Informatica® Cloud Data Quality
July 2024

Getting Started

Informatica Cloud Data Quality Getting Started
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 4

Informatica Resources 4

- Informatica Documentation 4
- Informatica Intelligent Cloud Services web site 4
- Informatica Intelligent Cloud Services Communities 4
- Informatica Intelligent Cloud Services Marketplace 4
- Informatica Knowledge Base 5
- Informatica Intelligent Cloud Services Trust Center 5
- Informatica Global Customer Support 5

Chapter 1: Getting started with Data Quality 6

Chapter 2: Installing Secure Agents 8

Secure Agent installation on Windows 8

- Secure Agent requirements on Windows 8
- Downloading and installing the Secure Agent on Windows 9
- Configure the proxy settings on Windows 11
- Configure a login for a Windows Secure Agent Service 11

Secure Agent installation on Linux 12

- Secure Agent requirements on Linux 12
- Downloading and installing the Secure Agent on Linux 13
- Configure the proxy settings on Linux 15

Chapter 3: Project setup 17

Creating projects and project folders 17

Creating assets 18

Chapter 4: Editing your user profile 19

Chapter 5: Switching to a different organization 20

Index 21

Preface

Refer to *Getting Started* to learn how to begin to use Informatica Intelligent Cloud Services ℠ Data Quality. Learn how to verify the runtime environment, create projects and project folders, and configure your user profile.

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

Getting started with Data Quality

You can create a data quality project in a few steps.

Step 1. Check system requirements

Be sure you're using a compatible browser when you're designing your projects. Check the Informatica Intelligent Cloud Services Product Availability Matrix for operating systems, databases, and other systems that Data Quality supports.

Step 2. Verify the runtime environment

A runtime environment is the execution platform for running tasks. A runtime environment consists of one or more Secure Agents. A Secure Agent is a lightweight program that runs tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. You must have at least one runtime environment in each organization so that users in the organization can run tasks.

You can use the following types of runtime environment:

Informatica Cloud Hosted Agent

When you want to access data in an SaaS environment, you can use the Informatica Cloud Hosted Agent. The Hosted Agent runs within the Informatica Intelligent Cloud Services hosting facility, so there is nothing to install.

The Hosted Agent can run synchronization, mapping, and replication tasks that use certain connectors. To find out if the connector that you use supports the Hosted Agent, see the help for the relevant connector.

Secure Agent Groups

When you need to access data on-premises or when you want to access SaaS data without using the Hosted Agent, use a Secure Agent group. A Secure Agent group contains one or more Secure Agents. The agents in a group run within your network or in a cloud computing services environment such as Amazon Web Services or Microsoft Azure.

To create a Secure Agent group, download and install the Secure Agent. You can install one Secure Agent on each physical or virtual machine. Each agent that you install is added to its own group by default. You can add multiple agents to a group to balance workloads and improve scalability.

You can associate a Secure Agent with an advanced cluster, which is a Kubernetes cluster that provides a distributed processing environment on the cloud. Fully-managed and self-service clusters can run data logic using a scalable architecture, while local clusters use a single node to quickly onboard projects for advanced use cases.

Serverless runtime environment

A serverless runtime environment is an advanced serverless deployment solution that doesn't require downloading, installing, configuring, and maintaining a Secure Agent or Secure Agent group.

Compared to the multi-tenant model on the Hosted Agent, a serverless runtime environment uses an isolated, single-tenant model that provides a dedicated server with virtual machine resources to run tasks. The serverless runtime environment auto-scales with the size of the workload while your data remains in your cloud environment.

Step 3. Verify a connection

When you use Data Integration to run mappings with data quality assets, you need to use a connection. A connection specifies the connector that enables the exchange of data between Data Integration and the source and target objects. For example, if you want to create a task that uses Salesforce data, you create a Salesforce connection. The Salesforce connection uses the Salesforce connector which enables the exchange of data between Salesforce and Data Integration.

Note: For information about how to configure Secure Agents and connections, see the Data Integration online help.

