Benefits of Grouping Multiple Agents

When you create a Secure Agent, it is added to its own group by default. You can add multiple agents to one Secure Agent group. All agents within a group must be of the same type, for example, all agents that run within your network or all agents that run on Amazon EC2 machines.

Add multiple agents to a group to achieve the following benefits:

Balance the workload across machines.
Add multiple agents to a group to balance the distribution of tasks across machines. When the runtime environment is a Secure Agent group with multiple agents, the group dispatches a task or a background process such as metadata call to an agent with the fewest number of tasks running or queued.

Improve scalability for connections and tasks.
When you create a connection or task, you select the runtime environment to use. If the runtime environment is a Secure Agent group with multiple agents, the tasks can run if any Secure Agent in the group is up and running. You do not need to change connection or task properties when you add or remove an agent or if an agent in the group stops running.

When you add multiple agents to a group, ensure that all of the Secure Agents are of the same type. For example, your organization installs four Secure Agents on physical machines within your network and two Secure Agents on Amazon EC2 machines. You can create a Secure Agent group that contains some or all of the local agents and a different group that contains the EC2 agents. Do not create a group that contains both a local agent and an EC2 agent.

If you need to access output files on the Secure Agent machine, you can view the job details to determine which Secure Agent ran the task. To view job details, open
Monitor
, select
All Jobs
, and click the job name

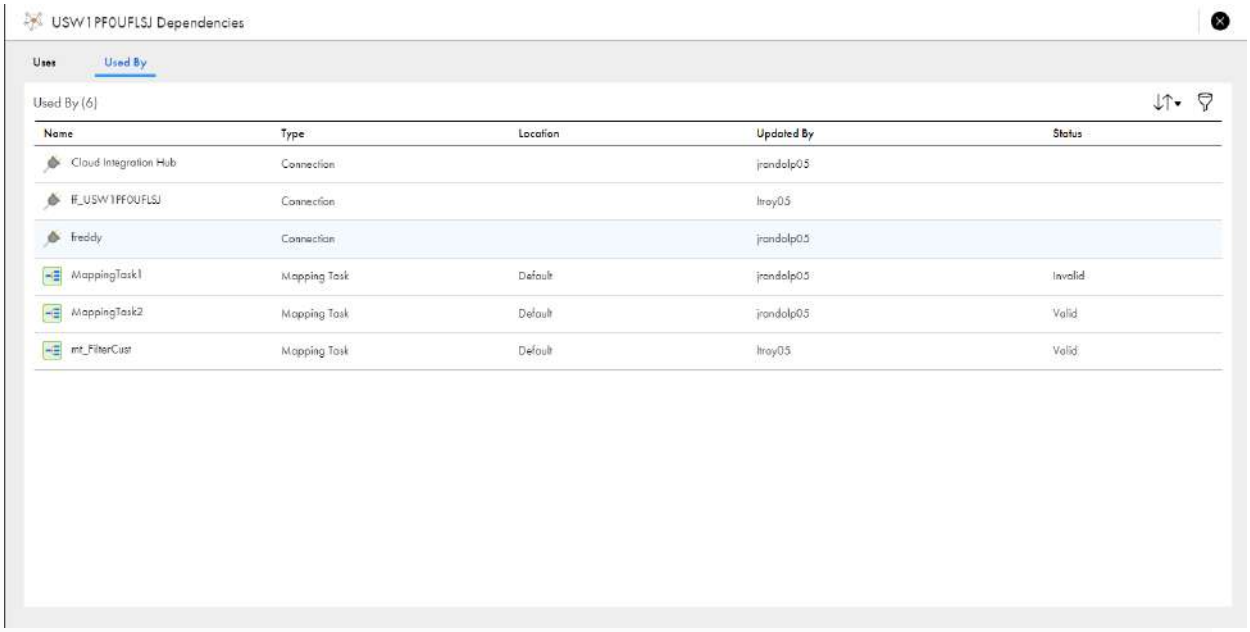
Viewing Secure Agent group dependencies

You can view object dependencies for Secure Agent groups.

When you view dependencies for a Secure Agent group,
Administrator
lists the connections and assets in each service that use the group as the runtime environment.

To view object dependencies for a Secure Agent Group, expand the Actions menu and select
Show Dependencies
.

The following image shows the
Dependencies
page for a Secure Agent group:



To sort the objects that appear on the page, click the sort icon and select the column name for the property you want to sort by.

