Informatica® Cloud Data Quality
July 2024

Asset Management

Informatica Cloud Data Quality Asset Management
July 2024
July 2024

© Copyright Informatica LLC 2019, 2024

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

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

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

Portions of this software and/or documentation are subject to copyright held by third parties.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

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

Publication Date: 2024-07-11

Table of Contents

Preface 5

Informatica Resources 5

- Informatica Documentation 5
- Informatica Intelligent Cloud Services web site 5
- Informatica Intelligent Cloud Services Communities 5
- Informatica Intelligent Cloud Services Marketplace 5
- Informatica Knowledge Base 6
- Informatica Intelligent Cloud Services Trust Center 6
- Informatica Global Customer Support 6

Chapter 1: Project and asset management 7

Copying projects, folders, and assets 7

Moving folders and assets 8

Renaming projects, folders, and assets 8

Deleting projects, folders, and assets 9

Tags 10

- Creating tags 11
- Assigning tags 12
- Editing and deleting tags 13

Asset dependencies 14

Permissions 15

- Rules and guidelines for permissions 16
- Configuring permissions 17

Chapter 2: Source control 19

Source control actions 19

Source control and the Git repository 20

Configuring repository access 20

Project-level repositories 21

- Linking a project to a source control repository 21

Source control pulls 22

- Project and folder pulls 22
- Pulling an object 23

Commit tags 24

Checking out and checking in objects 24

- Checking out an object 24
- Checking in an object 25

Deleting an object 25

Reverting to an older version 25

Undoing a checkout 26

Unlinking an object. . . . 26
Working with multiple objects. . . . 26
Viewing source control columns on the Explore page. . . . 27
Source control best practices. . . . 28

Chapter 3: Asset migration. . . . 30

Asset migration requirements. . . . 30
Dependent objects. . . . 30
Runtime environments and connections. . . . 31
Dependent objects example. . . . 31
Schedules. . . . 32
Bundle objects. . . . 32
Asset export. . . . 32
Export Files. . . . 33
Exporting assets. . . . 34
Asset import. . . . 35
Asset name conflicts. . . . 36
Importing asset tags. . . . 37
Importing assets with persisted values. . . . 37
Importing assets. . . . 38
Post-import tasks. . . . 39

Chapter 4: Bundles. . . . 40

Using bundles. . . . 40
Copying bundle assets. . . . 41
Referencing bundle assets. . . . 42
Creating and publishing bundles. . . . 42
Creating a bundle. . . . 44
Submitting a public bundle for review. . . . 45
Sharing a private bundle. . . . 45
Generating a bundle access code. . . . 45
Deprecating a bundle. . . . 46
Deleting a bundle. . . . 46

Index. . . . 47

Preface

Use *Asset Management* to learn how to manage Data Quality projects, folders, and assets. Learn how to configure asset permissions, manage asset versions, and tag, migrate, and bundle assets.

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.

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/

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

Project and asset management

You can manage projects and assets on the **Explore** page. The **Explore** page is an Informatica Intelligent Cloud Services feature that is available for most services. If you use multiple services, you might see projects, folders, and assets for all of your services on the **Explore** page.

You can manage your Informatica Intelligent Cloud Services projects and assets in the following ways:

- Copy projects, folders, or assets to create new versions of them.
- Move folders or assets to other locations.
- Rename projects, folders, or assets.
- Delete projects, folders, or assets.
- Apply tags so you can filter for related assets on the **Explore** page.
- Configure permissions for projects, folders, or assets.
- Use source control to manage versions of projects, folders, and assets.
- Migrate assets between organizations.

Copying projects, folders, and assets

You can copy projects, folders, and assets on the **Explore** page. You might want to copy an object to use as a template, or you might want to create a backup copy.

When you copy objects, Informatica Intelligent Cloud Services retains child elements in the following instances:

- When you copy a project, the new project contains all of the folders and assets that were in the original project. Similarly, when you copy a folder, the new folder contains all of the assets that were in the original folder.
- When you copy assets or a folder containing assets to another location, the assets retain their references to dependent objects.
  For example, a folder in the Customers project contains the m_cust and the mt_ca_cust assets. The mt_ca_cust asset requires the m_cust asset. If you copy the mt_ca_cust asset to a folder in the Customers_ca_upsell project, the mt_ca_cust asset in the Customers_ca_upsell project still references the m_cust asset in the Customers project.

When you copy an asset within a folder, you can keep both assets. When you copy an asset into a different folder that contains an asset with the same name, you can overwrite the asset in the folder or keep both. If you choose to overwrite the asset, you can merge the asset tags. If you choose to keep both assets, Informatica Intelligent Cloud Services appends the new asset name with "Copy x" where x is the sequential copy number.

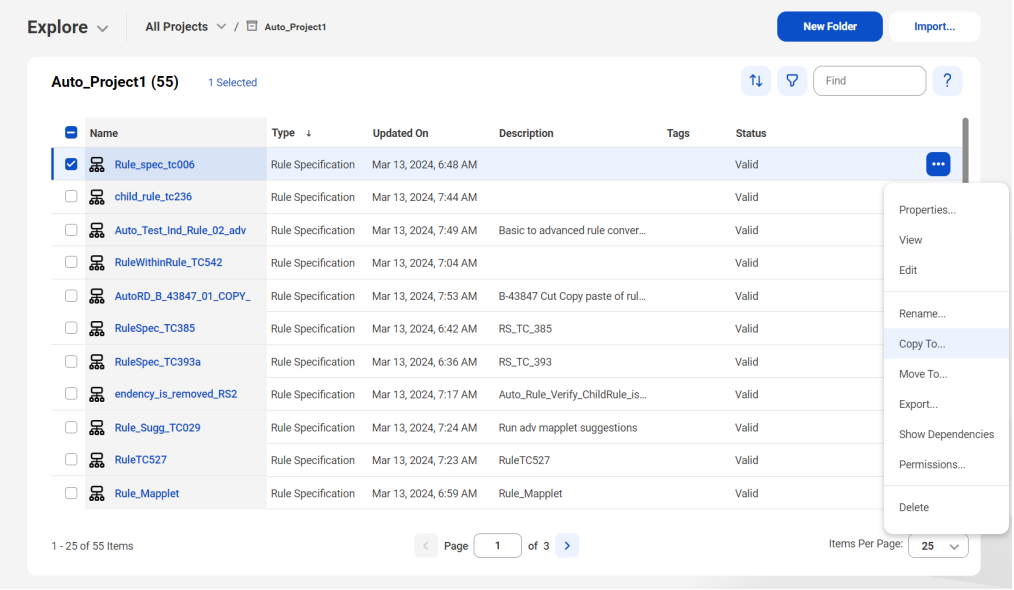
Note: To avoid naming conflicts with duplicate assets, rename assets with a "Copy x" suffix.

When you copy an asset with a schedule, the schedule is removed from the copied asset.

You can copy up to 1,000 objects at a time.

Perform the following steps to copy an object:

1. On the **Explore** page, navigate to the object that you want to copy.
2. In the row that contains the object that you want to copy, click **Actions** and select **Copy To**.



3. Browse to the new location and click **Select**.

Moving folders and assets

You can move folders and assets on the **Explore** page.

1. On the **Explore** page, navigate to the folder or assets that you want to move.
2. If your organization uses source control, check out the folder or assets that you want to move.

   If you want to move a folder, be sure to check out the folder and each of the assets within the folder.
3. To move a folder or a single asset, in the row that contains the folder or asset, click **Actions** and select **Move To**, and then browse to the new location and click **Select**.

Renaming projects, folders, and assets

You can rename projects, folders, and assets without losing references to objects that they use.

For example, if an asset named mt_ResolveClientList uses an asset named m_RegionToMainList, you can rename the mt_ResolveClientList asset to mt_ClientList and it will still reference the m_RegToMainList asset.

You can't use control characters or the following special characters in project, folder, asset, or tag names:

```
# ? ' | { } " ^ & [ ] / \
```

1. On the **Explore** page, navigate to the object that you want to rename.
2. If your organization has enabled source control, check out the object that you want to rename.
3. To rename an asset, in the row that contains the asset, click **Actions** and select **Rename**.
4. To rename a project or folder, in the row that contains the project or folder, click **Actions** and select **Properties**.
5. Enter the new name and click **Save**.

   You cannot use special characters in a name or use the same name as another object that is in the same folder.
6. If the object was checked out, check in the object so that the change is reflected in the Git repository.

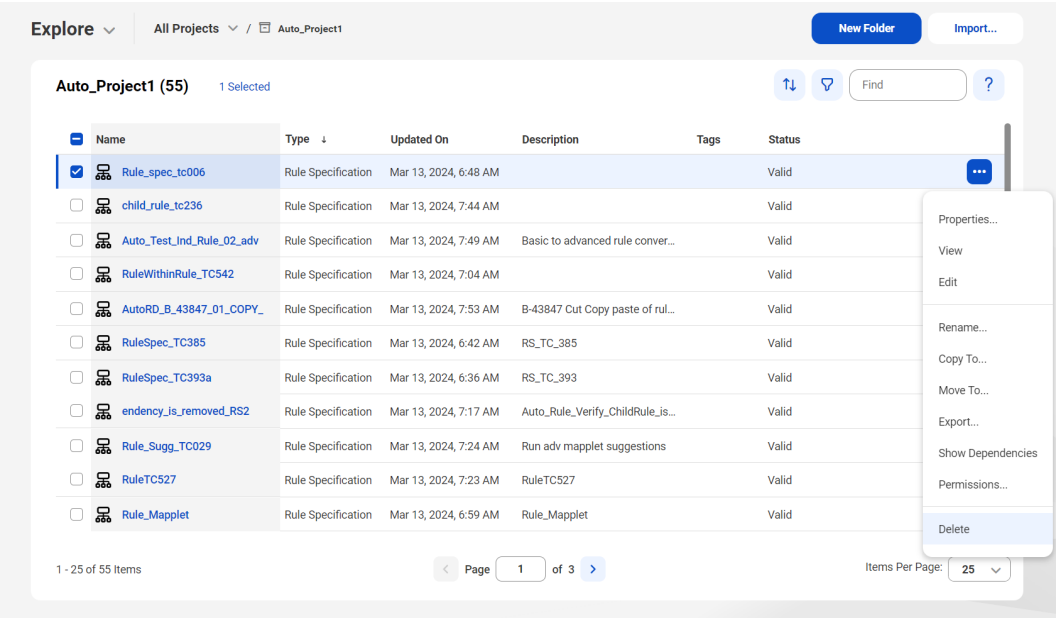
Deleting projects, folders, and assets

You can delete a project, folder, or asset if you no longer need it. However, before you delete it, verify that no users in the organization plan to use it. You cannot retrieve projects, folders, or assets after you delete them.

You cannot delete an asset in the following situations:

- The asset is a task that is currently running.
- The asset is a mapping that is currently running.
- The asset is used by another asset. You must first delete the dependencies of the asset before you can delete the asset.
  For information about viewing asset dependencies, see "Asset dependencies" on page 14.