Step 4. Create your project

Organize your data quality projects in folders that can contain the rule specifications, dictionaries, and verifiers that you create.

After you set up folders, create your project assets.

Step 5. Add your project to the source control repository (optional)

If your organization is enabled for source control and the organization has read-write access to the source control repository, add your project to the repository.

Before you can add your project, your organization administrator must configure a link between the organization and source control repository, and you must specify your source control user credentials in Informatica Intelligent Cloud Services.

Step 6. Configure reference data properties

When you run a mapping that uses a verifier or a deduplicate asset, the Secure Agent checks for the presence of the reference data files that the asset reads and downloads any file that is absent in the runtime environment.

Before you run a mapping that reads a verifier asset, enter the license keys for the reference data that the mapping reads. You enter the license keys as runtime environment properties in the Administrator service. You do not need to take additional steps to download and install the reference data files for a verifier or deduplicate asset.

You can review and update the properties that relate to the reference data in the Administrator service.

CHAPTER 2

Installing Secure Agents

You can install Secure Agents on Windows or Linux.

Secure Agent installation on Windows

On Windows, the Secure Agent runs as a Windows service. When you install the Secure Agent, you also install the Informatica Cloud Secure Agent Manager.

By default, the Secure Agent starts when you start Windows. You can stop and restart the Secure Agent using the Secure Agent Manager or Windows Services. If you install the Secure Agent on a different volume than you use to run the installation program, you must start and stop the Secure Agent from Windows Services.

You can also use the Secure Agent Manager to check the Secure Agent status and configure proxy information. The Secure Agent works with BASIC, DIGEST, and NTLMv2 proxy authentication.

You can launch the Secure Agent Manager from the Start menu or desktop icon. When you close the Secure Agent Manager, it minimizes to the Windows taskbar notification area for quick access.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.
2. Download the Secure Agent installer files.
3. Install and register the Secure Agent.

Secure Agent requirements on Windows

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services.

Verify the following requirements before you install the Secure Agent on Windows:

- The Secure Agent machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on the Knowledge Base.
- The Secure Agent machine has the Microsoft Visual C++ 2015 Redistributable.
- The Secure Agent machine has at least 4 CPU cores, 16 GB RAM, and at least 5 GB of free disk space.
- The Secure Agent machine is on a volume with at least 250GB disk space, with at least 5 GB free space or three times the size of the Secure Agent installation, whichever is greater.
- The account you use to install the Secure Agent has access to all remote directories that contain flat source or target files.

- No other Secure Agent is installed on the machine. If another Secure Agent is installed on the machine, uninstall it first.

For more information about Secure Agent requirements, see this article: https://knowledge.informatica.com/s/article/526096

Configure the firewall

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

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking on the Documentation Portal or click the link at the top of the **Runtime Environments** page in Administrator.

Secure Agent permissions on Windows

A Secure Agent requires certain permissions to transfer data between sources and targets.

When you install a Secure Agent on Windows, the Secure Agent must be part of the local Administrators group.

Configure Windows settings

Before you use the Secure Agent on Windows, configure proxy settings and a Windows Secure Agent service login.

You can configure proxy settings in Secure Agent Manager. Configure a login for the Windows Secure Agent service on Windows.

Note: If you use the Secure Agent for Informatica Cloud Data Wizard, you do not need to configure proxy settings or a Windows service login for the Secure Agent.

Downloading and installing the Secure Agent on Windows

To install the Secure Agent on a Windows machine, you must download and run the Secure Agent installation program and then register the agent.

Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine. If any other Secure Agent exists, you must uninstall it.