To filter the objects that appear on the dependencies page, click the Filter icon. Use filters to find specific objects. To apply a filter, click
Add Field
, select the property to filter by, and then enter the property value. You can specify multiple filters. For example, to find connections with Oracle in the name, add the Type filter and specify Connection. Then add the Name filter and enter "Oracle."

Working with Secure Agent groups

Create Secure Agent groups on the

Runtime Environments

page.

After you create a Secure Agent group, you can rename or delete the group, add and remove Secure Agents, and change group permissions. You can also enable services and connectors for the group.

Click the refresh icon next to

New Runtime Environment

to refresh the page before performing any actions on Secure Agent groups.

You can complete the following tasks:

Create a Secure Agent group.

To create a Secure Agent group, click

New Runtime Environment

and enter a name and optionally a description for the group. After you create a group, you can add Secure Agents to the group.

If you use multi-byte characters in the Secure Agent group name and you create the group in a cloud-hosted environment, verify that the environment also supports these characters.

Edit Secure Agent group properties.

To rename a Secure Agent group or to add or update the description, expand the Actions menu, select

Edit Environment Properties

, and complete the fields in the dialog box.

Informatica Intelligent Cloud Services

updates the group name in all services that use the group.

Enable or disable specific Informatica Intelligent Cloud Services and connectors for a Secure Agent group.

To enable or disable services for a Secure Agent group, expand the Actions menu and select

Enable or Disable Services, Connectors

. On the

Services

tab, select the services to enable or disable. You can enable or disable any service that your organization uses.

Before you disable a service, verify that no connection, task, or process that uses the group as the runtime environment requires the service. If a connection, task, or process has a Secure Agent group selected as the runtime environment and you disable a required service, the task or process cannot run. Similarly, if a feature has a Secure Agent group selected as the runtime environment and you disable a required service, the feature cannot be used.

To enable or disable connectors, expand the Actions menu and select

Enable or Disable Services, Connectors

. On the

Connectors

tab, select the connectors to enable or disable. You can enable or disable any connector that you organization is licensed to use.

To enable or disable additional services such as Self-Hosted Git Repo, expand the Actions menu and select

Enable and Disable Services and Connectors.

On the

Additional Services

tab, select the services to enable or disable. You can enable or disable any service that your organization uses.

Add Secure Agents to a group.

To add Secure Agents to a group, expand the Actions menu and select

Add or Remove Secure Agents

. You can add any agent that is in the Unassigned Agents group on the

Runtime Environments

page.

Alternatively, you can add a new Secure Agent to an existing group by setting the InfaAgent.GroupName property in the infaagent.ini file before you register the agent. When you add a Secure Agent to a Secure Agent group, the Secure Agent inherits the services and connectors that are configured for the Secure Agent groups.

For

Application Ingestion and Replication

and

Database Ingestion and Replication

, if you remove a Secure Agent from a Secure Agent group and add it to another Secure Agent group, wait at least 60 minutes before trying to use it to run application or database ingestion and replication jobs. The internal cache of Secure Agent runtime information is refreshed every hour by default.

When you add more than one Secure Agent to a Secure Agent group, all agents must meet the following requirements:

- All of the agents must be of the same type, for example, all local agents or all agents that run on Amazon EC2 machines.
- Each Secure Agent must be configured to connect to the same external systems and have access to files such as libraries, initialization files, and JAR files.
- Each Secure Agent must have access to the files used in tasks. Ensure that all files used in a task are available in a shared location.

Remove Secure Agents from a group.

To remove Secure Agents from a group, expand the Actions menu and select

Add or Remove Secure Agents

. When you remove an agent from a group,

Informatica Intelligent Cloud Services

adds it to a group named "Unassigned Agents."

You can remove an agent from a Secure Agent group if the group is not used as the runtime environment for a connection or task. If the group is used, you can remove an agent if it is not the only agent in the group.

Delete a Secure Agent group.

To delete Secure Agent group, expand the Actions menu and select

Delete

. You can delete a Secure Agent group if it does not contain any Secure Agents.

If the Secure Agent group is associated with an

advanced configuration

and the

advanced cluster

is running, you must stop the cluster and associate the configuration with a different runtime environment before you can delete the group.

Share or unshare a Secure Agent group.

