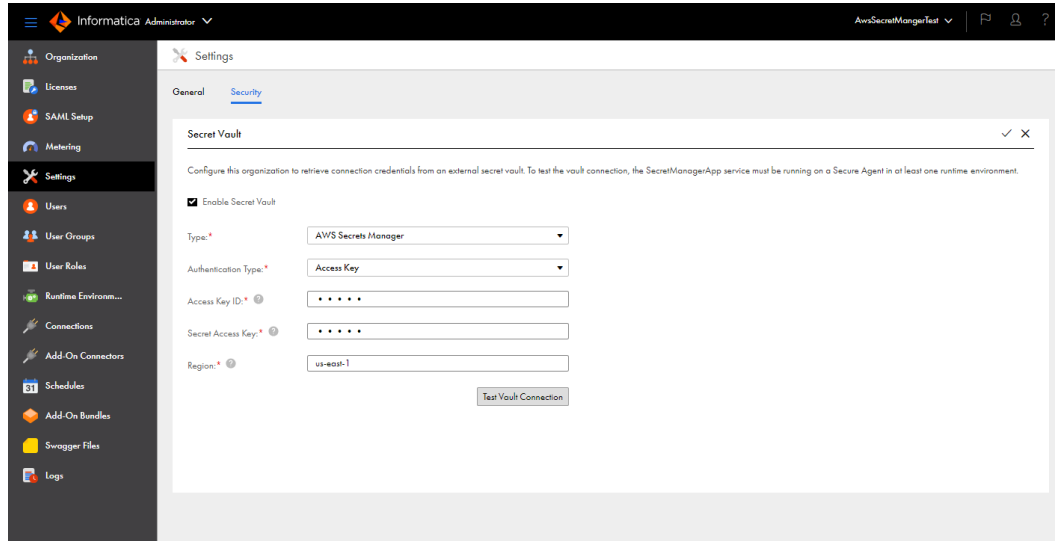
To configure your organization to use a secrets manager, you must have the Admin role or the SMS Manage Connection and SMS View Connection feature privileges as well as sufficient privileges to access the Administrator service. The organization must also be configured to store connection credentials on the cloud. You can't use a secrets manager if your organization stores connection credentials on a local Secure Agent.

After you configure a secrets manager for your organization, you can configure your connections to use the secrets manager. You can also choose which secrets to store and retrieve.

Note: If you configure a secrets manager, all connections must be created and edited in Administrator. You can't create and edit connections when you configure mappings and tasks in Data Integration.

Secret names and formats

AWS Secrets Manager and Azure Key Vault enforce restrictions on secret names. HashiCorp vault requires that secrets use a different format based on the version of the secrets engine.

The following secrets managers have restrictions on secret names or formats:

AWS Secrets Manager

In AWS Secrets Manager, secret names can contain only alphanumeric characters and the following special characters:

/ _ + = . @ - "

Azure Key Vault

In Azure Key Vault, secret names can only contain alphanumeric characters and dashes.

HashiCorp Vault

In HashiCorp Vault, secrets must be in either of the following formats based on the secrets engine version:

- Secrets engine v1: `secret/<secret_path>:<key>`

- Secrets engine v2: `secret/data/<secret_path>:<key>`

Note: Because a colon is used to separate the secret path from the key, Informatica Intelligent Cloud Services can't process keys that have a colon in the path.

For more information about restrictions on secret names and formats, see the documentation for your secrets manager.

AWS Secrets Manager connection properties

If you select AWS Secrets Manager as your secrets manager, configure connection properties such as the authentication type and region. The connection properties vary based on whether you use role-based authentication or an access key.

Note: To use role-based authentication, the Secure Agent must be installed in an EC2 instance.

Role-based authentication

Configure the following properties when you access Secrets Manager using role-based authentication:

Property	Description
Type	Secrets manager type. Choose **AWS Secrets Manager**.
Authentication Type	Authentication type that the Secure Agent should use to access Secrets Manager. For role-based authentication, choose **Role Based Access**.
IAM Role	Amazon Resource Name (ARN) of the IAM role that the Secure Agent should use to access secrets. Typically, the format is: `arn:aws:iam::<account>:role/<role-name-with-path>` The IAM role that you specify must be assigned an access policy with the GetSecretValue and ListSecrets permissions. For more information about setting up IAM roles on EC2, see the AWS documentation.
External ID	External ID required to assume the IAM role.
Region	Region code for the region where your Secrets Manager secrets are hosted, for example, `us-east-2`. Don't enter a full region name like `US East (Ohio)`.

Access key authentication

Configure the following properties when you access Secrets Manager using an access key:

Property	Description
Type	Secrets manager type. Choose **AWS Secrets Manager**.
Authentication Type	Authentication type that the Secure Agent should use to access Secrets Manager. For access key authentication, choose **Access Key**.

Property	Description
Access Key ID	AWS access key ID that the Secure Agent should use to access secrets, for example, `AKIAIOSFODNN7EXAMPLE`. The access key ID must be associated with an IAM role that is assigned an access policy with the GetSecretValue and ListSecrets permissions. You need to enter both the access key ID and the secret access key.
Secret Access Key	AWS secret access key that the Secure Agent should use to access secrets, for example `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`. You need to enter both the access key ID and the secret access key.
Region	Region code for the region where your Secrets Manager secrets are hosted, for example, `us-east-2`. Don't enter a full region name like `US East (Ohio)`.