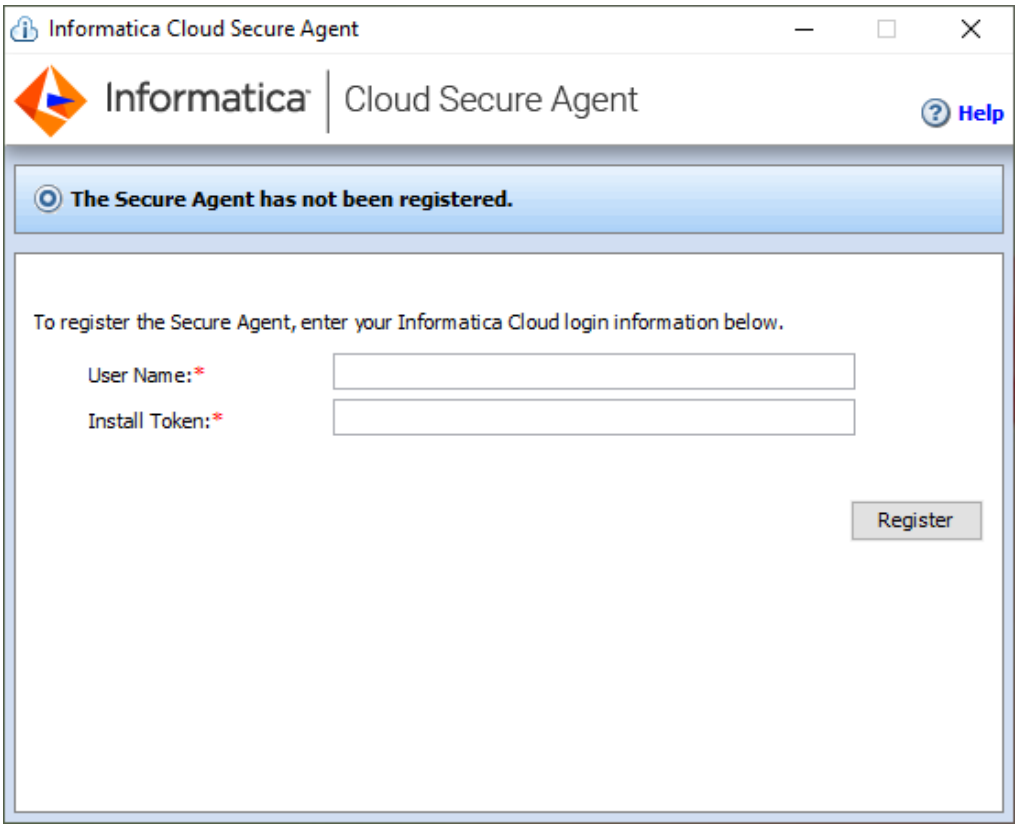
Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.

2. On the **Runtime Environments** page, click **Download Secure Agent**.
3. Select the Windows 64-bit operating system platform, copy the install token, and then click **Download**.

   The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.exe`.
4. Run the installation program as an Administrator:
   a. Specify the Secure Agent installation directory, and click **Next**.
   b. Click **Install** to install the agent.

   The **Cloud Secure Agent** dialog box opens and prompts you to register the agent as shown in the following image:



5. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.
6. In the Secure Agent Manager, enter the following information, and then click **Register**:

Option	Description
User Name	User name that you use to access Informatica Intelligent Cloud Services.
Install Token	Token that you copied.

   The Secure Agent Manager displays the status of the Secure Agent. It takes a minute for all of the services to start.

7. If your organization uses an outgoing proxy server to connect to the internet, enter the proxy server information.

8. Close the Secure Agent Manager.

   The Secure Agent Manager minimizes to the taskbar and continues to run as a service until stopped.

Configure the proxy settings on Windows

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server. The Secure Agent installer configures the proxy server settings for the Secure Agent based on settings configured in the browser. You can change the proxy server settings through the Secure Agent Manager.

Contact your network administrator for the correct proxy settings.

1. In the Secure Agent Manager, click **Proxy**.
2. To enter proxy server settings, click **Use a Proxy Server**.
3. Enter the following information:

Field	Description
Proxy Host	Required. Host name of the outgoing proxy server that the Secure Agent uses.
Proxy Port	Required. Port number of the outgoing proxy server.
User Name	User name to connect to the outgoing proxy server.
Password	Password to connect to the outgoing proxy server.

4. Click **OK**.

   The Secure Agent Manager restarts the Secure Agent to apply the settings.