If you are the administrator of a parent organization, you can share a Secure Agent group so that the sub-organizations can use it. You can unshare a group if it is not used in a connection or task. From the Actions menu associated with the group, choose

Share Secure Agent Group

or

Unshare Secure Agent Group

.

Change permissions for a Secure Agent group.

To change permissions for a Secure Agent group, expand the Actions menu and select

Permissions

. You can define permissions for a Secure Agent group for each user group in your organization.

You can set the following permissions:

Permission	Description
Read	View details about the Secure Agent group and use the Secure Agent group in a task.
Update	Edit the Secure Agent group.
Delete	Delete the Secure Agent group.
Change	Change permissions for the Secure Agent group.

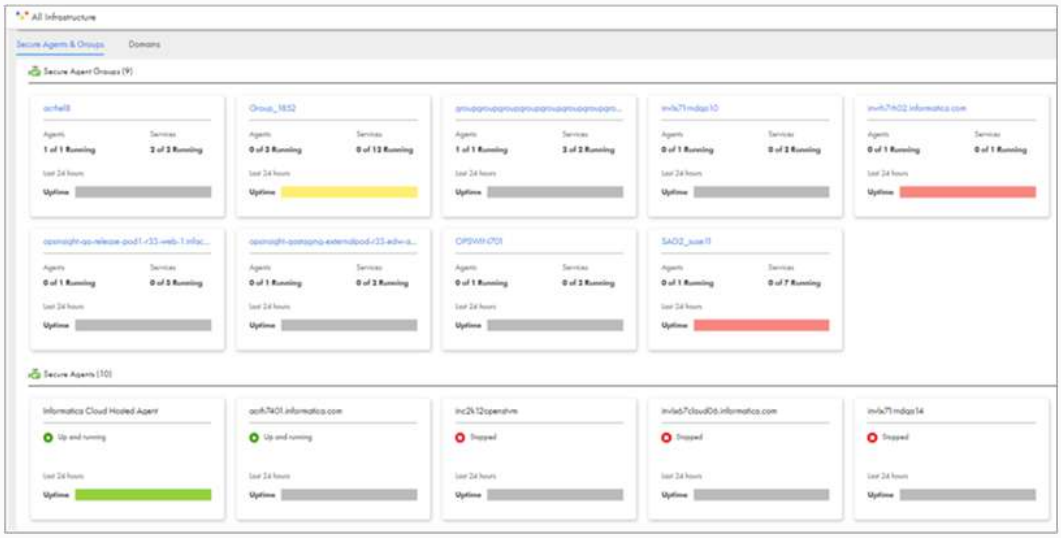
Viewing Secure Agent Details; Secure Agent Statuses;

Use the Secure Agents & Groups panel of the All Infrastructure page to view the status of a Secure Agent and the Secure Agent services it runs. Secure Agent services are microservices that the Secure Agent uses for data processing. You can log in to a sub-organization or switch from a parent organization to a sub-organization to use the

Secure Agents & Groups

panel of the sub-organization.

1. Click **All Infrastructure** on the Operational Insights navigation bar.
   The **All Infrastructure** page appears.
   The following image shows the **Secure Agents & Groups** panel of the All Infrastructure page:



   Hover over a Secure Agent group to view a list of all agents and services and their corresponding status in each runtime environment. Hover over an

   Uptime

   bar to view the status of all the Secure Agents according to their time range for the last 24 hours in each runtime environment. The status of the Secure Agents is shown by the following colors:

   - Green: all agents are running.

- Yellow: at least one agent is running.
- Red: all agents are down.
- Grey: no data was captured.

If a Secure Agent is stopped for over 30 days, the **Uptime** bar doesn't display data for the agent, and alerts about the agent aren't sent to email recipients. You must restart the Secure Agent to display data for the agent and to send alerts about the agent to email recipients.

2. Click the name of a runtime environment, agent, or service in a Secure Agent group.

   The Runtime Environment page appears. The page shows the status of the Secure Agents, the Secure Agent services, and jobs running in the environment.

   The Resource Utilization graph shows overall resource utilization by services running in the runtime environment for the selected time period. The Resource Utilization: Disk Usage graph shows the daily amount of used and free disk space for the last month

Secure Agent services

Secure Agent services are pluggable microservices that the Secure Agent uses for data processing. For example, the Secure Agent uses the Data Integration Server to run data integration jobs and Process Server to run application integration and process orchestration jobs. Each Secure Agent service runs independently of the other services that run on the agent.