For more information about AWS Secrets Manager properties, see the AWS documentation.

Azure Key Vault connection properties

If you select Azure Key Vault as your secrets manager, configure connection properties such as the client ID, client secret, and tenant ID.

Configure the following properties:

Property	Description
Type	Secrets manager type. Choose **Azure Key Vault**.
Client ID	Application (client) ID that the Secure Agent should use to connect to your key vault. The client ID is the unique application (client) ID assigned to your app by Azure AD when it was registered. **Tip:** You can find your application (client) ID in your Azure subscription in **Azure Active Directory** > **Enterprise applications** > **Application (client) ID**. The application (client) that you specify must have the Get and List permissions for secrets.
Client Secret	Secret string that the Secure Agent uses to prove its identity when requesting access to the key vault.
Tenant ID	Azure Active Directory (tenant) ID that should be used for authenticating requests to the key vault.
Vault URI	URI of the key vault that stores the connection credentials.

For more information about Azure Key Vault properties, see the Azure documentation.

HashiCorp Vault connection properties

If you select HashiCorp Vault as your secrets manager, configure connection properties such as the role ID, secret ID, and Vault URI.

Configure the following properties:

Property	Description
Type	Secrets manager type. Choose **HashiCorp Vault**.
Role ID	ID of the AppRole that the Secure Agent should use to authenticate with Vault. The AppRole must have the read and list permissions for secrets.
Secret ID	Secret ID of the AppRole that the Secure Agent should use to authenticate with Vault.
Vault URI	URI of the key vault that stores the connection credentials, for example: `https://my-hashicorp-vault-12343a56.a1b2345c.z1.hashicorp.cloud:8200`
Namespace	Namespace within the key vault, if used.

For more information about HashiCorp Vault properties, see the HashiCorp documentation.

Enabling and disabling a secrets manager

Enable and disable the use of a secrets manager on the **Security** tab of the **Settings** page.

1. On the **Settings** page, open the **Security** tab.
2. Click the edit (pencil) icon.
3. Select **Enable Secret Vault**, as shown in the following image:
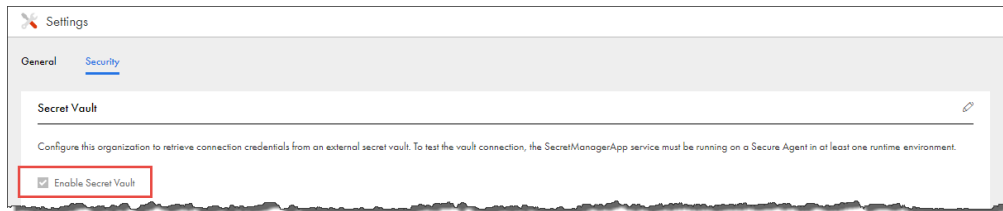
4. Select the secrets manager that you use, either AWS Secrets Manager or Azure Key Vault.
5. Enter the connection details such as the vault URI, authentication type, and region.
6. Test the connection.

   When you test the connection, you need to select a runtime environment. The runtime environment you select must contain a local Secure Agent that runs the SecretManagerApp service. The Hosted Agent, serverless agents, and cloud-hosted agents can't connect to an external secrets manager.

When the connection is successful, you can configure connections to use the secrets manager.

To disable the use of a secrets manager, clear the **Enable Secret Vault** option. However, you'll first need to disable the **Use Secret Vault** option in all connections.

Configuring a connection to use the secrets manager

You can configure any connection that has sensitive credentials to retrieve these credentials from the secrets manager.

Note: If you use a secrets manager, you need to create or edit connections in Administrator. You can't create and edit connections when you configure mappings and tasks in Data Integration.

1. Open the **Connections** page.

2. Perform either of the following actions:

   - To create a connection, click **New Connection** and enter the connection details.

   - To edit a connection, click the connection name, and then click **Edit**.

3. In the Connection Properties area, select **Use Secret Vault**.

4. Enable the checkbox next to each property that you store in the secrets manager, and then enter the secret name in the corresponding field.

   Enter the secret name in the following format:

   - AWS Secrets Manager: `<secret name>:<secret key>`

   - Azure Key Vault: `<secret name>`

   For example, you configure a relational connection and you store the database password in AWS Secrets Manager. The secret name is MySQLServerCredentials, and the secret key is MyPassword. Select **Use Secret Vault**, enable the checkbox next to the **Password** field, and enter `MySQLServerCredentials:MyPassword` in the **Password** field, as shown in the following image:

5. Select the runtime environment to be used with the connection.

   The runtime environment you select for the connection must contain a local Secure Agent that runs the SecretManagerApp service. The Hosted Agent, serverless agents, and cloud-hosted agents can't connect to an external secrets manager.

6. Configure the connection-specific properties.

7. To test the connection, click **Test Connection**.

8. Click **Save**.

For more information about configuring connections, see *Connections*.

CHAPTER 5

Permissions

Permissions determine the access rights that a user has for a Secure Agent, Secure Agent group, connection, schedule, or asset. Permissions add additional or custom security for an object. Permissions define which users and groups can read, update, delete, execute, and change permissions on the object.