Configure a login for a Windows Secure Agent Service

On Windows, configure a network login for the Secure Agent service. The Secure Agent can access the network with the privileges and permissions associated with the login.

Configure a login for the Secure Agent machine to allow the Secure Agent to access directories to configure and run tasks. When you configure connections, configure tasks, and run tasks that use flat file or FTP/SFTP connection types, the Secure Agent might require read and write permissions on the related directories.

For example, to browse to a directory to configure a flat file or FTP/SFTP connection, the Secure Agent login might require permission to access the directory. Without a Secure Agent login with the appropriate permissions, Informatica Intelligent Cloud Services cannot display the directory in the **Browse for Directory** dialog box.

1. Go to the **Services** window from the Windows Administrative tools.
2. In the **Services** window, right-click the Informatica Cloud Secure Agent service and choose **Properties**.
3. In the **Properties** dialog box, click the **Log On** tab.
4. To configure a login, select **This Account**.
5. Enter an account and password.

   Use an account with the required privileges and permissions for the network security defined for the domain. By default, the account format is <domain name>\<user name>.
6. Click **OK**.

7. In the **Services** window, restart the Secure Agent service for the changes to take effect.

Secure Agent installation on Linux

On Linux, the Secure Agent runs as a process. You can use a shell command line to install, register, start, stop, and uninstall the Secure Agent.

You can also use the shell command line to check the Secure Agent status.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.
2. Download the Secure Agent installer files.
3. Install and register the Secure Agent.

Consider the following guidelines:

- Create a specific user profile to install the Secure Agent with full access to all folders from the Secure Agent installation directory. Don't install the Secure Agent as the root user.
- You can't install more than one Secure Agent on the same machine under the same user account. Multiple agents may exist under different user accounts.
- Don't install the Secure Agent on any node within the Informatica domain.

For more information about Secure Agent requirements, see this KB article:
IICS Minimum requirements and best practices when installing Informatica Cloud Secure Agent.

Secure Agent requirements on Linux

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services. Before you install the Secure Agent on Linux, verify the system requirements.

Verify the following requirements before you install the Secure Agent on Linux:

- Verify that the machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on the Knowledge Base.
- Verify that the machine has at least 11 GB free disk space.
- Verify that the `libidn.x86_64` package is installed.
  If the package isn't present, install it using the following command: `sudo yum install libidn.x86_64`

  Note: The command to install the package might vary based on your Linux distribution.
- Verify that the `libidn.so.*` libraries are installed.
  If the libraries aren't present, install them using the following commands:

  - For 64-bit systems: `cd /usr/lib/x86_64-linux-gnu`
  - For 32-bit systems: `cd /usr/lib/i386-linux-gnu`

  After installing the libraries, create a symbolic link using the following command:

  ```
  sudo ln -s libidn.so.12 libidn.so.11
  ```

- If you are installing the Secure Agent on RHEL 9, verify that the `libnsl` library is installed.
  If the library isn't present, install it using the following command: `sudo yum install libnsl`

Note: The command to install the package might vary based on your Linux distribution.

To verify whether `libnsl` is present, use one of the following commands: `ldconfig -p | grep libnsl` or `which libnsl`.

- The account that you use to install the Secure Agent must have access to all remote directories that contain flat source or target files.
- If you use PowerCenter, install the Secure Agent using a different user account than the account you used to install PowerCenter.
  Informatica Intelligent Cloud Services and PowerCenter use some common environment variables. If the environment variables are not set correctly for Informatica Intelligent Cloud Services, your jobs might fail at run time.

For more information about Secure Agent requirements, see this article:
https://knowledge.informatica.com/s/article/526096

Configure the firewall

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

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking on the Documentation Portal or click the link at the top of the **Runtime Environments** page in Administrator.

Secure Agent permissions on Linux

A Secure Agent requires certain permissions to transfer data between sources and targets.

When you install a Secure Agent on Linux, the Secure Agent must have read/write/execute permissions for the installation directory.