The independent services architecture provides the following benefits:

- The Secure Agent does not restart when you add a connector or package.
- Services are not impacted when another service restarts.

  For example, process orchestration jobs continue to run when the Data Integration Server restarts.
- Downtime during upgrades is minimized. The upgrade process installs a new version of the Secure Agent, updates connector packages, and applies configuration changes for the Data Integration Server and Database Ingestion agent service. To minimize downtime, the old agent remains available and continues to run data integration jobs during the upgrade. The new version of the Secure Agent runs jobs that start after the upgrade process completes.

The services that run on a Secure Agent vary based on your licenses and the Informatica Intelligent Cloud Services that are enabled for the Secure Agent group.

Performance Tuning Overview

The goal of performance tuning is to optimize session performance by eliminating performance bottlenecks. To tune session performance, first identify a performance bottleneck, eliminate it, and then identify the next performance bottleneck until you are satisfied with the session performance. You can use the test load option to run sessions when you tune session performance.

If you tune all the bottlenecks, you can further optimize session performance by increasing the number of pipeline partitions in the session. Adding partitions can improve performance by utilizing more of the system hardware while processing the session.

Because determining the best way to improve performance can be complex, change one variable at a time, and time the session both before and after the change. If session performance does not improve, you might want to return to the original configuration.

Complete the following tasks to improve session performance:

1. **Optimize the target.**
   Enables the Integration Service to write to the targets efficiently.
2. **Optimize the source.**
   Enables the Integration Service to read source data efficiently.
3. **Optimize the mapping.**
   Enables the Integration Service to transform and move data efficiently.
4. **Optimize the transformation.**
   Enables the Integration Service to process transformations in a mapping efficiently.
5. **Optimize the session.**
   Enables the Integration Service to run the session more quickly.
6. **Optimize the grid deployments.**
   Enables the Integration Service to run on a grid with optimal performance.
7. **Optimize the PowerCenter components.**
   Enables the Integration Service and Repository Service to function optimally.
8. **Optimize the system.**
   Enables PowerCenter service processes to run more quickly.

Configuring Secure Agent service properties

To configure Secure Agent service properties, open the

Runtime Environments

page and edit the Secure Agent. You can change, mask, and reset Secure Agent service property values. You can add and remove custom properties for a service. You can also change the Secure Agent name.

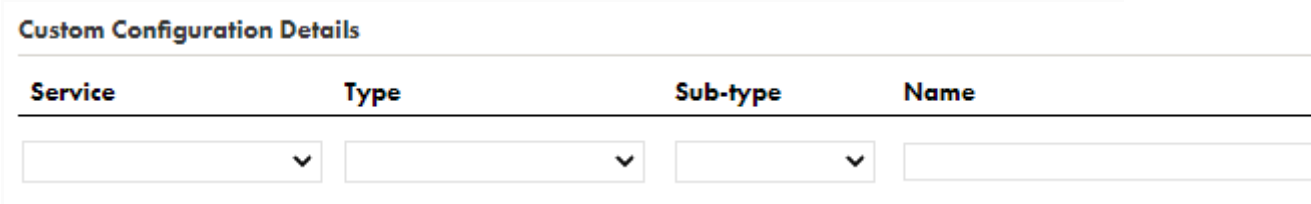
Custom properties are specific to connectors. For more details about custom properties, see the help for the appropriate connector.

Do not configure agent-level Secure Agent service property settings for an agent in a Secure Agent group that uses group-level property settings. If you want to configure agent-level property settings, delete the group-level property settings before you configure the agent properties. For more information about group-level property settings, see "Runtime Environments" in the *REST API Reference*
.

1. On the
   Runtime Environments
   page, click the name of the Secure Agent.
   You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
2. Click the
   Details

tab.

3. In the upper right corner, click **Edit**.
4. To change the Secure Agent name, enter a new name in the **Agent Name** field.
5. To edit a service property, perform the following steps:
   a. In the **System Configuration Details** area, select a service.
   b. Select the configuration property type.
   c. In the row that contains the property that you want to edit, click the **Edit Agent Configuration** icon.
   d. To change the property value, enter the new property value.
      If the property is a sensitive property, the existing value will be cleared when you edit the property.
   e. If the property contains sensitive data and you want to mask the value on the Secure Agent details page, enable the **Sensitive** option.
      When you enable the sensitive option, the value you enter is masked. If the field is a multi-line text field, the value is masked after you save the changes.
   f. To reset the property to the system default value, click the **Reset Agent Configuration to system default** icon.
6. To add a custom property for a service, perform the following steps:
   a. Scroll down to the **Custom Configuration Details** area.
      The following image shows the **Custom Configuration Details** area:



   b. If there are custom properties already configured, click the **Add** icon to add a new property row.
   c. Select the service that you want to configure.
   d. Select a configuration property type.
   e. If the configuration property type has a sub-type, select the appropriate sub-type.
      For example, to determine the logging level, choose INFO or DEBUG as the sub-type.