To configure permissions on an object, you need the following licenses and privileges:

- To configure permissions at the project level for all assets in a project, your organization must have the Set/Unset Security Permissions at Project Level license.

- To configure permissions at the folder level for all assets in a folder, your organization must have the Set/Unset Security Permissions at Folder Level license.

- To configure permissions on individual assets, your organization must have the Fine Grained Security license.

- The role assigned to your user account or to a group in which you are a member must have the Set Permission privilege for the object type. For example, to configure permissions on a Secure Agent, you must be assigned a role that has the Set Permission privilege for Secure Agents.

To configure permissions on an object, navigate to the object and set the appropriate permissions. For example, you want only users in the Development Team user group to have access to assets in the Development Data folder. Navigate to the folder, edit the permissions, and grant the Development Team user group permissions on the folder.

Permissions apply to the objects that you configure but not to copies of the object. Therefore, when you copy or export an asset, the permissions are not copied or exported with the asset. For example, you export a mapping task in which only user rjones has execute permission. When you import the mapping task, the imported mapping has no permissions assigned to it. Therefore, any user with privileges to run mapping tasks can run the imported task.

You can configure the following permissions on an object:

Permission	Description
Read	Open and view the object.
	If the object is source controlled, this permission allows the user or group to pull or check out the object from the source control repository. You must have the read permission to access the integration hub connection to perform any operations.
	If you select a task, this permission also allows the user or group to use a connection or schedule in the task.
Update	Edit the object.
	If the object is source controlled, this permission allows the user or group to check in, check out, pull, unlink, or roll back the object.
	Requires read permission, which is automatically granted.

Permission	Description
Delete	Delete the object.
Execute	Run the object. Applies to mappings, tasks, taskflows, and Cloud Integration Hub assets. Monitor, stop, and restart instances of the mapping, task, or taskflow.
Change permissions	Change the permissions that are assigned to the object.

Note: These permissions control permissions within Informatica Intelligent Cloud Services. They do not control operating system permissions, such as the ability to start, stop, or configure the Secure Agent on Windows or Linux.

Rules and guidelines for permissions

Use the following rules and guidelines for permissions:

- When you configure permissions on an object, verify that the user or group to which you grant permissions is assigned a role with the appropriate privileges for the object type.
- For example, if you grant a user with the Service Consumer role Update privilege on a particular folder, the user cannot update the folder because the Service Consumer role does not have update privileges for folders.
- To edit an asset, the user must have read permission on all assets used within the asset. For example, when you assign a user Read and Update permissions on a synchronization task, verify that the user also has Read permission on the connections, mapplets, schedules, and saved queries that are used in the task.
- To run a subscription or a publication that executes a mapping task, the user must have the Update privilege for the project and folder that contains the mapping task.
- When a user edits a task, assets without Read permission are not displayed. To avoid unexpected results, the user should cancel all changes and avoid editing the task until the user is granted the appropriate Read permissions.
- When configuring a taskflow, a user needs Execute permission on all tasks to be added to the taskflow.
- To edit a taskflow, a user needs Execute permission on all tasks in the taskflow. Without Execute permission on all tasks, the user cannot save changes to the taskflow.
- To run a taskflow, a user needs Read and Execute permissions on taskflows.
- To monitor jobs or to stop a running job, a user needs Execute permission on the mapping, task, or taskflow.
- If you assign custom permissions to a Data Integration task and invoke the Data Integration task through an Application Integration process or a guide, you must complete either of the following tasks:
  - Give the Application Integration anonymous user permission to run the associated Data Integration asset.
  - Add the Application Integration anonymous user to a user group that has permission to run the associated Data Integration asset.

Configuring permissions

You can configure permissions on an object if you are assigned a role with the Set Permission privilege for the object type. For example, to configure permissions on a folder, you must be assigned a role that has the Set Permission privilege for folders.

1. Navigate to the object for which you want to configure permissions.

    For example:

    - To configure permissions on a Secure Agent or Secure Agent group, in Administrator, select **Runtime Environments**.

      - To configure permissions on a connection, in Administrator, select **Connections**.

      - To configure permissions on a mapping, in Data Integration, open the project and folder that contain the mapping.

2. In the row that contains the object, either click **Actions** and select **Permissions**, or click the **Change Permission** icon.

    The **Permissions** dialog box lists the users and groups that have permissions on the object.

    If the **Permissions** dialog box lists no users or groups, then no permissions are configured for the object. Any user with appropriate privileges for the object type can access the object.

    The following image shows the **Permissions** dialog box for a mapping:

3. To configure user permissions on the object:

    a. Select **Users**.

    b. If the user does not appear in the **Users** list, click **Add**, and select a user.

    c. Enable or disable the appropriate permissions on the user.

    Note: When you grant any user permissions on the object, Informatica Intelligent Cloud Services also adds you as a user with permissions on the object. This prevents you from losing access to the object when you configure permissions.

4. To configure user group permissions on the object:

    a. Select **Groups**.

b.	If the group does not appear in the **Groups** list, click **Add**, and select a group.

c.	Enable or disable the appropriate permissions on the group.