Downloading and installing the Secure Agent on Linux

To install the Secure Agent on a Linux machine, you must download and run the Secure Agent installation program and then register the agent.

Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

When you register the agent, it is added to its own Secure Agent group by default. You can add the agent to a different Secure Agent group.

Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine using the same Linux user account. If there is, you must uninstall it.

Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Download Secure Agent**.
3. Select the Linux 64-bit operating system platform, copy the install token, and then click **Download**.

   The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.bin`.
4. Save the installation program to a directory on the machine where you want to run the Secure Agent.

   Note: If the file path contains spaces, the installation might fail.
5. From a shell command line, navigate to the directory where you downloaded the installation program and enter the following command:

   ```
   ./agent64_install_ng_ext.bin -i console
   ```
6. When the installer completes, navigate to the following directory:

   ```
   <Secure Agent installation directory>/apps/agentcore
   ```
7. To start the Secure Agent, enter the following command:

   ```
   ./infaagent startup
   ```

   The Secure Agent Manager starts. You must register the agent using the user name that you use to access Informatica Intelligent Cloud Services. You must also supply the install token.
8. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.
9. To register the agent, in the `<Secure Agent installation directory>/apps/agentcore` directory, enter one of the following commands using your Informatica Intelligent Cloud Services user name and the token that you copied:
   - To add the agent to its own Secure Agent group, use the following command:

     ```
     ./consoleAgentManager.sh configureToken <user name> <install token>
     ```
   - To add the agent to an existing Secure Agent group, use the following command:

     ```
     ./consoleAgentManager.sh configureTokenWithRuntime <user name> <install token>
     <Secure Agent group name>
     ```

     Note: If the command includes a Secure Agent group name that doesn't exist, the Secure Agent is not assigned to a group. Be sure to use a valid Secure Agent group name.

   The following table lists the command options:

Option	Description
User Name	Required. Informatica Intelligent Cloud Services user name of the user installing the Secure Agent.
Install Token	Required. The install token that you copied.
Secure Agent group name	Optional. Include when you want to add the agent to an existing Secure Agent group instead. If this option isn't included in the command, the agent will be in its own Secure Agent group.

   You can check the registration status of a Secure Agent using the following command:

   ```
   ./consoleAgentManager.sh isConfigured
   ```

Configure the proxy settings on Linux

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server. The Secure Agent installer configures the proxy server settings for the Secure Agent based on settings configured in the browser. Update the proxy server settings from the command line and in the Administrator service.

1. Open a command prompt and navigate to the following directory:

   ```
   <Secure Agent installation directory>/apps/agentcore
   ```

2. Use a shell command that updates the `proxy.ini` file. Contact the network administrator to determine the proxy settings.

   Use the following command to update the `proxy.ini` file:

   ```
   ./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name>
   <proxy password>
   ```

3. Log in to Informatica Intelligent Cloud Services.
4. Open the Administrator Service and select **Runtime Environments**.
5. Select the Secure Agent for which you want to configure a proxy server.
6. On the upper-right corner of the page, click **Edit**.
7. In the **System Configuration Details** section, set the **Service** property to **Data Integration Server** and set the **Type** property to DTM.
8. Add the parameters that you require to any available **JVMOption** field and specify appropriate values for each parameter.

   The following table describes the parameters that you can add:

Parameter	Description
-Dhttp.proxyHost=	Host name of the outgoing HTTP proxy server.
-Dhttp.proxyPort=	Port number of the outgoing HTTP proxy server.
-Dhttp.proxyUser=	Authenticated user name for the HTTP proxy server. This is required if the proxy server requires authentication.
-Dhttp.proxyPassword=	Password for the authenticated user. This is required if the proxy server requires authentication.
-Dhttps.proxyHost=	Host name of the outgoing HTTPS proxy server.
-Dhttps.proxyPort=	Port number of the outgoing HTTPS proxy server.
-Dhttps.proxyUser=	Authenticated user name for the HTTPS proxy server. This is required if the proxy server requires authentication.
-Dhttps.proxyPassword=	Password for the authenticated user. This is required if the proxy server requires authentication.