f. Enter the property name and value.

g. If the property contains sensitive data and you want to mask the value on the Secure Agent details page, enable the **Sensitive** option.

7. To remove a custom property, click the **Remove** icon next to the custom property.
8. To reset all configuration properties to the default settings, click **Reset All**.
9. Click **Save**.

Tuning the Data Integration Server

The Data Integration Server is the Secure Agent service that runs data integration jobs such as mapping, task, and taskflow instances. You can tune the Data Integration Server to achieve better task performance.

To improve performance, configure the maxDTMProcesses custom property and the JVM options.

You can configure these properties from the Runtime Environments page in Administrator. Select a Secure Agent on the Runtime Environments page to display and edit service properties for the agent.

Connections And File Transfer Settings:

What is a Connection?

A connection is a repository object that defines a connection in the domain configuration repository.

The Data Integration Service uses database connections to process jobs for the Developer tool and the Analyst tool. Jobs include mappings, data profiles, scorecards, and SQL data services.

You can create and manage connections in the Administrator tool, the Developer tool, and the Analyst tool.

The tasks that you can perform in each tool depend on the tool that you use. For example, you can create an SAP NetWeaver connection in the Developer tool and manage it in the Administrator tool, but you cannot create or manage it in the Analyst tool.

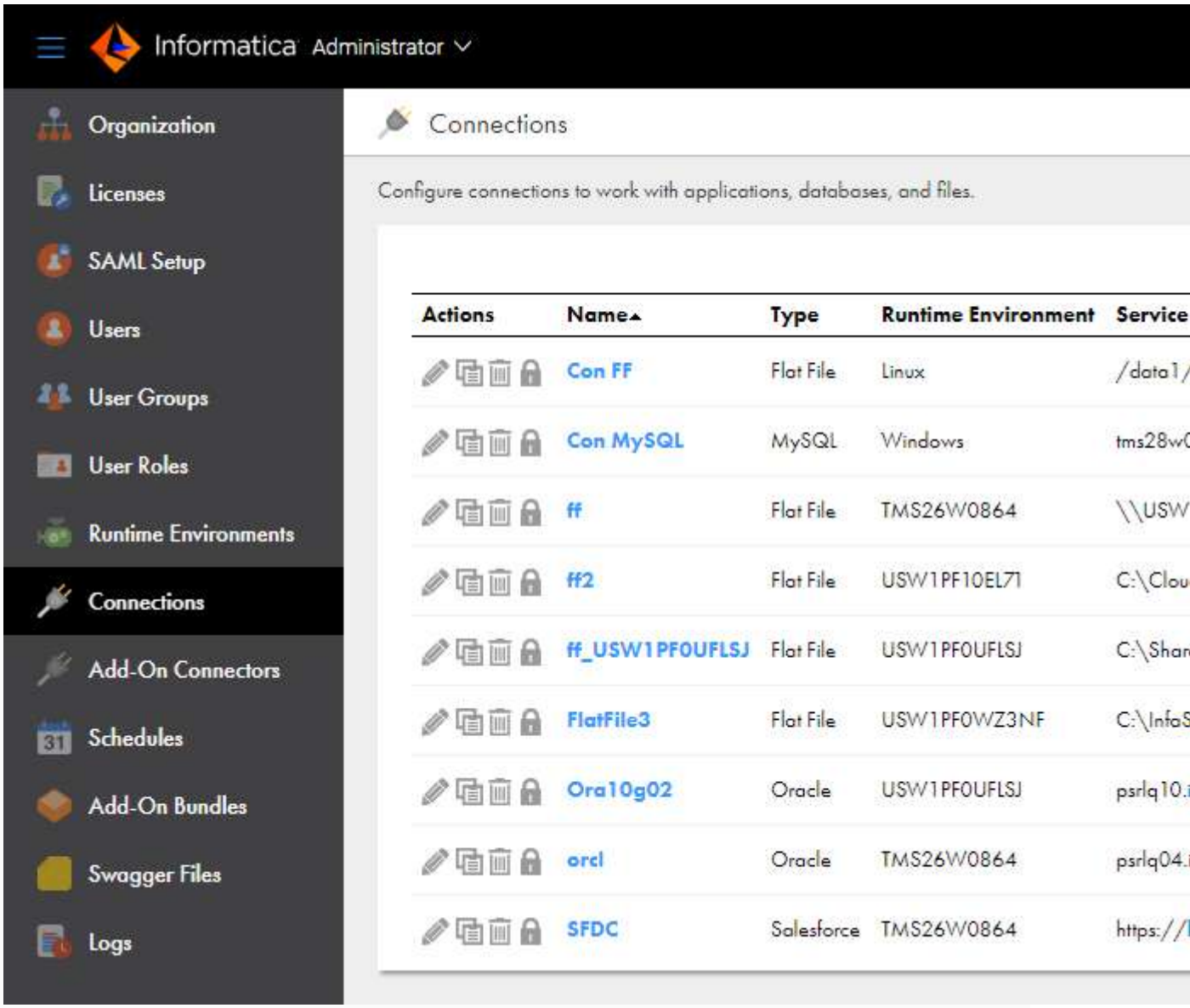
Connection configuration

When you configure a connection, the connection becomes available for use within the organization.

If you use sub-organizations and you want a connection to be available to multiple sub-organizations, create the connection in each sub-organization.

Configure connections on the Connections page. The Connections page lists all of the connections that have been configured in the organization. You can create a connection on this page. You can also search for an existing connection by name or description, by name only, or by description only.

The following image shows the Connections page:



When you configure a connection, you specify the runtime environment for the connection. The runtime environment must contain an agent that is running. You can override the runtime environment in the connection from the mapping or mapping task.

The runtime environment manages the connection between Informatica Intelligent Cloud Services

and the connection endpoint. It helps you perform the following tasks:

- Test the connection to the endpoint.
- Display objects available for the connection and retrieve metadata when you use the connection in an asset. You can preview data in the source, target, or lookup object selected in the asset.
- Run assets that use the connection to read from a source, transform data, or write data to a target.