Note: When you grant any group permissions on the object, Informatica Intelligent Cloud Services also adds you as a user with permissions on the object. This prevents you from losing access to the object when you configure permissions.

5.	To remove all permissions restrictions for the object, remove all users and groups from the **Permissions** dialog box.

When you remove all users and groups, any user with appropriate privileges for the object type can access the object.

6.	Click **Save**.

CHAPTER 6

Schedules

You can create schedules to run tasks or taskflows at specified times or at regular intervals. You can also define a blackout period during which scheduled tasks or jobs don't run.

You must have the Schedule privilege in the Administrator asset privileges to create, read, update, delete, or set permissions on project schedules. Create schedules and configure blackout periods on the **Schedules** page in Administrator. After you create a schedule, you can associate it with tasks and taskflows in another service such as Data Integration.

When you create a schedule, you specify the date and time. You can configure a schedule to run associated assets throughout the day between 12:00 a.m. and 11:55 p.m. Informatica Intelligent Cloud Services might add a small schedule offset to the start time, end time, and all other time configurations. As a result, scheduled tasks and taskflows might start later than expected. For example, you configure a schedule to run hourly until noon, and the schedule offset for your organization is 10 seconds. Informatica Intelligent Cloud Services extends the end time for the schedule to 12:00:10 p.m., and the last hourly task or taskflow starts at 12:00:10 p.m. To see the schedule offset for your organization, check the **Schedule Offset** organization property for the Data Integration Service.

You can perform the following tasks with schedules:

Associate a schedule with a task or taskflow

To associate a schedule with a task or taskflow, edit the task or taskflow. For example, to associate a schedule with a mapping task, edit the mapping task in Data Integration, and select the schedule on the **Schedules** page.

When you copy a task or taskflow that includes a schedule, the schedule is not associated with the new asset. To associate a schedule with the new asset, edit the asset.

Monitor scheduled tasks

You can monitor scheduled tasks from the **All Jobs** page in Monitor. Scheduled tasks do not appear on the **My Jobs** page.

Export a schedule

You can export a schedule from your organization and import it into another organization. Export a schedule on the **Schedules** page. If the schedule is associated with a task or taskflow, the task or taskflow is not included in the export file.

Delete a schedule

Delete a schedule on the **Schedules** page in Administrator.

Note: You cannot delete a schedule that is used in a task or taskflow. Remove the schedule from all tasks and taskflows before you delete the schedule.

Configuring a blackout period

A blackout period prevents all scheduled tasks and taskflows in the organization from running during a specified period of time. You can configure a blackout period during which the scheduled Data Integration and Data Ingestion and Replication file publications and file subscriptions don't run. You can also configure one blackout period for an organization.

If a task is scheduled to run during a blackout period, the task instance will not be started during the blackout period, and it will not restart automatically when the blackout period ends. After the blackout period, task instances will resume according to the schedule. If a task is already running when a blackout period starts, it will not be stopped.

To configure a blackout period, in Administrator, select **Schedules**, and then click **Blackout Period**. The blackout period is displayed on the **Schedules** page.

Repeat frequency

The repeat frequency determines how often tasks run. You can set the repeat frequency to every N minutes, hourly, daily, weekly, biweekly, or monthly.

The following table describes the repeat frequency options:

Option	Description
Does not repeat	Tasks run as scheduled and do not repeat.
Every N minutes	Tasks run on an interval based on a specified number of minutes. You can configure the following options: - Repeat frequency. Select a frequency in minutes. Options are 5, 10, 15, 20, 30, 45. - Days. Days of the week when you want tasks to run. You can select one or more days of the week. - Time range. Hours of the day when you want tasks to start. Select All Day or configure a time range. You can configure a time range between 00:00-23:55. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time.
Hourly	Tasks run on an hourly interval based on the start time of the schedule. You can configure the following options: - Repeat frequency. Select a frequency in hours. Options are 1, 2, 3, 4, 6, 8, 12. - Days. Days of the week when you want tasks to run. You can select one or more days of the week. - Time range. Hours of the day when you want tasks to start. Select All Day or configure a time range. You can configure a time range between 00:00-23:55. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time.
Daily	Tasks run daily at the start time configured for the schedule. You can configure the following options: - Repeat frequency. The frequency at which you want tasks to run. Select Every Day or Every Weekday. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time.

Option	Description
Weekly	Tasks run on a weekly interval based on the start time of the schedule. You can configure the following options: - Days. Days of the week when you want tasks to run. You can select one or more days of the week. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time. If you do not specify a day, the schedule runs regularly on the same day of the week as the start date.
Biweekly	Tasks run every two weeks based on the start time of the schedule. You can configure the following options: - Days. Days of the week when you want tasks to run. You can select one or more days of the week. You must select at least one day. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time. If you configure a biweekly schedule to start at 5 p.m. on a Tuesday and run tasks every two weeks on Mondays, the schedule begins running tasks on the following Monday.
Monthly	Tasks run on a monthly interval based on the start time of the schedule. You can configure the following options: - Day. Day of the month when you want tasks to run. You can configure one of the following options: - Select the exact date of the month, between 1-28. If you want the task to run on days later in the month, use the <n> <day of the week> option. - Select the <n> <day of the week>. Options for <n> include First, Second, Third, Fourth, and Last. Options for <day of the week> includes Day, and Sunday-Saturday. Tip: With the Day option, you can configure tasks to run on the First Day or the Last Day of the month. - Repeat option. The range of days when you want tasks to run. You can select Repeat Indefinitely or configure an end date and time.

