



Informatica® Cloud Data Profiling
July 2024

Getting Started

Informatica Cloud Data Profiling Getting Started
July 2024
July 2024

© Copyright Informatica LLC 2016, 2025

Publication Date: 2025-07-04

Table of Contents

Chapter 1: Getting Started with Informatica Cloud Data Profiling.....	4
Chapter 2: System Requirements.....	5
Enabling CORS in Internet Explorer 11.	5
Chapter 3: Installing Secure Agents.....	10
Secure Agent installation on Windows.	10
Secure Agent requirements on Windows.	10
Downloading and installing the Secure Agent on Windows.	12
Configure the proxy settings on Windows.	13
Configure a login for a Windows Secure Agent Service.	13
Secure Agent installation on Linux.	14
Secure Agent requirements on Linux	14
Downloading and installing the Secure Agent on Linux.	16
Configure the proxy settings on Linux.	17
Chapter 4: Connection Configuration.....	19
Configuring a connection.	19
Object search and selection.	20
Chapter 5: Project Setup.....	22
Creating projects and project folders.	22
Creating assets.	23
Chapter 6: Editing your user profile.....	24
Chapter 7: Switching to a different organization.....	25
Index.	26

CHAPTER 1

Getting Started with Informatica Cloud Data Profiling

You can create a data profiling project in just a few steps.

Step 1. Check system requirements

Make sure that you are using a compatible browser when you design your projects. Check the Informatica Intelligent Cloud Services Product Availability Matrix for operating systems, databases, and other systems that Data Profiling supports.

Step 2. Configure a 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.

Use a Secure Agent group to access data on-premises. 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. Based on your license, you can add multiple agents to a group to balance workloads and improve scalability.

Step 3. Create a connection

Before you can create a data profiling task, you need to create a connection. When you configure the connection, you specify the connector that enables the exchange of data between the profile and source object.

Step 4. Create your project

Create a project folder and folders to contain the assets that you need for your project. If you do not create any project or folder, data profiling saves the data profiling tasks in the Default project.

CHAPTER 2

System Requirements

Use one of the following browsers when you work with Data Profiling:

- Google Chrome 62 and higher
- Microsoft Internet Explorer 11

Note: To use Internet Explorer 11, you must enable cross-origin support (CORS) in the browser.

- Mozilla Firefox (64-bit) 56 and higher

For more information about system requirements, see the Product Availability Matrix (PAM) for Data Profiling. The PAM indicates the versions of operating systems, databases, and other types of data sources and targets that a product release supports. You can access the PAM on Informatica Network at <https://network.informatica.com/community/informatica-network/product-availability-matrices/>.