Delete a project, folder, or asset from the **Explore** page, as shown in the following image:



1. On the **Explore** page, navigate to the object that you want to delete.

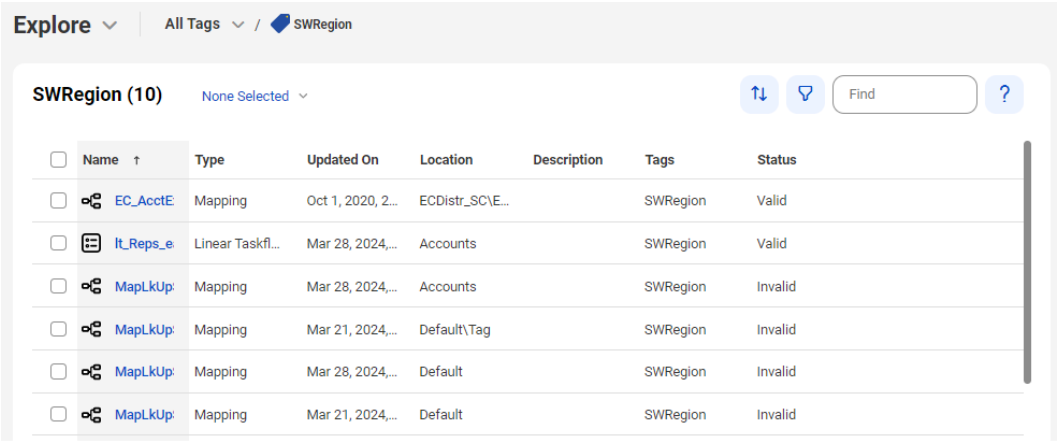
2. If your organization enabled source control, check out the object that you want to delete.
3. In the row that contains the project, folder, or asset, click **Actions** and select **Delete**.
4. If the object was checked out, check in the object so that the change is reflected in the Git repository.

Tags

A tag is an asset property that you can use to group assets. Create tags to filter for assets that share a common attribute on the **Explore** page.

For example, each of your organization's assets includes a tag that identifies the regional office that manages the asset. You want to view all of the assets that the Southwest regional office manages. On the **Explore** page, you explore by tag and then click the SWRegion tag.

The following image shows this configuration:

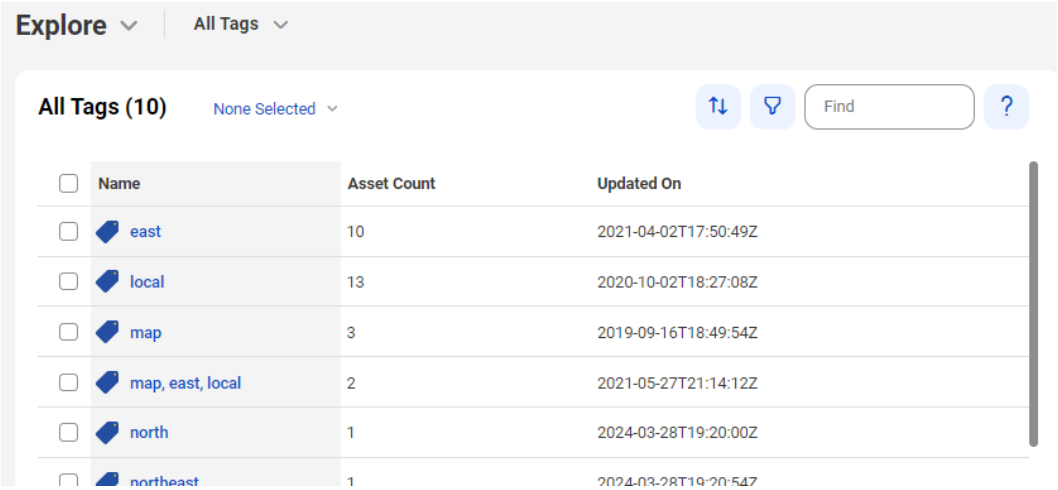


You can assign tags to all asset types. An asset can have up to 64 tags.

You can find all of the assets that have a particular tag using one of the following methods:

- Click the name of the tag in the **Tags** column, in any row.
- Explore by tag, and then in the list of tags that shows on the page, click the name of the tag.

The following image shows an **Explore** page that lists all the tags created for the organization:



Creating tags

Use an asset's **Properties** dialog box to create and assign tags for that asset or to create tags to be available for future use.

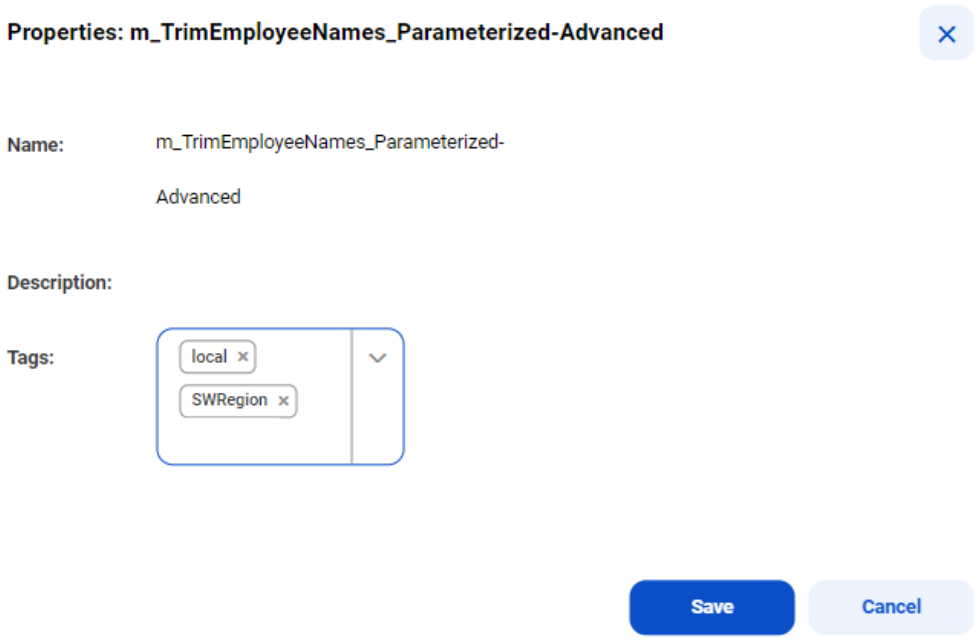
Perform the following steps to create multiple tags without assigning them to an asset:

1. On the **Explore** page, browse by asset type.
2. In a row that contains an asset, click **Actions** and select **Properties**.
3. In the **Tags** field, enter the name of a tag that you want to create, and then press Enter.

   A tag can have a maximum of 255 characters.
   You can't use control characters or the following special characters in project, folder, asset, or tag names:

   ```
   # ? ' | { } " ^ & [ ] / \
   ```

4. Continue to enter the desired tags. Press Enter after each tag name to add it to the tag list.



5. After you have entered the tags, delete the tags from the **Tags** field so that the asset does not become associated with the tags. The tags will still appear in the list of available tags.
6. Click **Save**.

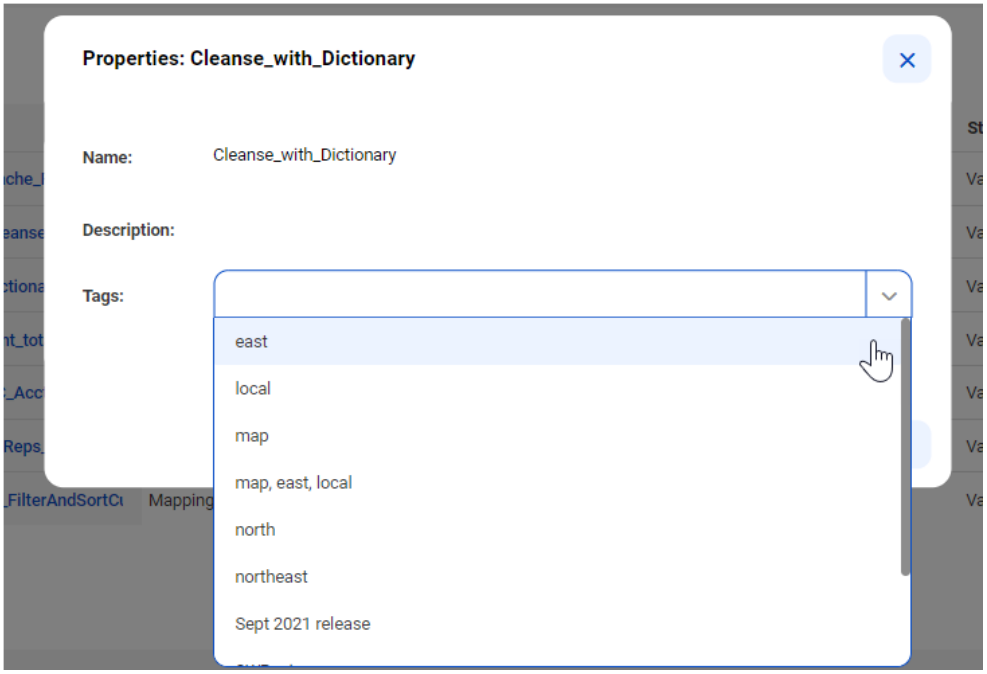
Assigning tags

You can assign a tag to one asset at a time or assign a tag to multiple assets at the same time. You can also assign multiple tags to one asset.

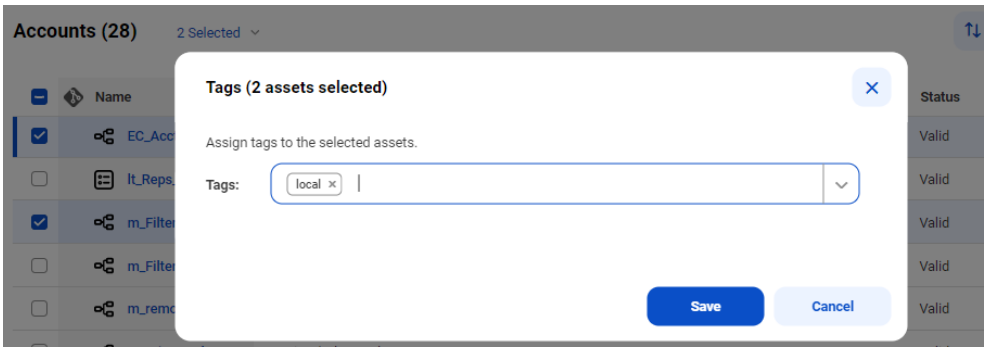
When you assign tags to an asset, you can choose an existing tag or create a new one.

1. On the **Explore** page, navigate to the asset or assets.

2. Perform one of the following tasks depending on whether you want to assign tags to one asset or assign tags to multiple assets at the same time.
   - To assign tags to one asset, in the row that contains the asset, click **Actions** and select **Properties**.



   - To assign tags to multiple assets at the same time, in the row for each asset, select the check box. After you have selected all of the assets, from the Selection menu, select **Tags**.



3. Select an existing tag or enter the name of a new tag.

   Continue adding tags or creating new tags until you have assigned all of the desired tags.

4. Click **Save**.

Editing and deleting tags

You can edit or delete a tag on the **Explore** page.