Time zones and schedules

Informatica Intelligent Cloud Services stores time in Coordinated Universal Time (UTC). When you log in, Informatica Intelligent Cloud Services converts the time and displays it in the time zone associated with your user profile.

When you create a schedule, you select the time zone for the scheduler to use. You can select a time zone that is different from your time zone or your organization time zone.

Daylight Savings Time changes and schedules

Informatica Intelligent Cloud Services applies Daylight Savings Time changes to all tasks except biweekly tasks.

When Daylight Savings time goes into effect, tasks scheduled to run between 2:00 a.m. and 2:59 a.m., do not run the day that the time changes from 2:00 a.m. to 3:00 a.m. If a task is scheduled to run biweekly at 2 a.m., it will run at 3 a.m. the day of the time change and at 2 a.m. for the next run.

Daylight Savings Time does not trigger additional runs for tasks that are scheduled to run between 1:00 a.m. - 1:59 a.m. when Standard Time begins. For example, a task is scheduled to run every day at 1:30 a.m. When the time changes from 2 a.m. to 1 a.m., the task does not run again at 1:30 a.m.

Tip: To ensure that Informatica Intelligent Cloud Services does not skip any scheduled runs near the 2 a.m. time change, do not schedule jobs to run between 12:59 a.m. and 3:01 a.m.

Configuring a schedule

Configure a schedule on the **Schedules** page. For mapping tasks and synchronization tasks, you can also create a new schedule when you configure the task. You can configure a schedule to run once or at a specific interval and to run indefinitely or until a specified end time.

1. In Administrator, select **Schedules**.
2. To create a schedule, click **New Schedule**.

   To edit a schedule, click the edit icon in the row that contains the schedule.
3. Configure the following properties:

Property	Description
Schedule Name	Name of the schedule. Each schedule name must be unique within the organization. Schedule names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Maximum length is 255 characters. Names are not case sensitive.
Description	Description of the schedule. Maximum length is 255 characters.
Starts	Date and time when the schedule starts. The date format is MM/DD/YYYY. Time appears in the 24-hour format. Click the calendar button to select the start date. The start date and time can affect the repeat frequency for tasks and taskflow jobs that repeat at regular intervals. For example, if the start date is November 10 and the repeat frequency is monthly, the schedule runs associated assets on the tenth day of each month. If the start time is 3:10 and the repeat frequency is hourly, the assets run every hour at 10 minutes past the hour. Default is the current date, current time, and time zone of the user who creates the schedule.
Time Zone	Select the time zone for the schedule to use. The time zone can differ from the organization time zone or user time zone.
Repeats	Repeat frequency for the schedule. Select one of the following options: - Does Not Repeat - Every N Minutes - Hourly - Daily - Weekly - Biweekly - Monthly Default is Does Not Repeat.

4. Click **Save**.

Exporting schedules

You can export schedules from your organization and import them into other organizations. Assets that are associated with the schedules are not included in the export file. Export schedules on the **Schedules** page.

1. In Administrator, select **Schedules**.

2. Click **Export**.

3. In the **Export Schedules** dialog box, select the schedules that you want to export.

4. Optionally, update the export job name.

   By default, the job name is `SchedulesExport_<date>`.

5. Click **Export**.

   Administrator creates an export job to export the schedule.

6. To check the status of the export job and download the export file, open the **Import/Export Logs** page in Monitor, and click the **Export** tab.

   You can download the export file in the row that contains the export job or on the job details page.

You can import schedules on the **Explore** page in another service such as Data Integration. For information about importing assets, see the help for that service.

After you import schedules, you can associate them with assets in the target organization.

Troubleshooting scheduled tasks

The task does not run at the scheduled time.

A task does not run at the scheduled time if another instance of it is already running when the schedule tries to start the task. For example, you schedule a task to run every 5 minutes. The first task starts at 12 p.m., but does not complete until 12:06 p.m. The second instance of the task does not run at 12:05 p.m. because the first instance has not completed. Data Integration starts the next task at 12:10 p.m.

To resolve this issue, change the schedule to allow the task to complete before starting the next task run.

CHAPTER 7

Bundle management

A bundle is a set of related mappings, mapping tasks, mapplets, and Visio templates that Data Integration users can use in data integration projects. Data Integration users design, create, and publish bundles. Administrators manage bundles.

If you are the administrator for an organization, you can perform the following actions to manage bundles:

Install a bundle.

You can install a public, private, or unlisted bundle that the bundle designer has configured to be used as a reference. When you install a bundle, the bundle is installed into the Add-On Bundles project in Data Integration. Users in your organization can use the assets in the bundle, but they cannot edit the assets.

Copy a bundle.

You can copy a public, private, or unlisted bundle that the bundle designer has configured for copying. When you copy a bundle, you select the Data Integration folder where you want to copy the bundle contents. You can copy a bundle multiple times and save the contents into a different project or folder each time that you copy it. After you copy a bundle, users in your organization can edit the assets.