   Example for HTTP:

   ```
   JVMOption1=-Dhttp.proxyHost=<proxy_server_hostname>
   JVMOption2=-Dhttp.proxyPort=8081
   JVMOption3=-Dhttp.proxyUser=<proxy_user_name>
   JVMOption4=-Dhttp.proxyPassword=<proxy_password>
   ```

Example for HTTPS:

```
JVMOption1=-Dhttps.proxyHost=<proxy_server_hostname>
JVMOption2=-Dhttps.proxyPort=8081
JVMOption3=-Dhttps.proxyUser=<proxy_user_name>
JVMOption4=-Dhttps.proxyPassword=<proxy_password>
```

9. Click **Save**.

   The Secure Agent restarts to apply the settings.

CHAPTER 3

Project setup

Create projects and project folders on the **Explore** page to organize your assets. After you have set up the runtime environment and connections that are required for a project, you can create the assets for the project.

You can't use the following characters:

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

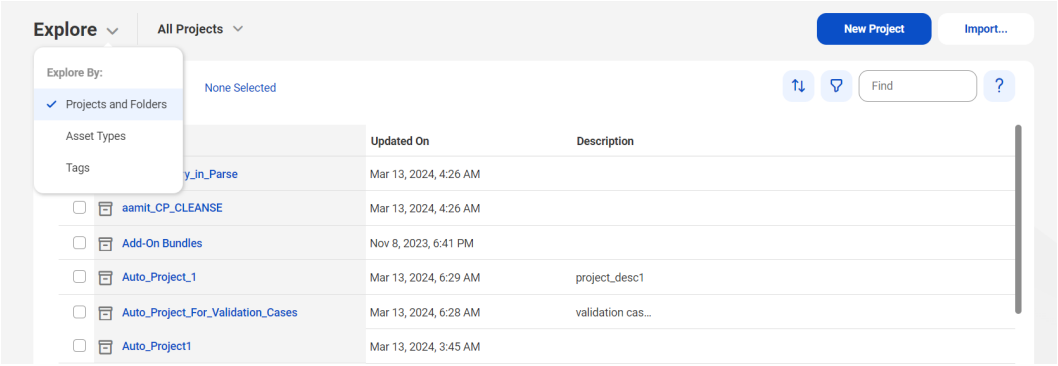
Do not use these characters in project, folder, asset, or tag names.

Creating projects and project folders

Projects can contain multiple folders that you can use to organize the assets used in the project. Create projects using the **Explore** page.

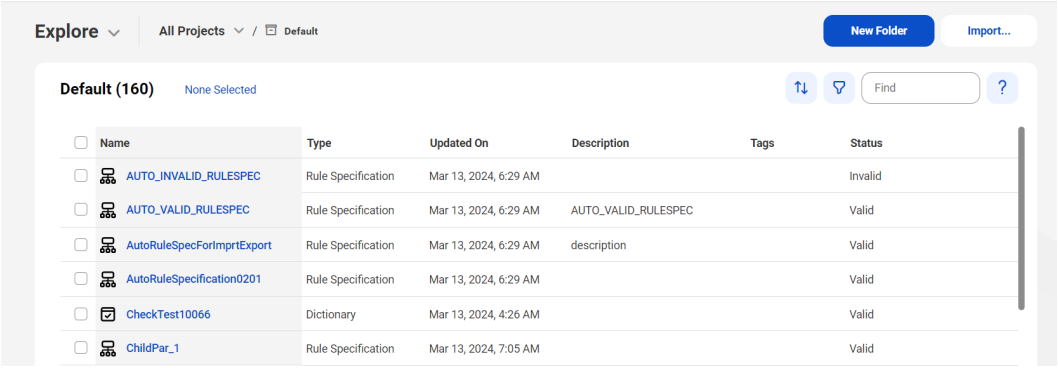
To create a project, go to the **Explore** page and select to explore by projects and folders, and then click **New Project**.

The following image shows the *Explore by* options and the **New Project** option on the **Explore** page:



To create a project folder, go to the **Explore** page and open the project, and then click **New Folder**.