Edit a tag name or description in the tag properties. When you edit a tag, the properties for associated assets update as well. For example, if your m_sales asset has the NorthWest tag and you change the name of the tag to NW, the name of the tag changes to NW in the m_sales asset properties.

If you delete a tag, the tag no longer appears in the asset properties.

1. On the **Explore** page, browse by tags.

2. In the row that contains the tag, perform one of the following tasks:
   - To edit a tag, click **Actions** and select **Edit**. After you make your changes, click **Save**.
   - To delete a tag, click **Actions** and select **Delete**.

Asset dependencies

You can view object dependencies for an asset. You might want to view object dependencies before performing certain operations on an asset.

For example, you can't delete an asset if another object depends on the asset. You must first delete the dependent objects and then delete the asset. You can find the dependent objects by viewing the asset dependencies.

You can view object dependencies for an asset on the **Explore** page. To view object dependencies for an asset, in the row that contains the asset, click **Actions** and select **Show Dependencies**. The **Dependencies** page opens showing the **Uses** tab by default.

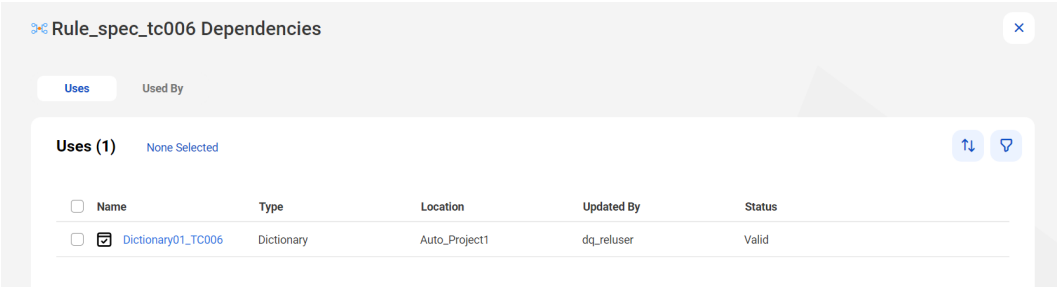
The **Uses** tab lists the objects that the selected asset uses.

For example, a rule specification might use a dictionary.

The **Used By** tab lists the objects that use the selected asset.

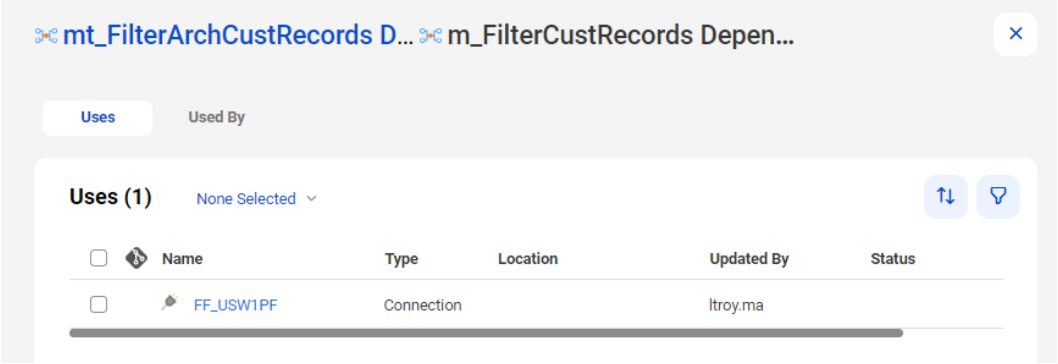
For example, a dictionary might be used by one or more rule specifications.

The following image shows the **Dependencies** page for a rule specification with the Uses tab open:



To drill down to the lowest level dependency, you can continue to show dependencies for each asset that appears on the **Dependencies** page. At the top of the **Dependencies** page, a breadcrumb shows the chain of dependencies.

The following image shows that the asset mt_FilterArchCustRecords is dependent on m_FilterCustRecords, which is dependent on FF_USW1PF:



If you have the appropriate permissions, you can perform actions on the **Dependencies** page such as viewing or deleting assets. To view or delete an asset, in the row that contains the asset, click **Actions** and select the action.

If you work with source controlled assets, you can view source control information such as the last pull time and the last check-in. To view source control information, you can add the following source control columns to the table:

- Last Pull Time
- Checked Out By
- Last Check in
- Git Hash

Note: You cannot view dependencies for advanced configurations.

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.
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.

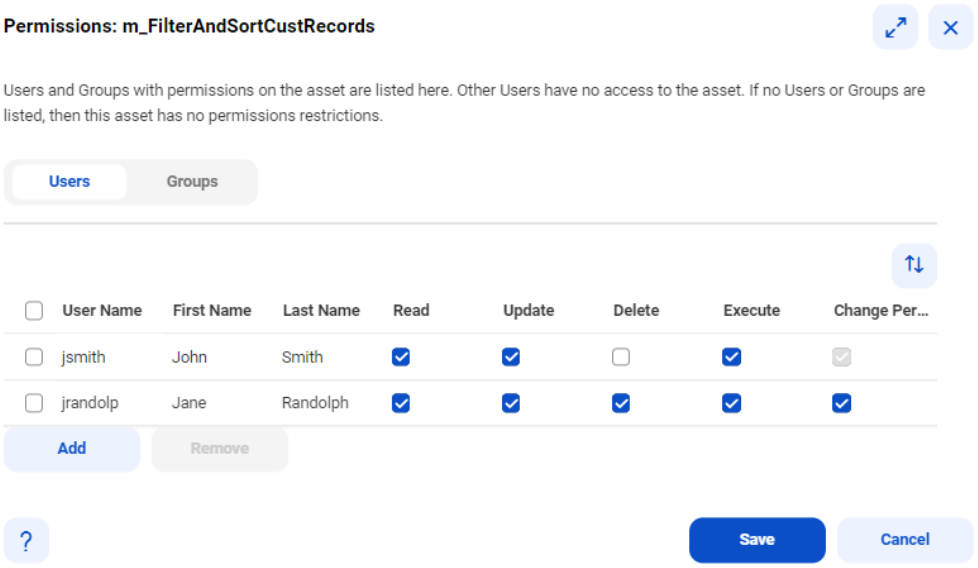
   For example:

   - 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 2

Source control

You can use a GitHub, Azure DevOps, or Bitbucket Git source control repository with Informatica Intelligent Cloud Services to manage and track changes made to Informatica Intelligent Cloud Services objects such as projects, folders, and assets.

You can use source control to enable version management for the Informatica Intelligent Cloud Services objects that appear on the **Explore** page, except for Data Integration bundles. You cannot apply source control to objects that don't appear on the **Explore** page such as runtime environments or connections. The source control repository structure mirrors the structure in the organization, with **Explore** as the top level directory.

Each time a user performs an action on an object that is source controlled, Informatica Intelligent Cloud Services logs the action. You can view source control logs in the Monitor service. For more information, see *Monitoring source control logs* in the Monitor help.

To use source control, the following prerequisites must be met:

- The organization has the appropriate Informatica Intelligent Cloud Services licenses to use source control.
- The organization administrator has configured a connection between the source control repository and the Informatica Intelligent Cloud Services organization.
- Your user role has privileges to use the Informatica Intelligent Cloud Services source control feature.
- You've entered your source control repository user credentials in Informatica Intelligent Cloud Services.

For information about configuring a connection between a Git source control repository and Informatica Intelligent Cloud Services, see the Administrator help.

Note: Informatica recommends that you include no more than 1000 objects in a container such as a project or folder when you use a source control repository with Informatica Intelligent Cloud Services.

Source control actions

You can perform the following actions on source-controlled objects such as projects, folders, and assets:

Pull an object.

Pull an object to add it to the organization or update a project with the version in the source control repository.

Check out an object.

Check out an object that you want to work on. When you check out an object, the object locks so that other users cannot make changes to it.

Check in an object.

Check in an object to add it to the source control repository or update the source control repository with the latest version of the object. When you check in an object, the lock releases.

Delete an object.

Delete an object from the organization and the source control repository. Before you can delete an object, you must check it out.

Restore an object version.

Restore an object to a previous version.

Undo a checkout.

Undo a checkout if you don't want to save the changes you made to the object. When you undo a checkout, the object reverts to the last source control version.

Unlink an object.

Unlink an object if you no longer want the object in the organization to stay in sync with the object in the source control repository.

Note: Some organizations do not have permission to update the source control repository. If your organization cannot update the repository, you can perform a pull action to get a specified version of the Informatica Intelligent Cloud Services objects. However, you cannot perform other source control actions such as checking out and checking in objects.

To check out, pull, unlink, or undo a checkout for an object, you must have update permissions on the object.

Source control and the Git repository

If you usually work directly in a Git source control repository, you might notice a few differences between using source control in Informatica Intelligent Cloud Services and working directly in the repository.

Note the following differences:

- A pull action in Informatica Intelligent Cloud Services is the same as a Git pull command. However, a pull in Informatica Intelligent Cloud Services cannot merge changes.
- A checkout action in Informatica Intelligent Cloud Services locks an object so that no one else can check it out or change it.
- A check-in action in Informatica Intelligent Cloud Services is the same as a Git commit command and push command combined. Use a check-in to add Informatica Intelligent Cloud Services objects to the source control repository and to commit changes to the repository.

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**.

Project-level repositories

If you're assigned a role with the Configure Custom Repository Source Control privilege, you can specify a source control repository to use at the project level, instead of using the global source control repository that's set up for your organization.

By default, when you perform a source control action on a project or folder, the action uses the global source control repository that's set up by the organization administrator. If the organization administrator enables project-level repositories, you can link a project to a repository other than the global repository.

If you use project-level repositories, be sure to add the Repository URL and Repository Branch columns to the Explore page.

Note: Before you link a project to a custom repository, make sure that other users who need access to the project have access to the repository.

Linking a project to a source control repository

You can link a project to a source control repository other than the global repository.

1. On the **Explore** page, in the row that contains the project, click Actions and select **Source Control Properties**.
2. Enter the Git repository URL and branch name that you want to use, and then click **Save**.
3. Click **Save** again to confirm that you want to use a repository other than the global repository.

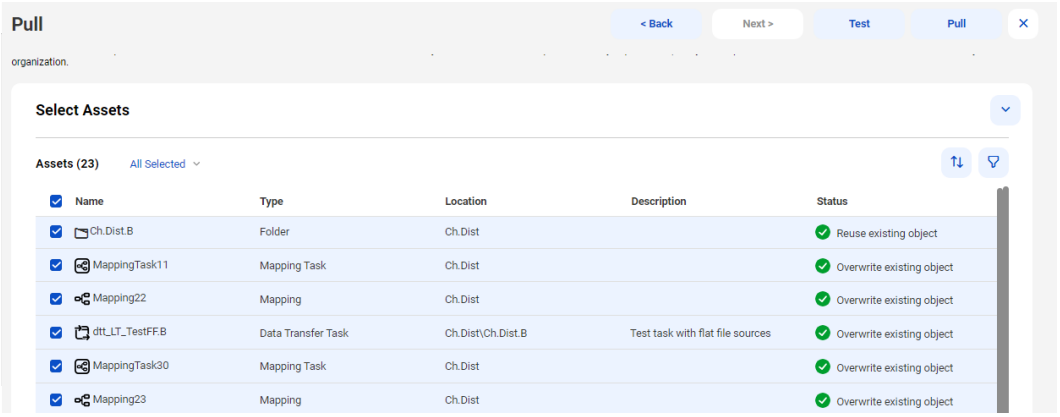
   After you click **Save**, only users who have access to the repository can check out and commit the project.