Upgrade a bundle.

If you installed a bundle and a newer version of the bundle is available, you can upgrade the bundle to get the latest version.

Uninstall a bundle.

If your organization no longer needs an installed bundle, you can uninstall it.

To view the bundles that are installed or are available to your organization, in Administrator, select **Add-On Bundles**. The **Add-on Bundles** page displays information about installed bundles, copied bundles, and bundles that are available for installation or copying.

For information about bundle types, creating bundles, or publishing bundles, see *Mappings* in the Data Integration service help.

Types of bundles

You specify a bundle type when you create a bundle. The bundle type determines who can use the bundle and it also determines how the bundle is published.

You can create the following types of bundles:

Public bundles

A public bundle is available to all organizations and sub-organizations. When you create a public bundle, you submit the bundle to Informatica for approval. When the bundle is approved, Informatica makes the bundle available to all organizations.

Private bundles

A private bundle is available only to a parent organization and its sub-organizations. You create a private bundle in the parent organization and then publish the bundle to the sub-organizations. Published private bundles appear on the Add-On Bundles page for sub-organizations. Informatica does not review private bundles.

If a pushed bundle contains objects with changes that aren't compatible with existing sub-organization tasks, it might cause the sub-organization tasks to become invalid or be removed.

You can't create private bundles if the organization doesn't have any sub-organizations.

Unlisted bundles

An unlisted bundle is one where the bundle designer has configured to be used as a reference. Installing an unlisted bundle requires an access code.

Installing a bundle

You can install a public, private, or unlisted bundle that the bundle designer has configured to be used as a reference. Install a bundle on the Available Bundles tab of the **Add-On Bundles** page.

Before you install an unlisted bundle, get the bundle access code. To get the access code for a bundle that was created in your organization, open the **Bundles** page in Data Integration, click the bundle name, and then click **Copy Access Code**. To get the bundle access code for a bundle that was created outside of your organization, contact the bundle publisher.

1. In Administrator, select **Add-On Bundles**.

2. Click **Available Bundles**.

   The Available Bundles tab lists the public and private bundles that are available for installation or copying.

3. If the bundle that you want to install is an unlisted bundle, enter the bundle access code in the **Find** field.

4. Click the bundle name to open the Bundle Details page.

5. Verify that the **Allow** field is set to **Reference** or to **Reference and Copy**.

   You cannot install a bundle that is configured for copying only.

6. Click **Install**.

In Data Integration, the bundle is added to the Add-On Bundles project, and the assets are ready for use. The bundle is also listed on the **Installed Bundles** tab of the **Add-On Bundles** page in Administrator.

Copying a bundle

You can copy a public, private, or unlisted bundle that the bundle designer has configured for copying. Copy a bundle on the Available Bundles tab of the **Add-On Bundles** page. Each time you copy a bundle, an event is logged on the Copied Bundles tab.

Before you copy an unlisted bundle, get the bundle access code. To get the access code for a bundle that was created in your organization, open the **Bundles** page in Data Integration, click the bundle name, and then click **Copy Access Code**. To get the bundle access code for a bundle that was created outside of your organization, contact the bundle publisher.

1. In Administrator, select **Add-On Bundles**.
2. Click **Available Bundles**.

   The Available Bundles tab lists the public and private bundles that are available for installation or copying.
3. If the bundle that you want to copy is an unlisted bundle, enter the bundle access code in the **Find** field.
4. Click the bundle name to open the Bundle Details page.
5. Verify that the **Allow** field is set to **Copy** or to **Reference and Copy**.

   You cannot copy a bundle that is configured to be used as a reference only.
6. Click **Copy Bundle Content to…**.
7. In the **Browse** dialog box, select the Data Integration project or folder into which you want to copy the bundle contents.
8. Click **Select**.

   The assets in the bundle are copied to the selected project or folder.

Upgrading a bundle

You can upgrade an installed bundle when an updated version becomes available. You can check the bundle status on the Installed Bundles tab of the **Add-On Bundles** page.

1. In Administrator, select **Add-On Bundles**.
2. Click **Installed Bundles**.

   The Bundle Status column indicates whether the bundle is up-to-date or whether an upgrade is available.
3. Click the bundle name to open the Bundle Details page.
4. Click **Upgrade**.

Uninstalling a bundle

Uninstall a bundle if users in your organization no longer need it. Uninstall the bundle on the Installed Bundles tab of the **Add-On Bundles** page.

Note: Uninstalling a bundle removes all of the bundle assets from the organization. If you want to keep tasks that use assets in the bundle, remove the assets from the task before you uninstall the bundle.

1. In Administrator, select **Add-On Bundles**.
2. Click **Installed Bundles**.
3. Click the bundle name to open the Bundle Details page.
4. Click **Uninstall**.

After you uninstall the bundle, it is listed on the Available Bundles tab.

CHAPTER 8

Event monitoring

You can monitor events for the assets, licenses, users, and Secure Agents in your organization through the asset and security logs. To view the logs, you must be assigned a role that has the Audit Log - View privilege.

You can monitor events through the following logs:

Asset log

Displays the following information:

- Events for assets such as when an asset was created, updated, copied, or deleted and the name of the user who modified the asset.