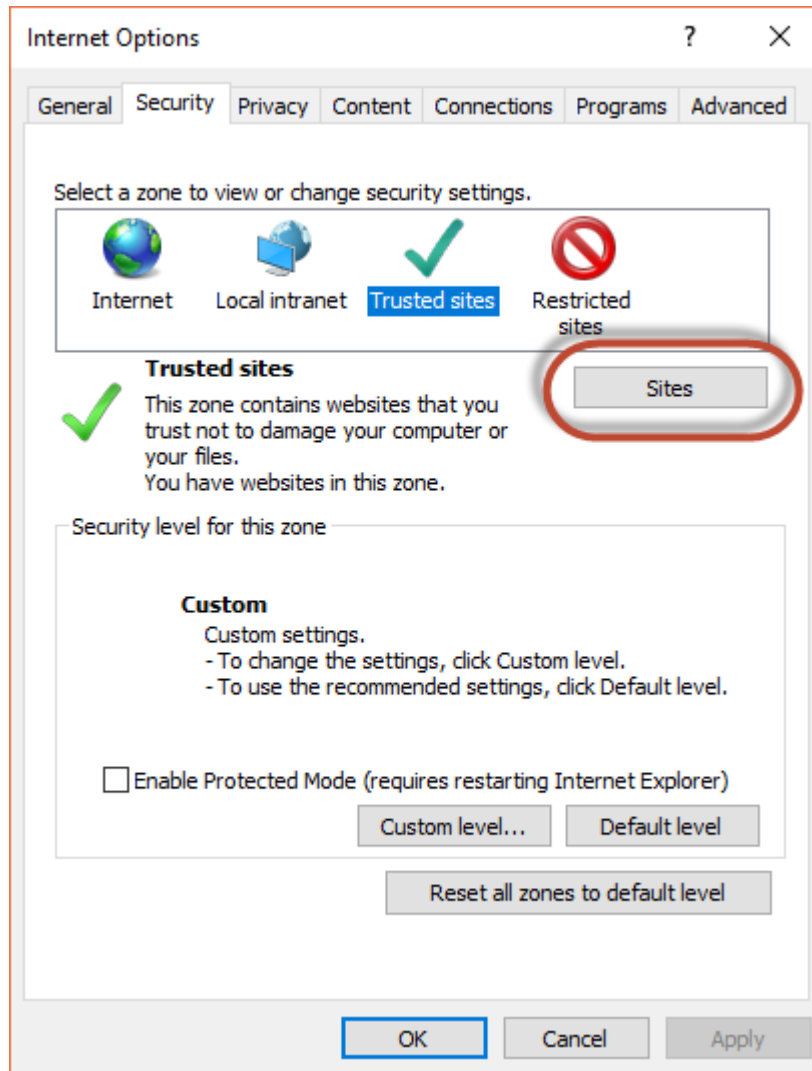
Enabling CORS in Internet Explorer 11

Informatica Intelligent Cloud Services requires that cross-origin support (CORS) be enabled in Internet Explorer 11. In Internet Explorer 11, CORS is not enabled by default.

Note: Some company security policies restrict the ability of users to enable CORS in a web browser. Before you update these settings, verify that your company or IT department allows you to change the CORS settings.

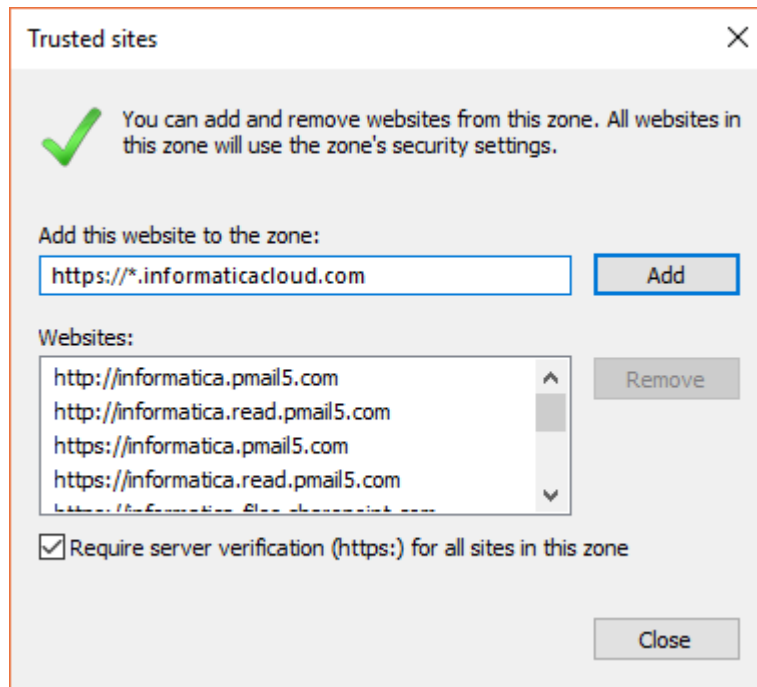
1. Open Internet Explorer 11.
2. On the **Tools** menu, select **Internet Options**.