You can configure a connection to a database, cloud data warehouse, or other endpoint type. When you create a source or target connection to a database or cloud data warehouse, you connect to a table, alias, or view. For example, when you create a Snowflake Data Cloud connection, you connect to a Snowflake table or view. For more information about creating connections to different types of endpoints, see the help for the appropriate connector.

When you configure connections for sources and targets in a mapping or task, where the connections require you to specify the code page, ensure that the code pages are the same. If the source system and target system in a task use different code pages, the Informatica Intelligent Cloud Services might load unexpected data to the target.

You can delete any connection that you create as long as the connection is not used by a saved query or task.

Commonly used connections

Connection Types

When you create a connection object, choose the connection type in the Connection Browser. Some connection types also have connection subtypes. For example, a relational connection type has subtypes such as Oracle and Microsoft SQL Server. Define the values for the connection based on the connection type and subtype.

When you configure a session, you can choose the connection type and select a connection to use. You can also override the connection attributes for the session or create a connection. Set the connection type on the mapping tab for each object.

The following table describes the connection types that you can create or choose when you configure a session:

Connection Types

Connection Types	Description
Relational	Relational connection to source, target, lookup, or stored procedure database. When you configure a session, you cannot change the relational connection type.
FTP	FTP or SFTP connection to the FTP host. When you configure a session, select an FTP connection type to access flat files or XML files through FTP. Specify the FTP connection when you configure source or target options. Select an FTP connection in the Value column.

Connection Types

Connection Types	Description
Loader	Relational connection to the external loader for the target, such as IBM DB2 Autoloader or Teradata FastLoad. When you configure a session, choose File as the writer type for the relational target instance. Select a Loader connection to load output files to teradata, Oracle, DB2, or Sybase IQ through an external loader. Select a loader connection in the Value column.
Queue	Database connection for message queues, such as WebSphere MQ or MSMQ. Select a Queue connection type to access an MSMQ or WebSphere MQ source, or if you want to write messages to a WebSphere MQ message queue. Select an MQ connection in the Value column. For static WebSphere MQ targets, set the connection type to FTP or Queue. For dynamic MQSeries targets, set the connection type to Queue.
Application	Connection to source or target application, such as Netezza or SAP NetWeaver. Select an Application connection type to access PowerExchange sources and targets and Teradata FastExport sources. You can also access transformations such as HTTP, Salesforce Lookup, and BAPI/RFC transformations.
None	Connection type not available in the Connection Browser. When you configure a session, select None if the mapping contains a flat file or XML file source or target or an associated source for WebSphere MQ.