The following image shows the **New Folder** option on the **Explore** page:



You can create one level of folders in a project. You cannot create folders within folders.

For more information about working with projects, see *Asset Management*.

Creating assets

You can create the following types of data quality assets:

- Cleanse. A cleanse asset performs standardization operations on data.
- Deduplicate. A deduplicate asset evaluates the degrees of similarity between the identities in a record set and assigns records with highly similar identities to clusters. A cluster is a set of records that are likely to represent the same information. A deduplicate asset optionally consolidates the records in each cluster into a preferred version of the records.
- Dictionary. A dictionary is a reference data set that you use to evaluate data in a rule specification.
- Labeler. A labeler asset identifies values in an input field that correspond to types of information that you specify. The asset returns a label for each value and optionally returns a standardized version of the value.
- Parse. A parse asset identifies one or more values in an input string and writes the values to discrete output fields according to the data that they contain.
- Rule Specification. A rule specification is an asset that represents the data requirements of a business rule in logical form.
- Verifier. A verifier asset evaluates the accuracy and deliverability of address records.

To create the assets, select the **New** page.

When you select the **New** page, Data Quality displays the options to create a cleanse asset, a dictionary, a deduplicate asset, a parse asset, a labeler asset, a rule specification asset, or a verifier asset.

Select the asset type that you want to create.

Note: For more information about an asset, including instructions on creating an asset, browse to the corresponding publication in the Cloud Data Quality documentation. For example, the Rule Specifications publication includes a topic on *Creating a rule specification.*

CHAPTER 4

Editing your user profile

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

You can update the following information in your profile:

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

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

1. Click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window and then select **Profile**.
2. On the **Profile** page, add or edit personal information such as your name, job title, phone number, and time zone.
3. To update your email address, click **Update Email**.

   Informatica Intelligent Cloud Services sends a verification email to your new email address. The email contains a link that is valid for 24 hours. When you click the link in the email, the new address is verified, and it appears in your profile. If the link expires, you can resend the verification email.
4. Optionally, change your password or security question.
5. Click **Save**.

CHAPTER 5

Switching to a different organization

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

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

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

To switch to a different organization:

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

INDEX

A

allowlist
  Secure Agent domains 9, 13
  Secure Agent IP addresses 9, 13

C

Cloud Application Integration community
  URL 4
Cloud Developer community
  URL 4
creating
  folders 17
  projects 17

D

Data Integration community
  URL 4
Data Integration Elastic
  setup 6
directories
  configuring Secure Agent login to access 11

E

email addresses
  for notification 19

F

firewall
  configuration 9, 13
folders
  creating 17

G

getting started
  activities 6

H

Hosted Agent
  definition 6

I

Informatica Global Customer Support
  contact information 5
Informatica Intelligent Cloud Services
  web site 4

L

Linux
  configuring proxy settings 15

M

maintenance outages 5

O

organizations
  switching to another organization 20

P

passwords
  changing 19
POD
  how to identify 9, 13
profiles
  editing 19
projects
  creating 17
  creating folders 17
proxy settings
  configuring on Linux 15
  configuring on Windows 11

R

requirements
  Secure Agent 8, 12
runtime environments
  configuring 6

S

Secure Agent groups
  definition 6
Secure Agent Manager
  launching 8

Secure Agents
communication port 9, 13
configuring a Windows service login 11
definition 6
domains allowlist 9, 13
installing on Linux 13
installing on Windows 9
IP address allowlist 9, 13
permissions on Linux 13
permissions on Windows 9
registering on Linux 13
registering on Windows 9
requirements on Linux 12
requirements on Windows 8
starting on Windows 8
security questions
editing 19
status
Informatica Intelligent Cloud Services 5
sub-organizations
switching to another organization 20
system status 5

T

time zones
changing user profile 19
trust site
description 5

U

upgrade notifications 5
user profiles
editing 19

W

web site 4
Windows
configuring proxy settings 11
Windows service
configuring Secure Agent login 11