3. On the **Security** tab, click **Trusted sites**, and then click **Sites** as shown in the following image:



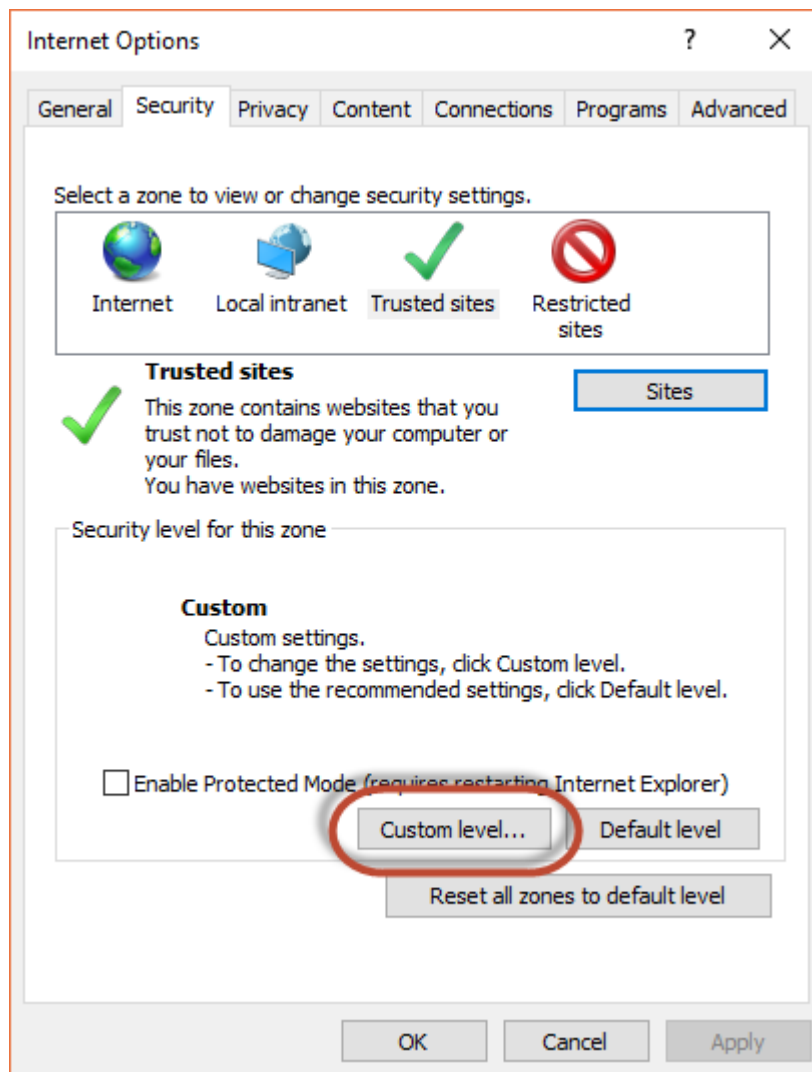
4. In the **Trusted Sites** dialog box, add the Informatica Intelligent Cloud Services domain to the zone, and click **Add**.

For example, the following image shows the domain `https://*.informaticacloud.com` added to the zone:

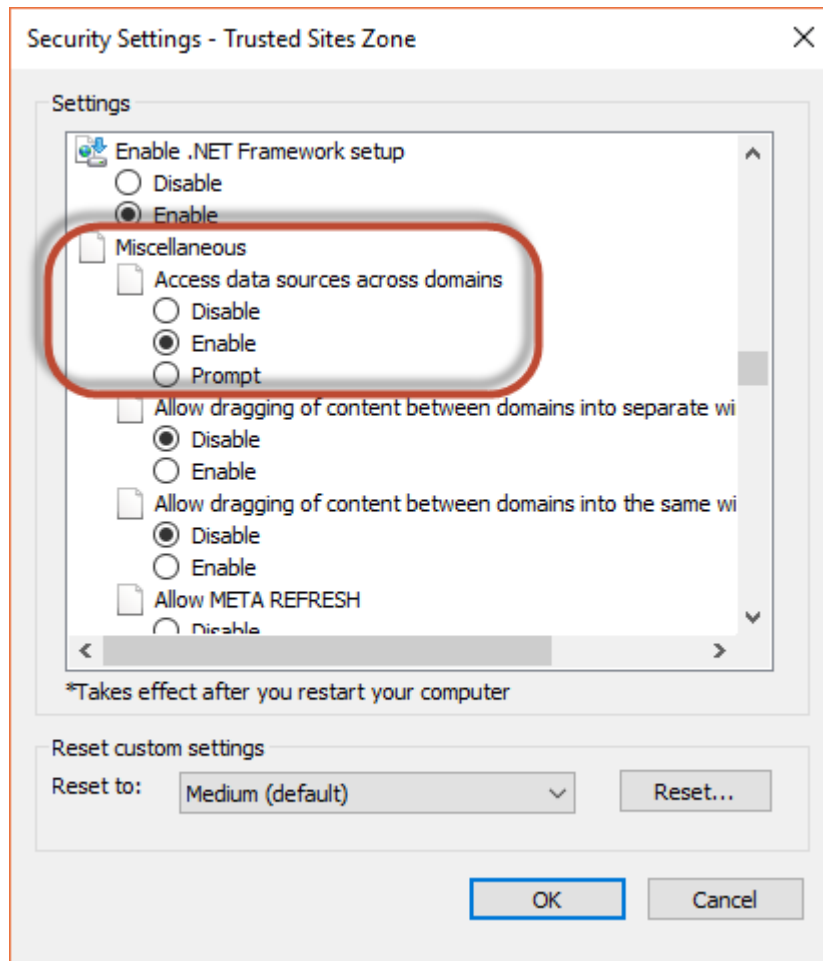


5. Click **Close**.

6. In the **Security level for this zone** area on the **Security** tab, click **Custom level** as shown in the following image:



7. In the **Security Settings - Trusted Sites Zone** dialog box, scroll down to the **Miscellaneous** heading, and enable **Access data sources across domains** as shown in the following image:



8. Click **OK**.
9. If prompted, confirm that you want to change the settings for the zone.
10. Click **OK**.
11. Restart Internet Explorer and re-open Informatica Intelligent Cloud Services.

CHAPTER 3

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 data center, which is also called a 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](#) in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

For information on the IP address ranges that you need to add to your list of approved IP addresses for AWS, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

For information on the IP address ranges that you need to add to your list of approved IP addresses for Azure, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

For information on the IP address ranges that you need to add to your list of approved IP addresses for GCP, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

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.

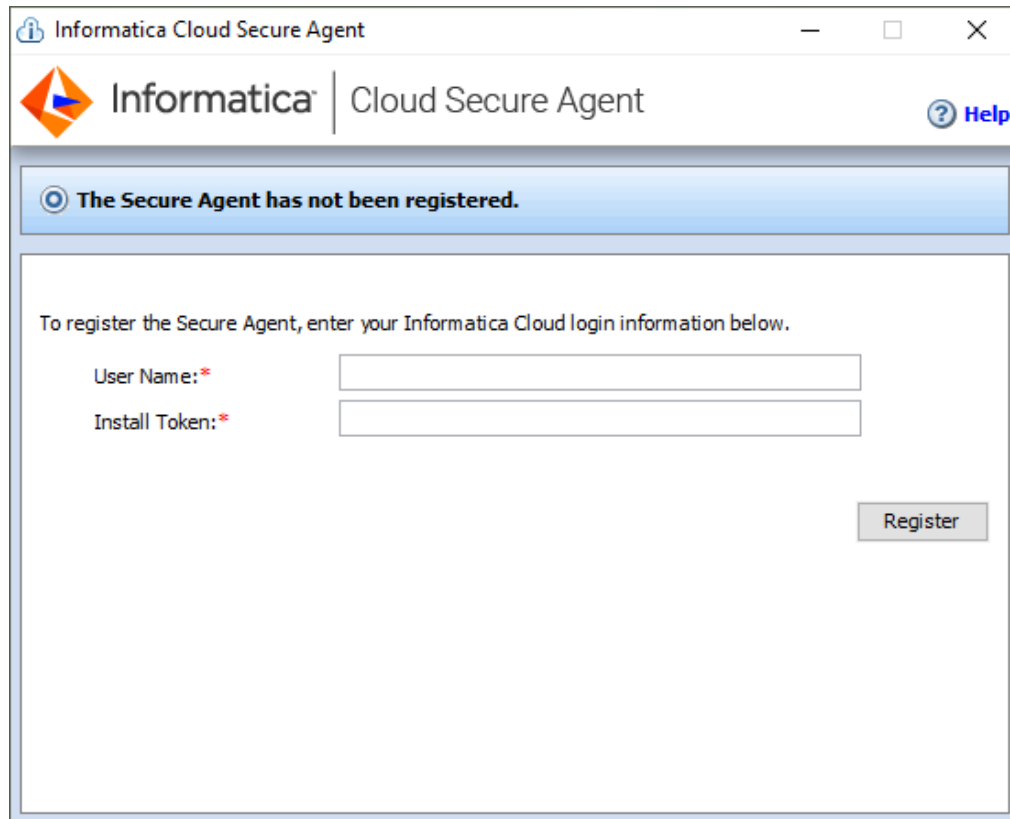
Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

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:



The screenshot shows a Windows-style dialog box titled "Informatica Cloud Secure Agent". The Informatica logo is on the left, and a "Help" button is on the right. A blue banner at the top states "The Secure Agent has not been registered." Below this, a message says "To register the Secure Agent, enter your Informatica Cloud login information below." There are two input fields: "User Name: *" and "Install Token: *". A "Register" button is located at the bottom right of the dialog.