For information about connections to PowerExchange see

PowerExchange Interfaces for PowerCenter

.

Assets

In Data Integration, assets are mappings, taskflows, and tasks such as mapping tasks,

synchronization tasks, and replication tasks. Assets also include components such as business

services, mapplets, and hierarchical schemas.

Create the assets you need to satisfy your business needs. Templates are available for certain asset types. You can use a template as-is, or you can use it as head start and customize it to meet your needs.

You can use assets in multiple projects. All assets must be part of at least one project. If you create an asset without specifying a project, the asset is created in the Default project.

Getting Started with Assets

Creating assets

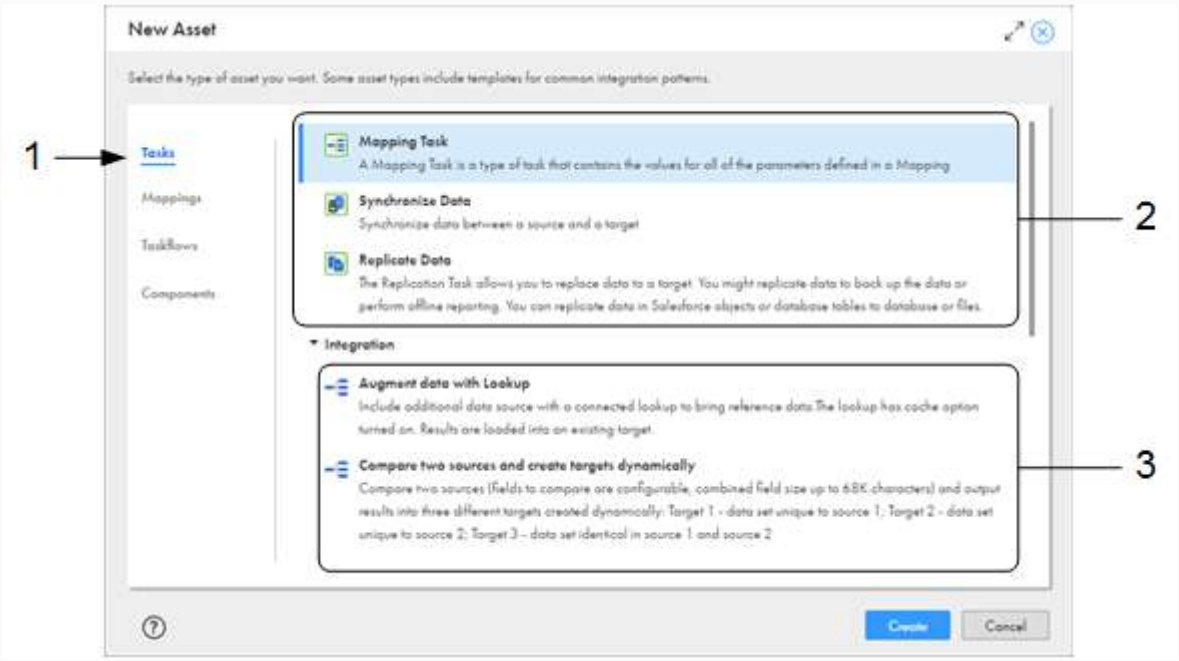
Create integration assets and assign them to projects.

You can create custom assets or create assets from a template.

To create a custom asset, click
New
and then select the asset type. For specific information on creating a particular type of asset, see the appropriate asset type in
Mappings
or
Tasks
.

To create an asset from a template, click
New
, select the asset type, and then select the appropriate template.
Mapping
task templates and mapping templates are listed below the heading that corresponds to the mapping type.

The following image shows the dialog box that appears when you create an asset:



1. *Select the type of asset that you want to create. In this image, Tasks is selected.*
2. *Select one of these options to create a custom asset. Since Tasks is selected on the left, this area lists the tasks that you can create.*
3. *Select one of the options below a heading to create a task from a template. In this image, the Integration heading is expanded, so the templates listed are based on data integration mappings.*

Informatica recommends that you use a standard naming convention that makes sense for your organization. Here are a few examples:

- You can begin all asset names with an abbreviation of the asset type. For example, mapping names begin with m_ and mapping tasks begin with mt_.