Source control pulls

Pull an object to add it to the organization or replace the version of the object in the organization with the version in the source control repository. You can pull a project, folder, or an individual object that isn't checked out by another user.

Before a pull takes place, you can review the potential results of the pull. You can cancel the action or select objects to exclude from the pull.

The following image shows a preview page with potential results in the **Status** column:



You can also test the pull to see if any errors might occur. If any errors appear, you can exclude the objects from the pull or close the page to cancel the pull.

A pull doesn't include dependent objects. For example, in Data Integration, if you pull a mapping that uses a saved query, the pull doesn't include the saved query.

A pull doesn't change the state of pulled objects in the organization. For example, if an object was checked out before the pull, it remains checked out after the pull.

Consider the following rules and guidelines:

- If you want to pull an object that uses a connection or runtime environment, be sure that the organization includes a connection and runtime environment before you perform the pull. When you select an object that uses a connection or runtime environment, you can select a runtime environment and connection to use on the test page.
- Informatica Intelligent Cloud Services doesn't consider capitalization in object names. As a result, you can't pull a project that contains multiple assets that have the same name with different capitalization. For example, if you try to pull a project that contains an asset named "sales" and an asset named "SALES", you receive an error because a project or folder can't contain multiple assets with the same name.
- You can pull objects regardless of whether your organization can or cannot update the source control repository.

Project and folder pulls

You can pull all of the objects in a project or folder, or pull only the objects that changed in a particular commit hash.

You specify the version of the objects that you want to pull. The versions of an object that you can select are based on the object's current location in Informatica Intelligent Cloud Services. For example, you check out version 5 of the m_customers object and move it to a project called NewCustomers. When you pull the object, the available versions do not include the versions of the object from the previous location.

If you pull a project or folder, the pull doesn't affect any objects in the project or folder that aren't source-controlled.

A pull updates the project or folder in the organization to be identical to the selected version of the project or folder in the repository. For example, if you pull an older version of a project and the project in the organization contains objects that were added in later versions, the pull deletes the objects.

Pulling an object

Use the pull action to update the organization with objects in the source control repository. You can pull a single asset, a project, or a folder. When you pull a project or folder, you can exclude any assets in the project or folder that you don't want to include in the pull.

1. To pull a project from the global repository, click **Pull from Global Git**. Select the project that contains the objects you want to pull and click **Next**.
2. To pull a project from a repository or branch that's configured at the project level, on the **Explore** page, select the asset or folder. Click **Actions** and select **Pull**.

   Note: You can't pull more than one project at a time.
3. To pull a single asset or folder, on the **Explore** page, select the asset or folder. Click **Actions** and select **Pull**.
4. For a project or folder, select the pull method that you want to use, and then click **Next**. You can use one of the following methods:
   - Pull all assets in a commit hash.
   - Only pull modified assets in a commit hash.
5. Select the Git hash that you want to pull and click **Next**.
6. Review the list of assets. You can clear the check box for any of the assets that you don't want to include in the pull. By default, all of the assets are selected.
7. Review the actions in the **Status** column for each asset. These actions will occur when the pull action is performed.
8. If an asset requires a connection, select a target connection to use in the organization or accept the default.

   Note: You can't create a new connection during the pull process.
9. If an asset requires a runtime environment, select a target runtime environment to use in the organization or accept the default.

   Note: You can't create a new runtime environment during the pull process.
10. Optionally, click **Test** to see if errors might occur as a result of the pull action.
11. Click **Pull**.

    The pull action generates a log showing details of this action. You can view the log on the **Source Control Logs** page in Monitor.

Commit tags

When you check in assets to your source control repository, you can include a commit tag. The tag appears as an annotated tag in your Git repository.

You might want to include a commit tag to mark assets within a check-in that are ready for deployment. When you add a commit tag, the tag is applied to each asset in the commit. You can add one tag for each commit, and the tag must be unique.

When you pull assets, Informatica Intelligent Cloud Services displays commit tags in the **Tag** column on the **Pull** page.

Note: The pull operation can take longer based on the number of commit tags you have in your repository.

Checking out and checking in objects

Check out an object so you can make changes to it. Check in the object when you want to update the source control repository with your changes. You can also check in objects to add them to the source control repository.

When you check out an object, the object locks so that other users can't make changes to it. When you check in an object, a new version of the object is created in the source control repository.

If you check in an object that's in a folder or project that isn't source controlled, the folder or project becomes source controlled. An asset can't reside in a source control repository unless it's in a container such as a project or folder.

If you import assets into an organization that uses source control, the assets must be checked out so that they can be overwritten.

Note: The size of a check-in cannot exceed 50 MB.

Checking out an object

When you check out an object, the object is locked so that other users can't update it while you are making your changes.

You can check out individual objects, multiple objects, or a project or folder to check out all of the objects within the project or folder.

Before you check out an object, you might want to perform a pull to be sure you update the latest version of the object. For more information about the pull action, see "Source control pulls" on page 22

1. On the **Explore** page, navigate to the object you want to check out.
2. In the row that contains the object, click **Actions** and select **Check Out**.
3. If the checkout includes multiple objects, on the preview page, review the results in the **Status** column. If you want to exclude an object, clear the check box next to the object name.
4. Click **Check Out**.

Checking in an object

Check in an object to add the object to the source control repository or to update the source control repository with the latest version of the object in the organization.

If no changes were made to the object, the check-in isn't reflected in the source control history and a new version of the object isn't created in the source control repository.

Note: The size of a check-in cannot exceed 50 MB.

1. On the **Explore** page, navigate to the object you want to check in.
2. In the row that contains the object, click **Actions** and select **Check In**.
3. If the check-in includes multiple objects, on the preview page, review the results in the **Status** column. If you want to exclude an object, clear the check box next to the object name. If you want to cancel the action, close the page.
4. Add a summary and optionally, a description and commit tag.

   A summary is required and has a max length of 255 characters.
5. Click **OK**.

Deleting an object

To delete a source controlled object, you delete it from the organization and from the source control repository.

You must check out an object before you can delete it.

You can't delete an object that's checked out by another user or delete a project or folder recursively.

1. On the **Explore** page, navigate to the object that you want to delete.
2. On the row that contains the object, click **Actions** and then click **Delete**.
3. To confirm that you want to delete the asset from the organization, click **Delete**.
4. Add a summary that describes the reason for the delete action and optionally, a description.

   A summary is required and has a max length of 255 characters.
5. To delete the object from the repository and complete the delete action, click **OK**.

Reverting to an older version

You might want to revert to a previous version of an object if you want to discard changes that were made to the object.

To revert to a previous version, perform a pull action and select the version that you want to restore in the organization.

If you revert the version of a project or folder and the project or folder in Informatica Intelligent Cloud Services contains objects that are not in the repository's project or folder, the pull action deletes the additional objects if they are source controlled. If the objects are not source controlled, the action doesn't delete the additional objects.

For more information about the pull action, see “Source control pulls” on page 22.

Undoing a checkout

When you undo a checkout, the object reverts to the last version that was pulled. The object's version history will not include a record of the checkout and undo checkout actions. The undo checkout releases the lock so that the object is available for checkout.

You can undo the checkout of individual objects, multiple objects, or a project or folder in a single checkout action.

You can undo the checkout of any object that you have checked out. You cannot undo the checkout of an object that has been checked out by another user unless you have the Admin role or your user role has the Force Undo Checkout feature privilege for the Administrator service.

If you undo the checkout of a project or folder, you can select which objects within the project or folder to include or exclude. By default, all of the objects are included.

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

1. On the **Explore** page, navigate to the object.
2. In the row that contains the object, click **Actions** and select **Undo Check Out**.
3. If the undo checkout includes a project or folder, on the preview page, select the objects within the project or folder to exclude from the undo checkout action.

Unlinking an object

You can unlink an object so that it's no longer source controlled.

Unlinking an object doesn't delete the object from the source control repository or the organization, but you can no longer update the repository for any changes you make to the object in the organization. If you decide to link the object in the future, you can check in the object to reestablish the link. If the name of the object or the path to the object has not changed, the checked in object becomes a new version of the object in the source control repository.

The object must be checked in before you can unlink it. You can unlink an object that's checked out by 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't unlink a project or folder that contains source controlled objects. To unlink a project or folder, unlink each object within the project or folder first.

1. On the **Explore** page, navigate to the object that you want to unlink.
2. On the row that contains the object, click **Actions** and select **Unlink**.

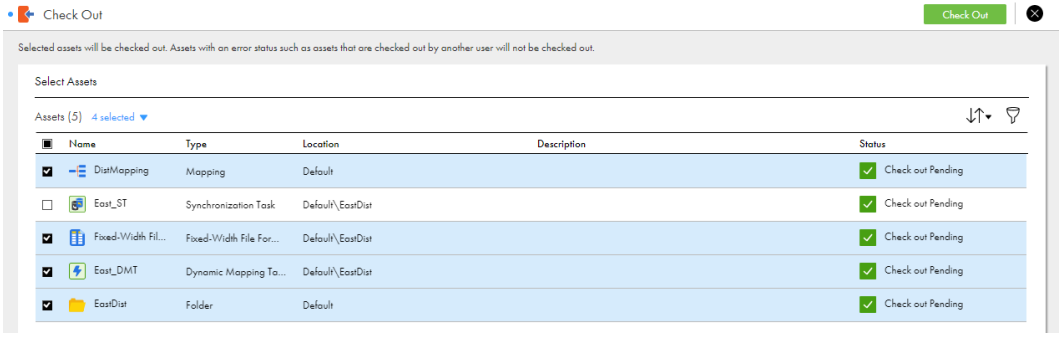
Working with multiple objects

You can select multiple objects to check in, check out, undo checkout, pull, or unlink.

The total size of the selected objects cannot exceed 50 MB.

You can select a project or folder or select multiple objects within a project or folder. When you include a project or folder or multiple objects in a source control action, a preview page appears that shows you the expected results of the action if you proceed. If an object listed on the preview page is not source controlled, it will be ignored. If an object is checked out by another user or you do not have permission to update the object, the status on the preview page shows that the action will fail. You can opt to remove any of the objects before you continue.