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
```

- 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 data center, which is also called a 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](#) in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

For information on the IP address ranges that you need to add to your list of approved IP addresses for AWS, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

For information on the IP address ranges that you need to add to your list of approved IP addresses for Azure, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

For information on the IP address ranges that you need to add to your list of approved IP addresses for GCP, see [this Knowledge Base article](#) on Informatica Network. You can follow this Knowledge Base article for receiving notifications on updates made to the article.

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 4

Connection Configuration

When you create a data profiling task, you need a connection to the source object. You can create a connection in Administrator service.

For most connection types, when you configure a connection, you specify the runtime environment for the connection. The runtime environment must contain an agent that is running when you configure the connection. For other connection types, you specify the runtime environment when you configure the task.

This section includes general information about setting up a connection. For more information about connections and for specific information about configuring Flat File and FTP connections, see *Connections*. For specific information about other connection types, see the Data Integration Connector topics in the **Connectors** section of the Data Integration help.

Configuring a connection

You can configure a connection on the **Connections** page in Administrator service.

To access the **Connections** page, in Administrator, select **Connections**.

1. Configure the following connection details:

Connection detail	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the connection. Maximum length is 255 characters.
Type	Type of connection, such as Salesforce or Oracle.

2. Configure the connection-specific properties. For example, if this is a Flat File connection type, enter the runtime environment to be used with the connection, the directory where the flat file is stored, the date

format for date fields in the flat file, and the code page of the system that hosts the flat file. The following image shows the property fields for a flat file connection:

The screenshot shows the 'New Connection' dialog box. At the top, there is a title bar with a plug icon, the text 'New Connection', and two buttons: 'Save' and 'Test Connection'. Below the title bar is a section titled 'Connection Details' with the following fields: 'Connection Name:' (text box with 'SalesAccounts-FlatFile'), 'Description:' (empty text box), and 'Type:' (dropdown menu with 'Flat File' selected). Below this is a section titled 'Flat File Connection Properties' with the following fields: 'Runtime Environment:' (dropdown menu with 'CAB123456' selected), 'Directory:' (text box with 'C:\OurCompany\Sales' and a 'Browse...' button), 'Date Format:' (dropdown menu with 'MM/dd/yyyy HH:mm:ss' selected), and 'Code Page:' (dropdown menu with 'UTF-8' selected).

3. To test the connection, click **Test**. The results of the test display on the page, as shown in the following image:

The screenshot shows the 'SalesAccounts-FlatFile' dialog box. At the top, there is a title bar with a plug icon, the text 'SalesAccounts-FlatFile', and two buttons: 'Save' and 'Test Connection'. Below the title bar is a green checkmark icon and the text 'The test for this connection was successful.' Below this is a section titled 'Connection Details' with the same fields as the previous screenshot. Below this is a section titled 'Flat File Connection Properties' with the same fields as the previous screenshot. The 'Directory:' field is highlighted with a blue border.

If a database connection fails, contact the database administrator.

4. Click **Save** to save the connection.

Object search and selection

You can search for the source object when you select a connection for a data profiling task.

When you search for an object, the **Select Object** dialog box displays the first 200 objects available for the connection. You can select one of the objects or you can enter a search string. To begin a search, click **Search** or press **Enter**.

A search returns a maximum of 200 objects. If your search returns 200 objects without displaying the object that you want to use, enter a more specific search string.

You can use the object search at any time, but you must use the object search when the selected connection returns more than 200 objects.

Use the following guidelines when you enter a search string:

- Use an asterisk (*) as a wildcard character.
- Use quotation marks (") to perform an exact search. An exact search is case-sensitive.
- You can use the following search parameters based on the connection type:

Connection type	Search parameters
Databases	Name
Flat File	Name

CHAPTER 5

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.

The **Explore** page does not support the following characters:

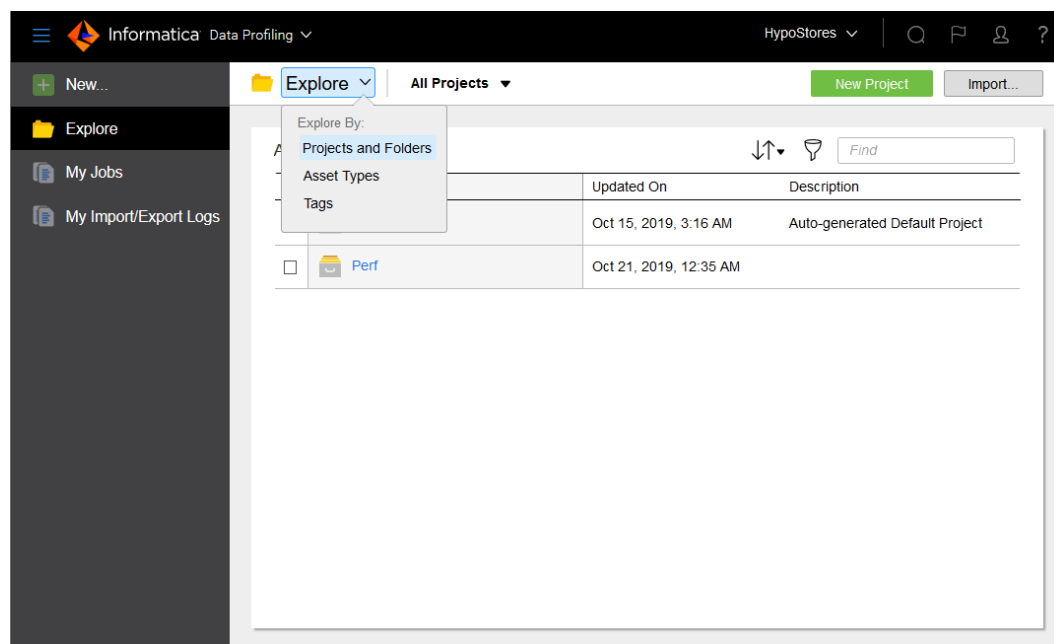
? ` | { } " ^ & [] / \

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

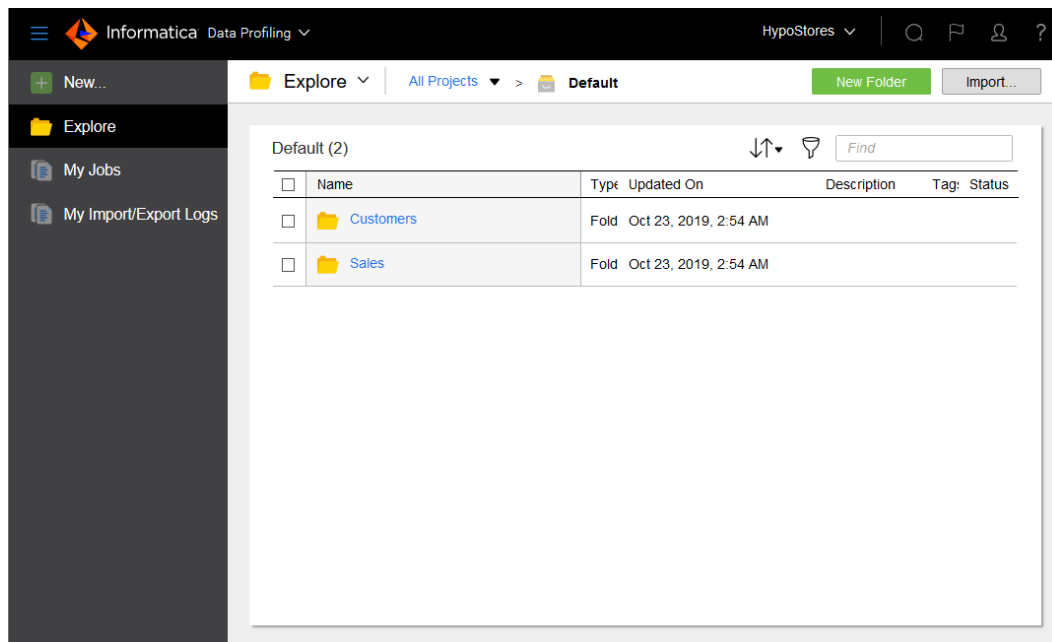
Creating projects and project folders

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**.



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



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

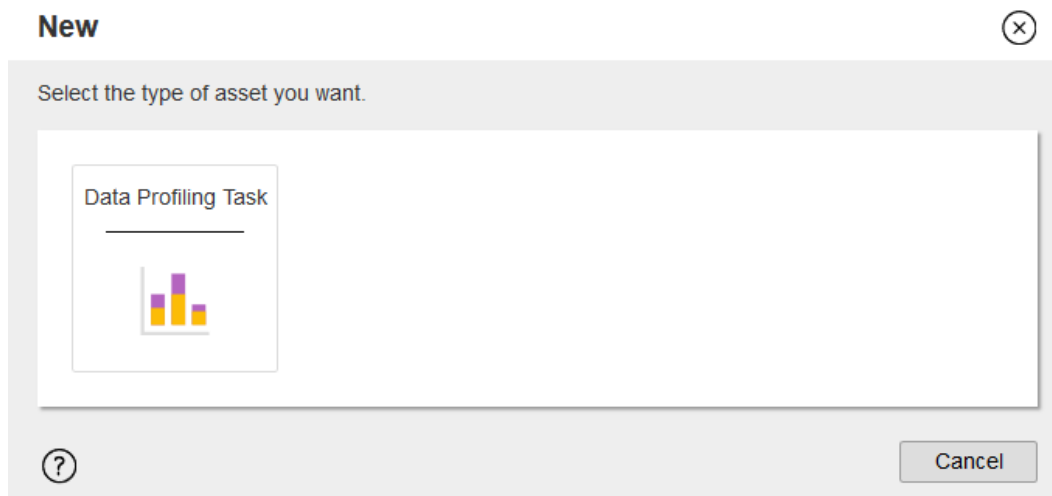
For more information about working with projects, see *Asset Management*.