- Within mappings, you can begin all Source transformation names with src_, all parameter names with p_, and so on.
- You can use names that explain the purpose of the object, For example, filter names begin with flt_.

A standard naming convention is particularly helpful when you are working with large, complex mappings so that you can easily identify the type and purpose of each object.

Asset Management

You can manage Data Ingestion and Replication assets such as projects, folders, and ingestion tasks from the Explore page.
You can perform the following management tasks depending on your user role and permissions:

- Edit ingestion tasks.
- Copy projects, folders, and ingestion tasks.
- Move folders and ingestion tasks.
- Rename projects, folders, and ingestion tasks.
- Delete projects, folders, and ingestion tasks.
- Apply tags so you can filter assets on the
  Explore
  page.
- Configure user permissions for projects, folders, or assets.
- Use source control to manage versions of projects, folders, and tasks.
- Migrate assets between organizations.

Managing Assets:

Example : In Informatica, an Ingestion Task, part of Ingestion and Replication or Taskflows, is a step used to move data, typically files or data from databases, to a target system. It's a core component in processes like Mass Ingestion and Data Integration

Configuring user permissions on an ingestion task

You can configure permissions for an ingestion task if you are assigned a user role that has the

Set Permission

Privilege for the asset type of Database Ingestion and Replication Task or Streaming Ingestion and Replication Task.
Typically, the organization administrator assigns user roles to specific users of the
Data Ingestion and Replication
service.

1. In Data Ingestion and Replication, open the Explore page and navigate to the row for the ingestion task for which you want to set permissions.
2. In the Actions menu for the row, select

Permissions.

The Permissions dialog box lists the users and user groups that have permissions set on the task. Other users cannot access the task.If the Permissions dialog box lists no users or user groups, no permissions are configured for the task. In this case, any user can access the task without permission restrictions.

3. To add a user to the users list and grant permissions on the task to that user, perform the following steps:
   a. On the **Users** tab, click **Add**.
   b. In the Add User dialog box, select a user and click **Add**.
   c. In the Permissions dialog box, select the permissions on the task that you want to grant to the user.
   d. Click **Save**
4. To add a user group to the groups list and grant permissions on the task to that user group, perform the following steps:
   a. On the **Groups** tab, click **Add**
   b. In the Add Group dialog box, select a group and click **Add**.
      If no groups are listed, no user groups are defined.
   c. In the Permissions dialog box, select the permissions on the task that you want to grant to the group.
   d. Click **Save**.
5. To edit the permissions that are set for a listed user or user group, on the **Users** or **Groups** tab in the Permissions dialog box, select or clear the permission check boxes for the user or group. Then click **Save**.
6. To remove all of the permissions that you set for one or more users or user groups, on the **Users** or **Groups** tab in the Permissions dialog box, select the users or groups from which you want to remove all permissions. Then click **Remove** and click **Save.**.

Editing ingestion tasks

You can edit an ingestion task from the Explore page.

1. In Data Ingestion and Replication, open the Explore page.
2. If a list of projects is displayed, select the project or project folder that contains the ingestion task that you want to edit.
3. In the list of tasks, select the row for the ingestion task that you want to edit.
4. In the Actions menu for the selected row, click **Edit**.
   The Definition page of the task wizard appears in edit mode.
5. Edit the available fields on the Definition, Source, Target, and Runtime Options pages.
   For a database ingestion and replication task, the following considerations apply:
   - You can edit any properties that are available for editing and then redeploy the associated job. If you need to edit a connection or property that is not available, first undeploy the associated job. Then edit the task and deploy the task again to create a new job instance.

- If you change the name of a task that has been deployed, the associated job name remains the same as the original task name. If you want the job name to match the updated task name, undeploy the job and then deploy the task again to generate a new job that has a matching name.
- If you change the rules for renaming target tables for a deployed database ingestion task, the associated job creates new target tables and performs an initial load of data to these tables. If the job is for a combined initial and incremental load, after the initial load is complete, the job begins propagating data changes to the target.

  The
  database ingestion and replication
  job does not drop or truncate the original target tables based on the old renaming rules.

6. When you are finished, click
   Save
   .