For example, in the Default project, you select the EastDist folder and the DistMapping asset to check out. The preview page includes the DistMapping asset, the EastDist folder, and all of the objects in the EastDist folder. You don't want to check out the East_ST asset so you clear its check box before you proceed with the checkout action. The following image shows the preview page:



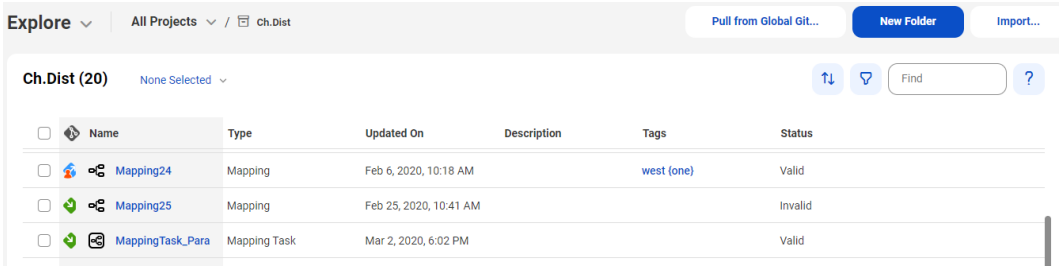
If you select multiple objects for a pull, the preview page lists all of the versions in the repository.

Note: You can't delete multiple objects in one transaction.

Viewing source control columns on the Explore page

If your organization has any objects that are source controlled, the **Explore** page displays an additional column that indicates whether an object is checked in, checked out, or is not source controlled.

In the following image, the blue and red icon indicates that the Mapping24 object is checked out:



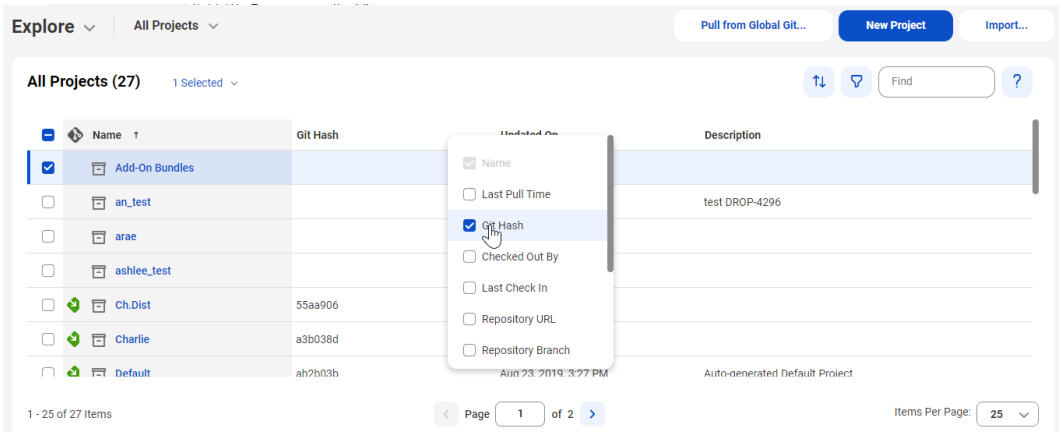
Additional source control columns are available but are not displayed by default. You might want to customize the **Explore** page to show all of the source control-related columns. This way you can easily identify source controlled objects, and you can use the columns to filter and sort source controlled objects on the page.

You can add the following source control-related columns to the **Explore** page:

- Last Pull Time
- Checked Out By
- Last Check In

- Git Hash
- Repository URL
- Repository Branch

To display these columns, right-click a column heading and select the columns that you want to add, as shown in the following image:



Source control best practices

To use source control effectively, use the following guidelines as best practices.

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.

CHAPTER 3

Asset migration

You can migrate Informatica Intelligent Cloud Services assets from one organization to another organization. To migrate assets, you export the assets from the source organization and then import the assets into the target organization.

You can export single assets, groups of assets, or export all of the assets in a project. If you export a project or folder, the file structure remains intact so that when you perform the import in the target organization, you can duplicate the original structure.

To export or import assets in a sub-organization, log in to the sub-organization. If you have administrator privileges in the parent organization, you can also switch to the sub-organization and export or import assets.

Asset migration requirements

To migrate assets from one organization to another, the organizations and your user accounts in the organizations must meet certain requirements.

Ensure that you meet the following requirements:

- You have a user account in the source and target organizations with a role that has import and export privileges, such as the Admin or Designer role.
- The source and target organizations have the required license to import and export assets.
- The target organization has the required licenses for the assets that you want to import.
- The target organization uses the same version or a newer version of Informatica Intelligent Cloud Services. The versions might differ temporarily if the organizations aren't on the same POD (Point of Delivery) during an Informatica Intelligent Cloud Services upgrade.

Dependent objects

Dependent objects are assets that are required by other assets.

For example, a dictionary that a rule specification reads at run time is dependent object.

When you set up an export, you have the option to include or exclude dependent objects in the export file. The dependent objects must exist either in the export file or in the target organization, else the import fails.

You might want to include dependent objects if they do not exist in the target organization. Or, you might want to include dependent objects if you want to replace the dependent objects in the target organization

with updated versions from the source organization. If you choose to include dependent objects, the export file includes dependent objects for all of the assets that you include in the export. When you configure the import, you can choose which dependent assets to import.

You might want to exclude an asset's dependent objects if the objects exist in the target organization and you do not want to replace them.

Note: Schedules are not dependent objects and are not included when you export assets that use them.

Runtime environments and connections

Runtime environments and connections are dependent objects.

If you configure an export to include dependent objects, you can use the source connections and runtime environments in the export file, or you can select connections and runtime environments in the target organization.

If you configure an export to exclude dependent objects, be sure that a suitable connection and runtime environment for the assets exists in the target organization. If a dependent connection or runtime environment does not exist in the target organization, during the import operation you must select a connection or runtime environment in the target organization.

When you select a connection or runtime environment in the target organization during the import, the connector type and version must be the same as the connector type and version that the asset used in the source organization.

If the target organization has connections or runtime environments with the same name as those in the export file, Informatica Intelligent Cloud Services uses the connections or runtime environments that exist in the target organization. Informatica Intelligent Cloud Services does not overwrite the connections or runtime environments in the target organization.

Note: An export or import cannot include a Cloud Hosted Agent or shared agent. If an asset uses a Cloud Hosted Agent or a shared agent, you can select a runtime environment to use for the asset during import.

Dependent objects example

You want to migrate a mapping task. The mapping task depends on the following objects:

- The connection to the source object and the runtime environment used for the connection.
- The connection to the target object and the runtime environment used for the connection.
- The mapping on which the mapping task is based.

The connections, the runtime environment, and the mapping exist in the target organization. The mapping in the source organization is an updated version of the mapping in the target organization. You configure an export that includes dependent objects so that the source organization and target organization have the same version of the mapping.

When you configure the import, you specify that you want to overwrite existing assets. For connections and runtime environments, you accept the default.

During import, Informatica Intelligent Cloud Services overwrites the mapping in the target organization with the mapping from the source organization. The imported assets use the connections and runtime environments that exist in the target.

Schedules

You can migrate schedules from one organization to another organization. You might want to migrate a schedule if you migrate an asset that uses it.

When you export an asset that uses a saved schedule, the schedule is not included in the export file.

To migrate a schedule, you export the schedule from the source organization using Administrator and import the schedule into the target organization using the service that will use the schedule. For example, to migrate a schedule that's used for Data Integration mapping tasks, you export the schedule from the source organization using Administrator and import the schedule into the target organization using Data Integration.

For information about exporting schedules, see the Administrator help. For information about importing schedules, see "Importing assets" on page 38.

Bundle objects

A bundle is a collection of reusable assets. You can migrate assets that use bundled assets.

A bundle can be copy-only, reference-only, or allow both copy and reference. Copyable bundles contain assets that you can copy and modify for your projects. When you export an asset that uses a copy of an asset from a copyable bundle, the bundle does not need to exist in the target organization.

Reference-only bundles contain assets that you cannot modify, but you can reference the assets in your projects. When you export an asset that references an asset in a bundle, both the source organization and the target organization must include the installed bundle.

For example, in the source organization, you create a mapping task that references a mapping that is in a reference-only bundle. You include the mapping task in an export file and then try to import the mapping task in the target organization. If the bundle exists in the target organization, the import is successful. If the bundle does not exist in the target organization, the import fails.

Asset export

When you export assets, Informatica Intelligent Cloud Services creates an export ZIP file that contains the assets that you selected for export.

You can select individual assets to export, or you can select an entire project or folder. When you export a project or folder, the export file includes all of the assets in the project or folder.

To export an asset, you need the following privileges and permissions:

- Your user role must have privileges to export assets.
- You must have read permission on the asset.

Note: Informatica recommends that you include no more than 1000 objects in an export file.

Export Files

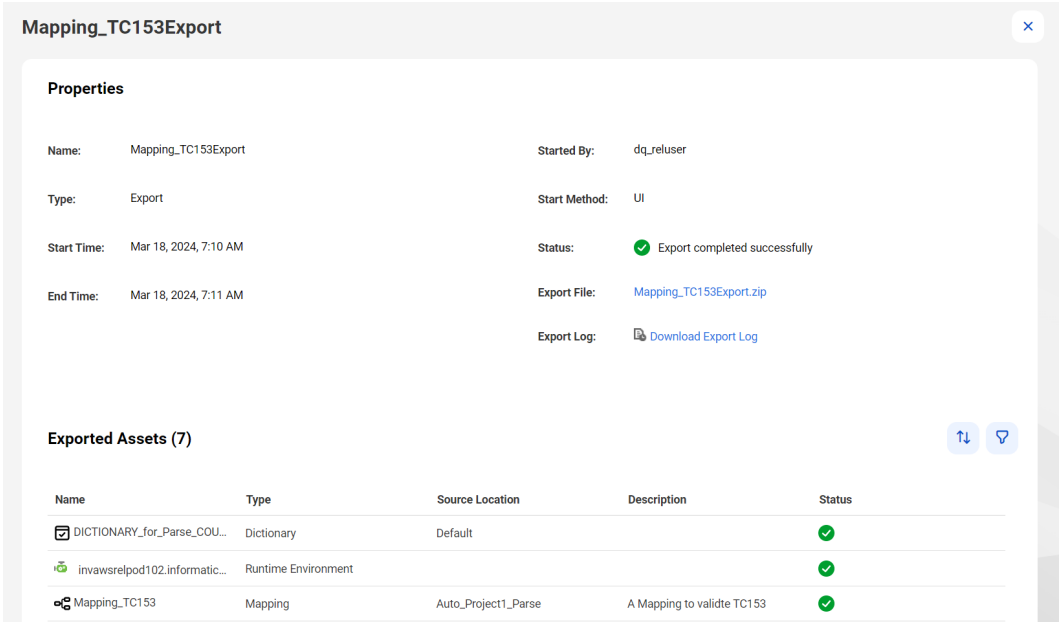
The export file retains the file structure of the source organization's **Explore** page for projects, folders, and assets. Connections and runtime environments are located in the SYS folder. The export file includes a spreadsheet that lists the objects within the file.