- Events related to licenses such as when a license was added, removed, or changed.

To open the asset log, in Administrator, select **Logs**, and then select **Asset Logs** at the top of the page.
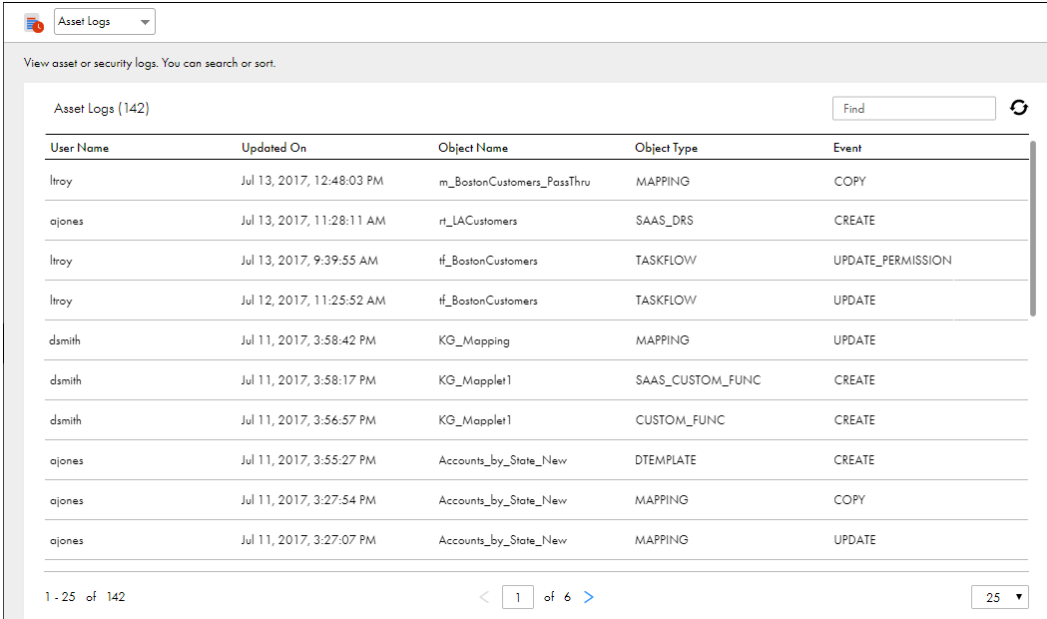
Security log

Displays the following information:

- Authentication events for users such as when a user in the organization logged in to or out of Informatica Intelligent Cloud Services.

- Events for Secure Agents and organizations such as when each agent was created or updated, when organization information was updated, and the name of the user who modified the agent or organization.

To open the security log, in Administrator, select **Logs**, and then select **Security Logs** at the top of the page.

The following image shows the asset log:

Asset logs display events for the past 90 days. Security logs display events for the past 400 days.

You can customize the properties that are displayed in the logs in the following ways:

- To hide a column, right-click the column heading area and uncheck the column that you want to hide.

- To sort the log events, click the column heading for the property that you want to sort by. To reverse the sort order, click the column heading again.

- To search the logs for specific events, enter the search string in the **Find** field. You can search for an object name or event type.

CHAPTER 9

Troubleshooting security

I received the following security violation error:

```
There may have been a security violation while accessing the site. Verify that there are
no malicious scripts running in your browser. This error also appears when you submit
the form multiple times through a browser reload.
```

This error appears when you click an option on a page while the page is still loading from a previous click. Click the Here link to return to Data Integration.

When I try to view the details about an object, such as a connection or replication task, the Object Not Found page displays.

The object was recently deleted. The Object Not Found page appears when an object no longer exists. Refresh the page to display current objects.

When I try to perform a task, the Access Denied page displays.

The Access Denied page displays when you try to perform a task that is not allowed for your user account. You might not have the appropriate role or asset permissions to perform the task. If you need to perform the task, ask your organization administrator to review your user account.

CHAPTER 10

Licenses

Licenses determine the Informatica Intelligent Cloud Services subscription level for the organization and provide access to Informatica Intelligent Cloud Services features, connectors, and bundles.

As an administrator, you can review the licenses that are set up for your organization, verify license expiration dates, and manage sub-organization licenses.

You can also review metrics for licensed job limits and usage. For information about reviewing metrics, see .

License categories

Licenses are categorized as edition licenses, connector licenses, and custom licenses.

The following license categories are available:

Edition licenses

Edition licenses can be feature-based or usage-based. Feature-based edition licenses provide access to Informatica Intelligent Cloud Services features such as Data Integration mapping tasks, business services components, and fine-grained security. Usage-based edition licenses, such as the license for the Intelligent Cloud Data Management feature, provide access to Informatica Intelligent Cloud Services using a pre-paid consumption model.

Connector licenses

Connector licenses provide connectivity to entities such as Amazon Redshift, Microsoft SQL Server, and Oracle.

Custom licenses

Custom licenses are licenses that are not part of an edition. They provide access to features, packages, or bundles. If your organization uses a custom license that provides access to a feature that is also included in an edition license, the terms of the custom license override the terms of the edition license.

License types

When you create an organization, Informatica Intelligent Cloud Services assigns the organization a license type for each licensed edition.