Creating assets

You can create data profiling tasks in Data Profiling. You can create and run a data profiling task on a data source to determine the quality of data and understand the completeness, conformity, and consistency of data.

To create a data profiling task, click **New** and then select **Data Profiling Task**.

The following image shows the **New** dialog box:



For more information about creating a data profiling task, see *Data Profiling*.

CHAPTER 6

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 7

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
- Validate or run 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 [11, 15](#)
 Secure Agent IP addresses [11, 15](#)
assets
 creating [23](#)

B

browser
 requirements [5](#)

C

connections
 configuring properties [19](#)
 creating [19](#)
 testing [19](#)
creating
 assets [23](#)
 folders [22](#)
 projects [22](#)

D

directories
 configuring Secure Agent login to access [13](#)

E

email addresses
 for notification [24](#)

F

firewall
 configuration [11, 15](#)
folders
 creating [22](#)

G

getting started
 activities [4](#)

I

Internet Explorer 11
 requirements [5](#)

L

Linux
 configuring proxy settings [17](#)
lookups
 searching in a task wizard [20](#)

O

object search
 in a task wizard [20](#)
organizations
 switching to another organization [25](#)

P

passwords
 changing [24](#)
POD
 how to identify [11, 15](#)
Product Availability Matrix [5](#)
profiles
 editing [24](#)
projects
 creating [22](#)
 creating folders [22](#)
proxy settings
 configuring on Linux [17](#)
 configuring on Windows [13](#)

R

requirements
 browser [5](#)
 Internet Explorer 11 [5](#)
 Product Availability Matrix [5](#)
 Secure Agent [10, 14](#)
runtime environments
 configuring [4](#)

S

search
 for objects for a task wizard [20](#)
Secure Agent groups
 definition [4](#)

- Secure Agent Manager
 - launching [10](#)
- Secure Agents
 - communication port [11](#), [15](#)
 - configuring a Windows service login [13](#)
 - definition [4](#)
 - domains allowlist [11](#), [15](#)
 - installing on Linux [16](#)
 - installing on Windows [12](#)
 - IP address allowlist [11](#), [15](#)
 - permissions on Linux [16](#)
 - permissions on Windows [11](#)
 - registering on Linux [16](#)
 - registering on Windows [12](#)
 - requirements on Linux [14](#)
 - requirements on Windows [10](#)
 - starting on Windows [10](#)
- security questions
 - editing [24](#)
- sources
 - searching in a task wizard [20](#)
- sub-organizations
 - switching to another organization [25](#)

- system requirements [5](#)

T

- targets
 - searching in a task wizard [20](#)
- time zones
 - changing user profile [24](#)

U

- user profiles
 - editing [24](#)

W

- Windows
 - configuring proxy settings [13](#)
- Windows service
 - configuring Secure Agent login [13](#)