The following image shows a sample of an export spreadsheet:

	A	B	C	D	E
1	objectPath	objectName	objectType	id	
2	/Explore	Test_Project_4	Project	57QcqdPMFW4eq39boMcLWx	
3	/SYS	target_connection	Connection	9WLJdfmjRIPfHo4aNOOkyz	
4	/SYS	INW1PF0MPYX0	AgentGroup	0rSzCO99bA2b67GQyDRKw8	
5	/Explore	Test	Project	iW1yEvJnseDe5RLenGFpOl	
6	/Explore	Default	Project	fgMA8vWGb4Dbn3PfPTScwq	
7	/Explore/Default	test	DICTIONARY	jqk1hZpDjWMjL2gdvKwOgp	
8	/Explore/Test_Project_4	Dictionary_121	DICTIONARY	lURdE3M1tkHjDn4N7yCOY2	
9	/Explore/Suite1	rs_retrieve_city	RULE_SPECIFICATION	8V431Odtf6BclFA9vDwf2r	
10	/Explore/Default	Dictionary_232	DICTIONARY	dkVUlwIcwa3eqhAZOM0z6A	
11	/Explore/Default	Dictionary_343	DICTIONARY	9ipRiMW7I7dh2DfmCAOsQJ	
12	/Explore/Suite1	ind_phone_number_format_from_areacode_infa	DICTIONARY	aypuddMveRNcdSi8EwUeQp	

Export file structure

The following image shows the exported objects in the export notification:



Object names

Each asset is contained in a ZIP file along with its associated metadata and JSON file. The zip file includes the asset name appended by the asset type.

For example, a mapping with the name of m_totals in the source organization has the name of m_totals.DTEMPLATE in the export file. When you export the m_totals mapping to the target organization, the asset has its original name of m_totals.

The following table lists the asset types and the associated extension appended to Data Quality and Data Integration asset names:

Asset Type	Extension
Cleanse	CLEANSE
Deduplicate	DEDUPLICATE
Dictionary	DICTIONARY
Rule Specification	RULE_SPECIFICATION
Verifier	VERIFIER
Mapping	DTEMPLATE
Elastic mapping	ATSCALEDTEMPLATE
Mapping task	MTT
Replication task	DRS
Synchronization task	DSS
Masking task	DMASK
Labeler	LABELER
Linear taskflow	WORKFLOW
Parse	PARSE
PowerCenter task	PCS
Mapplet	CUSTOM_FUNC
Saved query	CUSTOM_SOURCE
Visio template	TEMPLATE
Taskflow	TASKFLOW

Exporting assets

You can select a single asset, multiple assets, or a project to export.

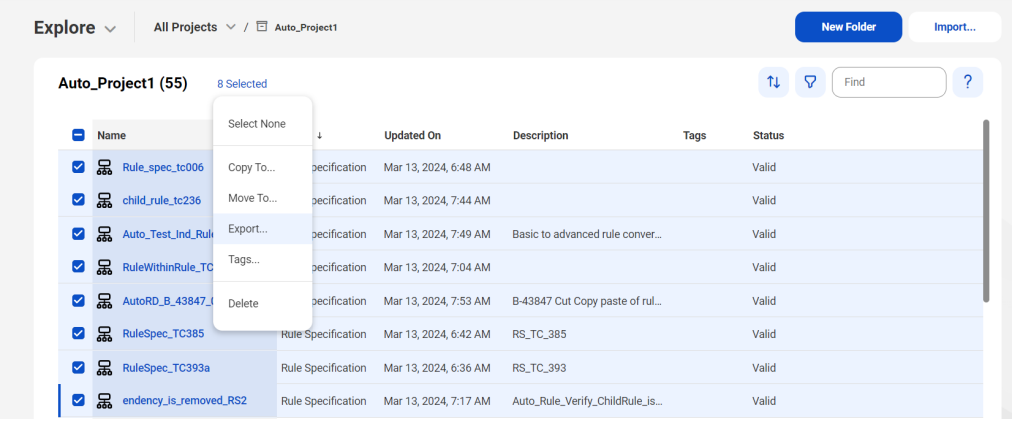
To include multiple assets, you can either select each asset within a folder or select a project or folder to export all of its assets. If you export a project, during import you can import the entire project or import only the assets that you select.

1. Log in to the source organization.
2. On the **Explore** page, navigate to the assets that you want to export.
3. Select the assets that you want to export.

To export a single asset or project, select the asset or project, and then click **Actions** and select **Export**.

To export multiple assets, select the check box to the left of each asset to export. Or, select the check box for each project or folder that contains the assets to export. From the Actions menu, select **Export**.

The following image shows the selection menu with multiple assets selected:



4. On the **Export Assets** page, change the job name or leave the default.
5. Select whether to include dependent objects for the assets.
6. Click **Export**.
7. To see the progress of the job, select **My Import/Export Logs** from the navigation bar and then select **Export** from the menu at the top of the page. Click the name of the log to open the log details page.
8. To download the export file when the job completes, on the log details page, click the export file name.

   Tip: You can quickly open the log details page for a completed export job in **Notifications**. When the export process is complete, a message appears in **Notifications**. Click the link in the message to open the log details page.

Asset import

You can import all of the assets in an export file or select the assets that you want to import.

When you import assets, you specify the following information:

- The assets in the export file that you want to import and the projects in which to import them.
- Whether to overwrite assets in the target project with assets in the export file when there is a name conflict.
- Whether to merge tags when you overwrite assets in the target project.

To import an asset, you need the following privileges and permissions:

- Your user role must have privileges to import assets.
- If you import an asset into the target project as a new asset, you must have create, update, and read permissions on the asset.
- If you overwrite an asset in the target project, you must have update and read permissions on the asset.

Note: To overwrite a source-controlled asset in the target project, the asset must be checked out.

The target organization must have all of the required licenses for the assets being imported.

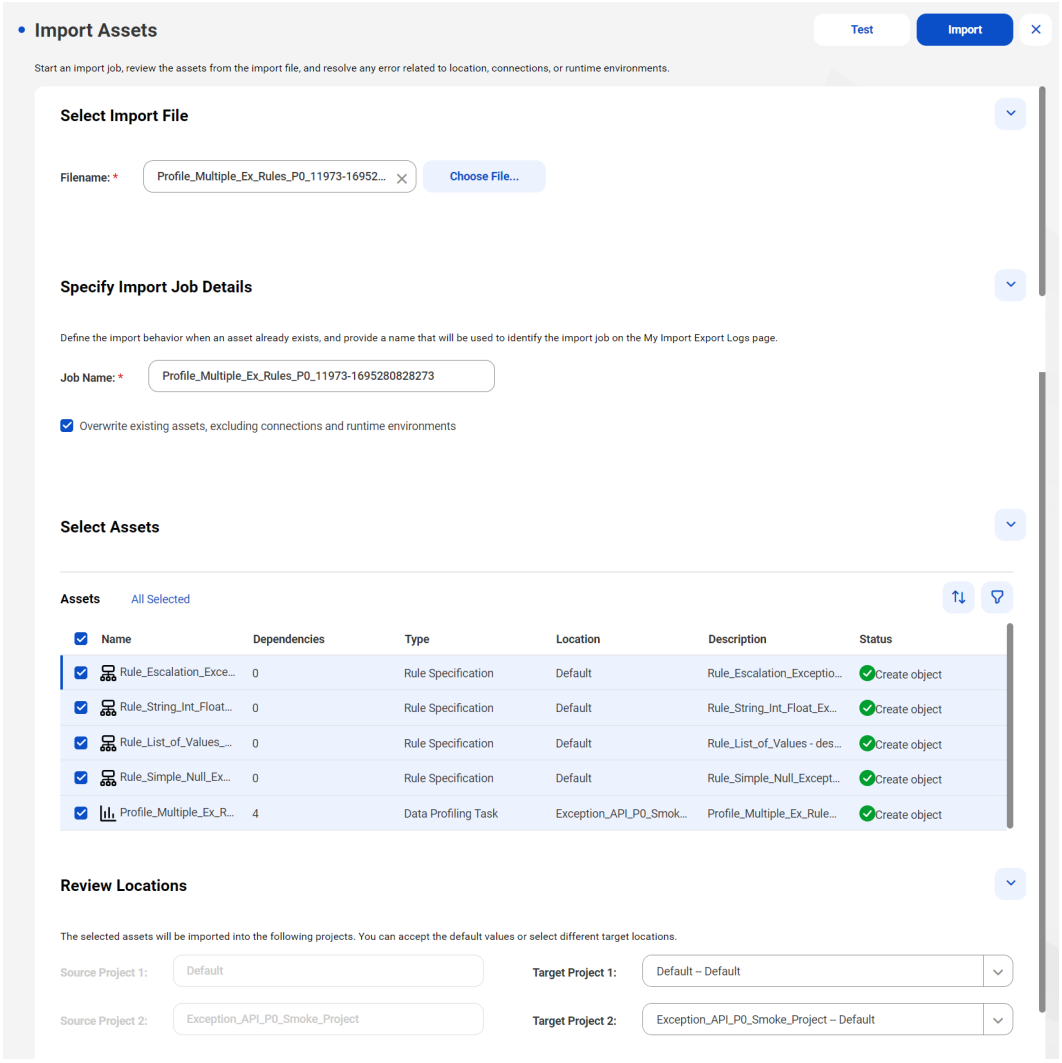
The **Import Assets** page lists the assets that are in the export file. You can select which assets you want to import, and then specify which project to import the assets to. You can accept the default project, which is the same project name as the source project, or you can select a different project. If the project does not exist in the target organization, Informatica Intelligent Cloud Services creates it.

Asset name conflicts

You can specify how Informatica Intelligent Cloud Services handles asset name conflicts when the export file contains assets with the same name as assets in the target project. You can choose whether to overwrite the assets in the target project or use the existing assets in the target project.

To see how the import handles any asset name conflicts before you start the import job, you can test the import on the **Import Assets** page before you import the assets. The import action displays in the **Status** column for each asset. You can filter the list of assets by asset name, asset type, or status.

The following image shows a list of assets and the import action to be performed when overwriting existing assets is enabled:



Importing asset tags

Asset tags are included in the export file and imported with the asset to the target project. When you overwrite existing assets, you can choose to merge tags in the target project with tags in the export file or keep only the tags in the export file.

When you import a new asset, its tags are also imported to the target project. When you overwrite existing assets in the target project, you can choose to merge tags. When you merge tags, after import, both export and target project tags are assigned to the asset.

You can choose to merge tags for all assets or for some assets in the export file. You can only merge tags when you overwrite existing assets in the target project.

If you choose to merge tags and the asset in the export file does not have tags but the asset in the target project does, after import, the asset will retain tags from the target project. To remove the target project tags, navigate to the asset on the **Explore** page and remove the tags.

The following table shows how Informatica Intelligent Cloud Services merges tags when you overwrite existing assets on import:

Asset name	Export file tags	Target project tags	Merge tags	Tags after import
Asset_1	Tag_1, Tag_2	Tag_3	Yes	Tag_1, Tag_2, Tag_3
Asset_2	Tag_1, Tag_2	Tag_4, Tag_5	No	Tag_1, Tag_2
Asset_3	Tag_1, Tag_2	-	Yes	Tag_1, Tag_2
Asset_4	-	Tag_5, Tag_6	Yes	Tag_5, Tag_6
Asset_5	-	Tag_5, Tag_6	No	Tag_5, Tag_6

Importing assets with persisted values

When you import a shared sequence or a mapping task that contains in-out parameters or sequences, you can choose to retain, reset, or overwrite persisted values.

The actions you can take for persisted values depends on whether or not the asset exists in the target project and if you choose to overwrite existing assets.