Informatica Intelligent Cloud Services uses the following types of licenses:

Trial

You can use the edition free of charge for a 30-day period. At the end of the trial period, you can subscribe to the edition. A trial subscription might provide limited access to the features, connectors, and packages that are associated with the license.

Subscription

You can use the licensed edition for the duration of the contract period. Near the end of the contract period, Informatica Intelligent Cloud Services indicates that the contract is about to expire. Renew the contract to continue to use the edition.

Free subscription

You can use the synchronization task free of charge. A free subscription might provide limited access to the features of the synchronization task.

Sub-organization licenses

A sub-organization has licenses that are maintained by the parent organization. If a sub-organization requires a license that does not belong to the parent organization, contact Informatica Global Customer Support to obtain the license for the parent organization.

When you create a sub-organization, each sub-organization inherits licenses from the parent organization as custom licenses. The sub-organization inherits all licenses except for the following licenses:

- The license to create sub-organizations
- Bundle licenses. To use a bundle in the sub-organization, a user in the sub-organization must install the bundle.

If your organization has the Intelligent Cloud Data Management license, the sub-organization also has this license. The parent organization and the sub-organization share the balance of Informatica processing units (IPUs).

You can manage sub-organization licenses in the following ways:

Manage the licenses individually

When you manage licenses individually, administrators for the parent organization can disable, enable, and shorten the expiration dates for the inherited licenses. They manage the licenses separately for each sub-organization. Sub-organization administrators can view licenses but cannot change them.

This is the default option.

Automatically synchronize sub-organization licenses with the parent organization

If you have the appropriate license, you can automatically synchronize sub-organization licenses with the parent organization. When this license is enabled, each time a license is changed in the parent organization, all sub-organizations inherit the license change.

You might want to enable license synchronization when your organization has many sub-organizations and the sub-organizations have the same licenses.

If license synchronization is not enabled for your organization, then you must manage sub-organization licenses individually.

Note: If you link a sub-organization that has a license that the parent organization does not have, the sub-organization loses the license.

Editing sub-organization licenses

You can edit sub-organization licenses if you are an administrator in the parent organization and if license synchronization between the parent organization and sub-organizations is not enabled. You can edit sub-organization licenses from within the parent organization or from within the sub-organization.

1. Log in to the parent organization.
2. To edit licenses from within the parent organization:
    a. Open Administrator and select **Organization**.
    b. Click **Sub-Organizations**.
    c. Select the sub-organization for which you want to edit licenses.
    d. Click **Licenses**.
3. To edit licenses from within the sub-organization:
    a. From the **Organization** menu in the upper right corner, select the sub-organization for which you want to edit licenses.
    b. Open Administrator and select **Licenses**.
4. Select licenses to enable features, and clear licenses to disable features.
5. Optionally, modify expiration dates.

    All licenses must have expiration dates. You cannot extend a license past its original expiration date.
6. Click **Save**.

Synchronizing licenses with the parent organization

You can automatically synchronize sub-organization licenses with the parent organization. Each time a license is changed in the parent organization, all sub-organizations inherit the license change.

To enable license synchronization, contact Informatica Global Customer Support and request the license for this feature. When the license is enabled for the parent organization, license synchronization with the sub-organizations happens automatically. The parent organization administrator does not have to take any action to synchronize the licenses.

Note: When the license for this feature is enabled, you cannot edit sub-organization licenses individually.

When the license for this feature is enabled and you disable a sub-organization, the sub-organization loses its license settings. When you re-enable the sub-organization, the sub-organization inherits all license settings from the parent organization.

License synchronization between a parent organization and sub-organizations does not affect the license meter counts in the sub-organizations.

Configuring the organization type

When you view the **Licenses** page, you can view details about the organization licenses and other details, including the organization type. The organization type specifies whether the organization is a trial, production, or sandbox organization. If you are a parent organization administrator, you must configure the organization type for each sub-organization.

The organization type is editable when a parent organization administrator views the **Licenses** page for a sub-organization. It is not editable by sub-organization users or in a parent organization.

If you are a parent organization administrator, you can configure the organization type for the sub-organization from within the parent organization or from within the sub-organization. You can change the organization type after you configure it.

1. Log in to the parent organization.
2. To edit the organization type from within the parent organization:
   a. Open Administrator and select **Organization**.
   b. Click **Sub-Organizations**.
   c. Select the sub-organization for which you want to configure the type.
   d. Click **Licenses**.
   e. In the **Type** list in the Sub-Organization Details area, select the organization type.
3. To edit the organization type from within the sub-organization:
   a. From the **Organization** menu in the upper right corner, select the sub-organization for which you want to configure the type.
   b. Open Administrator and select **Licenses**.
   c. In the **Type** list in the Sub-Organization Details area, select the organization type.
4. Click **Save**.

License expiration

When a license expires, you cannot access the features, connectors, or packages that are associated with the license. Scheduled jobs that are associated with the license are also disabled. If all licenses for the organization expire, you cannot log in to Informatica Intelligent Cloud Services.

You can review the expiration date for licenses on the **Licenses** page in Administrator. To extend a license, contact Informatica Global Customer Support. After you extend a license, you can access the associated features, connectors, and packages, and the scheduled jobs resume processing.

INDEX