The following table describes the actions you can take when you import new assets or choose not to overwrite existing assets:

Setting	Description
Reset to default values	Default. Informatica Intelligent Cloud Services creates a new asset in the target location with default in-out parameter values and initial sequence values.
Retain persisted values	Informatica Intelligent Cloud Services creates a new asset with the persisted in-out parameter and sequence values .

The following table describes the actions you can take when you overwrite existing assets:

Setting	Description
Retain persisted values in the target	Default. Informatica Intelligent Cloud Services ignores values coming from the export file and retains the values persisted in the target project.
Reset persisted values to default values	Informatica Intelligent Cloud Services resets persisted values to the default in-out parameter value and initial sequence value.
Overwrite persisted values in the target with source values	Informatica Intelligent Cloud Services overwrites values in the target with persisted values in the export file.

Importing assets

Import assets from an Informatica Intelligent Cloud Services export file.

1. Log in to the target organization.
2. On the **Explore** page, navigate to **All Projects** and click **Import**.
3. On the **Import Assets** page, navigate to the export file and click **Open**, or drag the zip file from the Downloads folder in Windows.

   The **Import Assets** page lists the assets in the file.
4. Optionally, change the import job name.
5. Choose whether to overwrite existing assets with the assets in the import.
   - If you choose to overwrite existing assets, when an asset has the same name as an asset in the target project, the asset replaces the existing asset in the target project.
   - If you do not choose this option, if an asset with the same name exists in the target project, the asset is not imported.
6. Select the assets to import.

   If the export file contains a project and you want to import the entire project, select all of the assets. Informatica Intelligent Cloud Services creates the project in the target organization.
7. Select the target project or accept the default.
8. Click **Test** to see the potential results of the import.

   In the Select Assets area, the status for each asset shows the action that the service performs when you import the files.
9. If necessary, revise your selections to resolve any issues in the test results.
10. Click **Import**.

    You can see the progress of the import on the **Import** tab of the **My Import/Export Logs** page. When the import process is complete, a message appears in **Notifications**. Click the link in the message to open the log details page and see the results of the import.

Post-import tasks

To complete the migration process you need to perform certain tasks based on the types of assets that you imported.

Perform the following tasks after you import assets:

- Configure connection passwords and security tokens. Informatica Intelligent Cloud Services does not include connection passwords and security tokens in imports for security reasons.

CHAPTER 4

Bundles

A bundle is a set of Informatica Intelligent Cloud Services assets that you can use to improve productivity and enhance the quality of your Informatica Intelligent Cloud Services projects. You can create a bundle and share it with others in your organization, or use the contents of a bundle that someone else created instead of creating assets that already exist.

A bundle can be one of the following types:

- A public bundle is available to any Informatica Intelligent Cloud Services organization.
- A private bundle is created by a parent organization and published to sub-organizations.
- An unlisted bundle is available to use if you have a bundle access code from the bundle publisher.

Before you can use a public or unlisted bundle, an administrator must install it so that it is available to your organization. You can find installed bundles in the Add-on Bundles project on the **Explore** page. For information on installing bundles, see *Bundle Management* in the Administrator help.

If your organization has the Publish Content license, you can create and publish bundles. You might want to create a bundle when you have created a set of assets that can be reused for a common purpose. By creating the bundle, you allow users in other organizations to use the assets for their projects.

Note: You cannot apply source control to bundles.

Using bundles

Use the assets in a bundle when the assets are designed to meet the same objectives as your project.

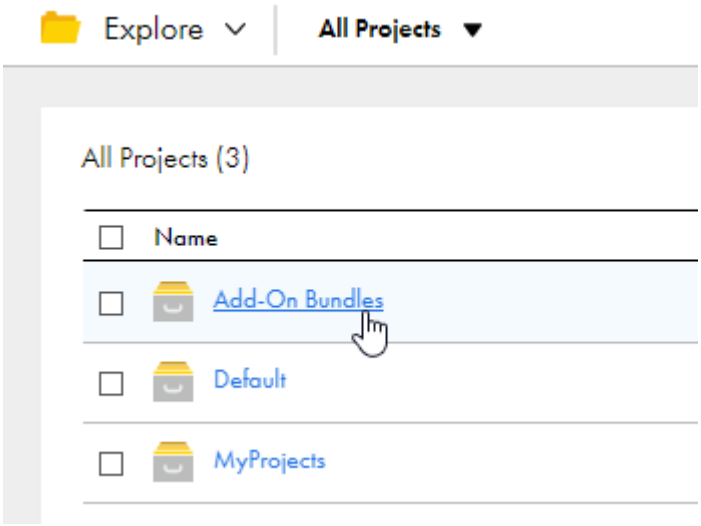
How you can include bundle assets in your project depends on the permissions that the bundle designer designates for the bundle. You can perform one of the following actions depending on which option the bundle designer allows:

- Copy the bundle assets to your project folder and edit the assets for your project. Bundles that allow copy only can be located in any project folder.
- Reference the bundle assets. Select the assets from the Add-on Bundles project when you configure a task. You cannot change a bundle that only allows reference. Bundles that allow reference only are always located in the Add-on Bundles project.
- Copy or reference the bundle assets. Either copy the bundle assets to your project folder or reference the bundle assets in the Add-on Bundles project. Bundles that allow reference or copy are always located in the Add-on Bundles project.

Copying bundle assets

If a bundle allows the copy action, you can copy all of the assets in a bundle to a project or folder.

1. On the **Explore** page, explore by projects and navigate to the **Add-On Bundles** folder.



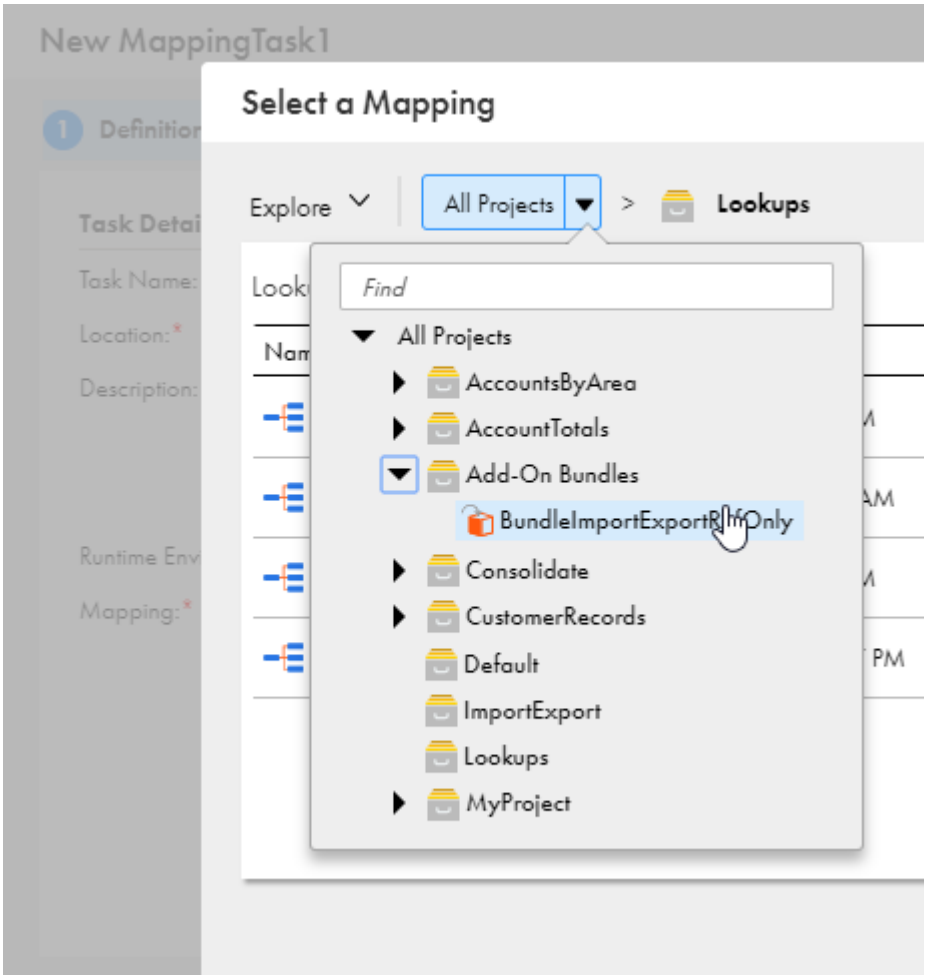
2. Open the **Add-On Bundles** folder.
3. In the row that contains the bundle, click **Actions** and select **Copy Bundle Content To**.
4. Browse to the folder to contain the bundle assets and click **Select**.

Referencing bundle assets

Certain asset types allow you to select an asset to use in the asset. If a bundle allows the reference action, you can select the assets in the bundle to use in your asset.

Add a reference to a bundle asset when you configure a mapplet or a mapping in Data Integration.

1. Click **Select** in the asset that you're working on, and then navigate to the Add-On Bundles folder.



2. Open the bundle folder that contains the asset you want to use.
3. Click the row that contains the asset, and then click **Select**.

Creating and publishing bundles

If your organization has the Publish Content license, you can create bundles to share assets with other organizations.

When you create a bundle, you specify the bundle type. The bundle type determines who can use the bundle and also determines how the bundle is published.

You can create the following types of bundles:

Public bundles

A public bundle is available to all Informatica Intelligent Cloud Services 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 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.

After you publish a private bundle, you can push the bundle to all of the sub-organizations. When you push a private bundle, you install the bundle on all sub-organizations.

The Informatica review team does not review private bundles.

Note: If a pushed bundle contains objects with changes that are incompatible with existing sub-organization tasks, it might cause the sub-organization tasks to become invalid or be removed.

If your organization does not have any sub-organizations, the option to create a private bundle is not available.

Unlisted bundles

An unlisted bundle is similar to a public bundle. However, only users who have the bundle access code have access to the bundle. When you create an unlisted bundle, Informatica Intelligent Cloud Services generates a bundle access code. The review team does not review unlisted bundles.

When you create a bundle, you specify how users can use the bundle assets. You can allow users to use bundle assets in one of the following ways:

Copy bundle assets

With this option, users can copy bundle assets to their projects and edit the assets.

Reference bundle assets

With this option, users can use bundle assets in tasks but they cannot copy or edit the bundle assets.

Copy or reference bundle assets

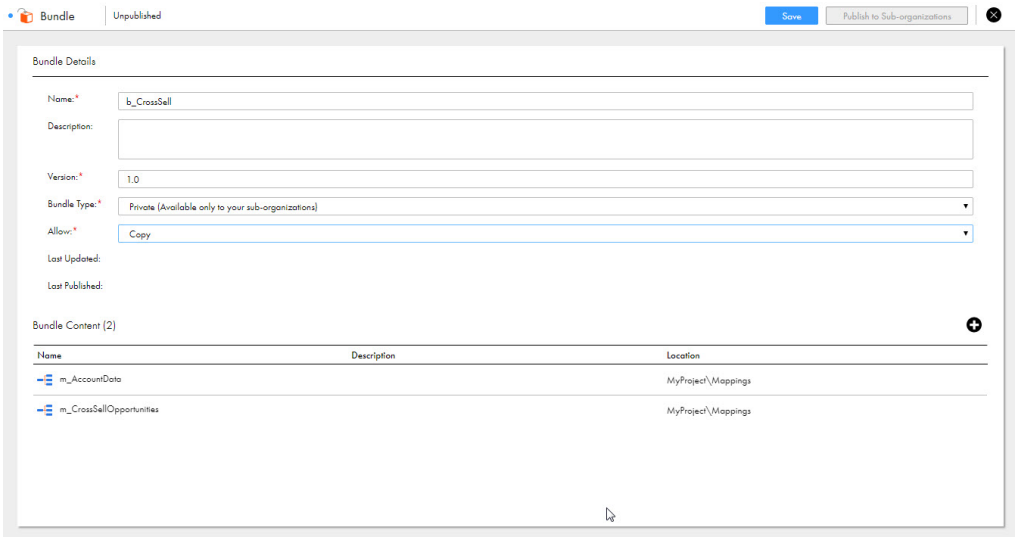
With this option, users can either copy and edit bundle assets or reference bundle assets in tasks.

Creating a bundle

Create a bundle to share assets with other organizations.

Before you create a bundle, put all of the assets that you want to include in the same folder. This helps to ensure that the bundle is versioned correctly if any of the assets are modified.

1. Click **Bundles** > **New Bundle**.



2. Configure the following details:

Bundle Property	Description
Name	Name of the bundle. Bundle names must be unique across all organizations.
Description	Optional description of the bundle.
Version	Version number of the bundle. The initial version number defaults to 1.0. The new version number must be greater than the current version in the format #.#, for example, 1.2.
Bundle Type	Select the bundle type that you want to publish: - Public. Available to all organizations after the bundle is approved by the Informatica Intelligent Cloud Services review team. - Private. Available to publish or push to from a parent organization to its sub-organizations. - Unlisted. Available to users who have a valid bundle access code.
Allow	Select one of the following options: - Reference. Allows others to select the assets in the bundle to use in their projects. The assets remain in the bundle folder and cannot be edited. - Copy. Allows others to copy and edit the assets in the bundle. - Reference and Copy.

3. To add assets to the bundle, in the Bundle Content list, click **Add** and select an asset that you want to include. You can select any asset with a Valid status.

   Repeat this step until you have selected all of the assets for the bundle.

4. Click **Save**.

5. When the bundle is complete, you can choose one of the following options based on the bundle type:

- For a public bundle, click **Submit for Review**.
  After you submit a bundle for review, you can remove it from the review queue by clicking **Withdraw from Review**.
- For a private bundle, click **Publish to Sub-organizations**.
- For an unlisted bundle, click **Publish**.
  Informatica Intelligent Cloud Services generates an access code for the bundle. For more information about generating access codes, see "Generating a bundle access code" on page 45.

After you create a bundle, you can open the saved bundle and edit the bundle contents at any time, unless you are awaiting review and approval by Informatica. After a bundle is published, you must update the version number to save the changes.

Submitting a public bundle for review

You can submit a public bundle to Informatica for approval when you are satisfied with the bundle design. The Informatica Intelligent Cloud Services team reviews the bundle and responds to you by email.

You cannot edit the bundle until the review team completes the review or you withdraw your review request.

1. To submit a bundle, click **Bundles** and open the bundle.
2. Click **Submit for Review**.
3. Create a support ticket with Informatica Global Customer Support to provide additional details about the bundle.

   The support ticket must describe the bundle use case in detail and include documentation on how to use the bundle contents. Bundles submitted without this documentation cannot be approved.

After the bundle is submitted for review, you can cancel the review before the bundle is approved. To cancel the review, open the bundle and click **Withdraw from Review**. If desired, you can edit the withdrawn bundle and send it for review again.
After the bundle is approved, the Informatica Intelligent Cloud Services team publishes the bundle so that it is available to all Informatica Intelligent Cloud Services organizations.

Sharing a private bundle

When you work in a parent organization, you can share a private bundle with sub-organizations. After you publish a private bundle, the bundle is available for sub-organizations to install. You can also push a published private bundle to install the bundle on all sub-organizations.

Note: If a published bundle contains asset changes that are incompatible with existing sub-organization tasks, it might cause those tasks to become unavailable. For example, in Data Integration, adding a new parameter in a mapping could invalidate the existing task when a new bundle is published.

1. Click **Bundles** and open the bundle.
2. Perform one of the following steps:
   - To publish a private bundle, click **Publish to Sub-organizations**.
   - To push a published private bundle, click **Push to Sub-organizations**.

Generating a bundle access code

Use a bundle access code to share a published unlisted bundle with other organizations.

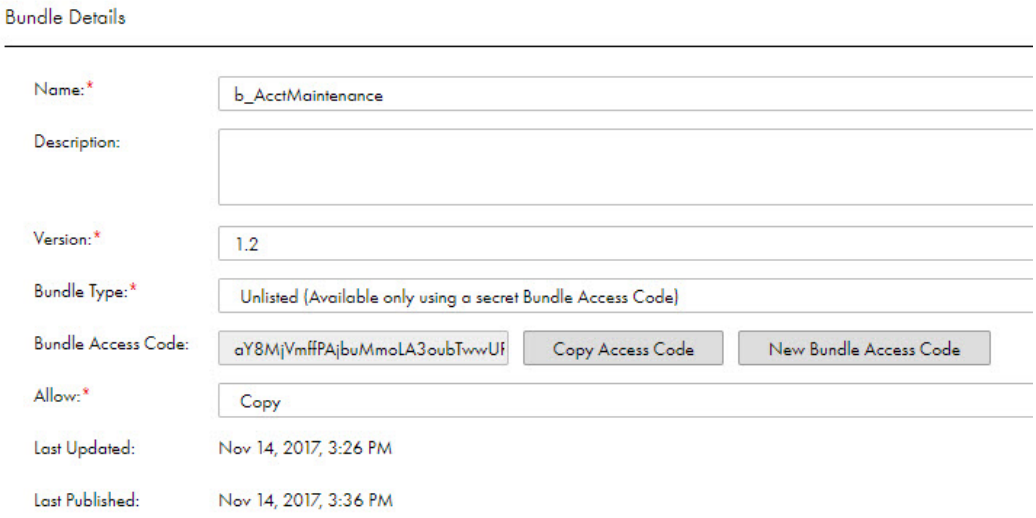
When you publish an unlisted bundle, Informatica Intelligent Cloud Services provides a system-generated bundle access code. You can give the bundle access code to users in other organizations. With the bundle

access code, a user can view and install the unlisted bundle. When a user installs the unlisted bundle, the bundle becomes usable in the organization like other bundles.

To see the bundle access code, open the bundle from the **Bundles** page. The bundle access code displays in the Bundle Details area.

The bundle access code is reusable so you can use a single code to share an unlisted bundle with multiple organizations. You can generate a new access code at any time, which invalidates the previous bundle access code.

1. Click **Bundles** and open the bundle.
2. To generate an access code, click **New Bundle Access Code**.



Deprecating a bundle

If a bundle is outdated, you can deprecate the bundle so that it is no longer available to other organizations.

When you deprecate a bundle, organizations that have installed the bundle can continue using the bundle. Organizations that have not installed the bundle cannot see it listed as available to install.

Note: If the bundle is published, only the bundle approver can deprecate the bundle.

1. Click **Bundles** and open the bundle.
2. Click **Deprecate**.

Deleting a bundle

You can delete a private or unlisted bundle when the bundle's status is Deprecated.

You can delete an unpublished public bundle if the bundle status is Unpublished or Withdrawn. If a public bundle is published, the bundle approver must deprecate the bundle before you can delete it.

When you delete a bundle, it no longer appears on the **Bundles** page.

1. Click **Bundles**.
2. In the row that contains the bundle, click **Actions** and select **Delete**.

INDEX

A

asset name conflicts
  importing 36
assets
  assigning tags 12
  copying 7
  creating tags 11
  deleting 9
  exporting 32, 34
  importing 35, 38
  migrating between organizations 30
  migration requirements 30
  moving 8
  renaming 8
  source control 19
  tags 10
Azure DevOps user credentials 20

B

Bitbucket user credentials 20
bundle access code
  for unlisted bundles 45
bundles
  bundle access code for unlisted bundles 45
  bundle types 42
  copying contents 41
  creating 44
  creating and publishing 42
  deleting 46
  deprecating 46
  editing 44
  installing private bundles in sub-organizations 45
  overview 40
  publication process 42
  publishing private bundles 45
  publishing public bundles 45
  pushing private bundles to sub-organizations 45
  referencing assets 42
  submitting for approval 45
  using 40
  withdrawing from review 45

C

Cloud Application Integration community
  URL 5
Cloud Developer community
  URL 5
connections
  importing 35
  migrating 31
copying
  assets 7
  bundle assets 41
  folders 7
  projects 7
creating
  tags 11

D

Data Integration community
  URL 5
deleting
  assets 9
  bundles 46
  folders 9
  projects 9
  tags 13
dependencies
  viewing dependencies 14
dependent objects
  in export files 30
  runtime environments and connections 31

E

editing
  tags 13
Explore page
  source control columns 27
  tags 10
exporting
  assets 32, 34
  bundle objects 32
  dependent objects 30
  export file 33
  projects 34
exporting assets
  overview 30
  requirements 30

F

folders
  copying 7
  deleting 9
  importing 38
  moving 8

G

GitHub user credentials 20

I

importing
  asset name conflicts 36
  assets 35
  bundle objects 32
  connections 35
  dependent objects 30
  name conflicts 35
  post-migration tasks 39
  projects 35
importing assets
  overview 30
  requirements 30
Informatica Global Customer Support
  contact information 6
Informatica Intelligent Cloud Services
  web site 5

M

maintenance outages 6
mapping tasks
  using bundles 40
migrating
  assets 34
migration
  assets 38
  of assets between organizations 30
moving
  assets and folders 8

O

object migration 30

P

permissions
  best practices 16
  configuring for objects 17
  for copied assets 15
  for imported assets 15
  overview 15
  permission descriptions 15
  rules and guidelines 16
projects
  copying 7
  deleting 9
  exporting 34
  importing 35, 38
publishing
  public bundles 45

R

referencing bundle assets 42
renaming
  assets 8
renaming *(continued)*
  folders 8
  projects 8
runtime environments
  migrating 31

S

schedules
  migrating 32
scheduling
  copying tasks and taskflows 7
source control
  actions 19
  best practices 28
  checking in and checking out objects 24
  checking in objects 25
  checking out objects 24
  configuring access to the repository 20
  deleting objects 25
  Explore page columns 27
  Git commands 20
  project-level repositories 21
  pulling objects 22
  pulling objects from the repository 23
  pulling projects and folders 22
  reverting to previous versions 25
  selecting multiple objects 26
  supported objects 19
  supported source control systems 19
  undoing a checkout 26
  unlinking objects 26
  updating organization with repository versions 22
status
  Informatica Intelligent Cloud Services 6
system status 6

T

tags
  assigning 12
  creating 11
  deleting 13
  editing 13
  importing 37
  properties 13
tasks
  deleting 9
trust site
  description 6

U

upgrade notifications 6

W

web site 5