Informatica®

Informatica® Cloud Data Integration
July 2024

Getting Started

Informatica Cloud Data Integration Getting Started
July 2024

© Copyright Informatica LLC 2016, 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, PowerCenter, PowerExchange, 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. Required third party notices are included with the product.

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: 2024-07-12

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
- Data Integration connector documentation 6
- Informatica Knowledge Base 6
- Informatica Intelligent Cloud Services Trust Center 6
- Informatica Global Customer Support 6

Chapter 1: Getting Started with Informatica Cloud Data Integration 7

Chapter 2: System requirements 8

Enabling CORS in Internet Explorer 11 8

Chapter 3: Runtime environment configuration 13

Hosted Agent 14

Runtime environment configuration in a cloud environment 16

- Installing in AWS 16
- Installing in Google Cloud 19
- Installing in Azure 21

Secure Agent installation on Windows 22

- Secure Agent requirements on Windows 23
- Downloading and installing the Secure Agent on Windows 24
- Configure the proxy settings on Windows 25
- Configure a login for a Windows Secure Agent Service 26

Secure Agent installation on Linux 27

- Secure Agent requirements on Linux 27
- Downloading and installing the Secure Agent on Linux 28
- Configure the proxy settings on Linux 29

Chapter 4: Connection configuration 32

Configuring a connection 32

Object search and selection 33

Chapter 5: Project setup 35

Creating projects and project folders 35

Creating assets 36

Chapter 6: Enabling source control. 37

Configuring repository access. 37

Chapter 7: Editing your user profile. 38

Chapter 8: Inviting users to join your organization. 39

Chapter 9: Primary cloud data warehouse setup. 40

Configuring a primary cloud data warehouse. 40

Changing or unselecting a primary cloud data warehouse. 40

Chapter 10: Switching to a different organization. 42

Index. 43

Preface

Refer to *Getting Started* for information about how to begin using Informatica Cloud® Data Integration. *Getting Started* explains how to configure a runtime environment, connect Data Integration to your system, and begin a project.

Informatica Resources

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

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

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

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

Getting Started with Informatica Cloud Data Integration

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

Step 1. Check system requirements

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

Step 3. Create a connection

Before you can use Data Integration to run data integration tasks, you need to create a connection. When you configure the connection, you specify 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.

Step 4. Create your project

Organize your data integration projects in folders that contain assets such as mappings, tasks, and taskflows. Create a project folder and folders to contain the assets you need for your project.

After you set up folders, create your project assets. Assets include the following objects:

- Mappings
- Tasks
- Taskflows
- Components such as business services, mapplets, and hierarchical schemas

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.

CHAPTER 2

System requirements

You can find information about system requirements in the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services.

The PAM indicates the versions of browsers, 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/.

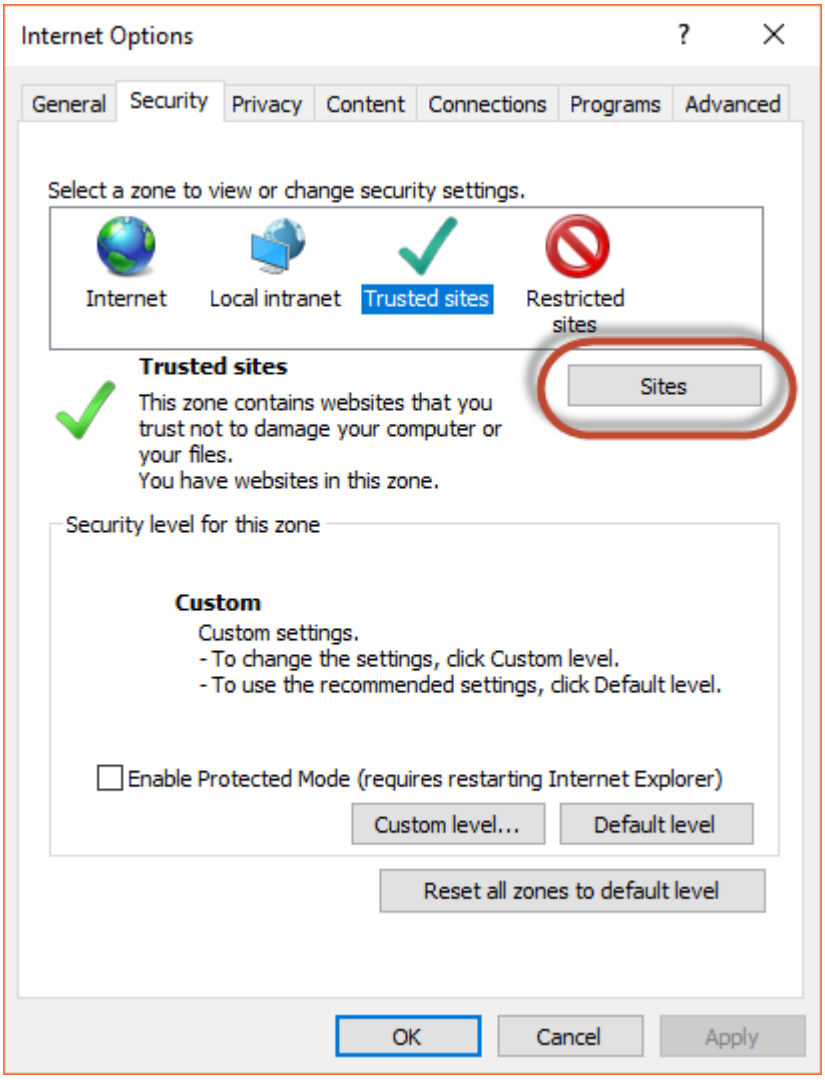
Enabling CORS in Internet Explorer 11

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.

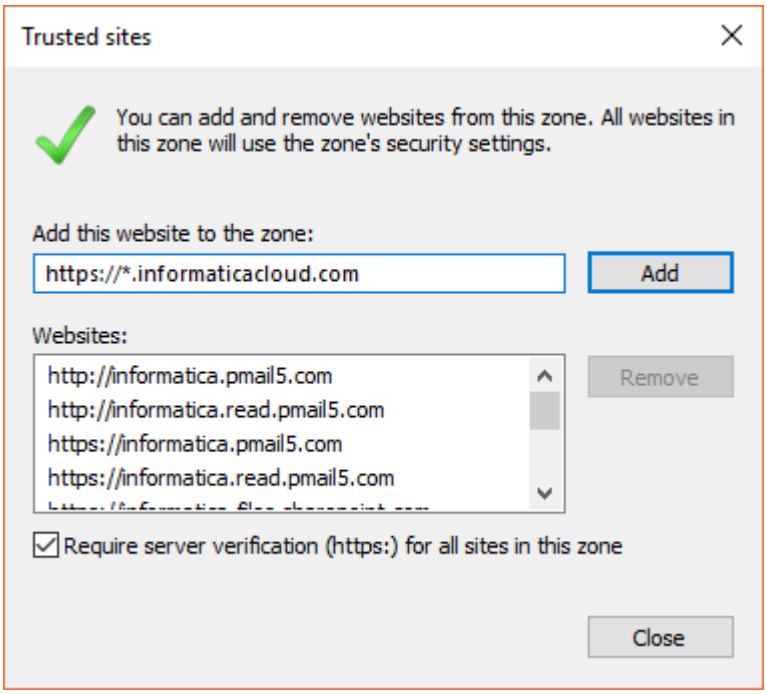
1. Open Internet Explorer 11.
2. On the **Tools** menu, select **Internet Options**.

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



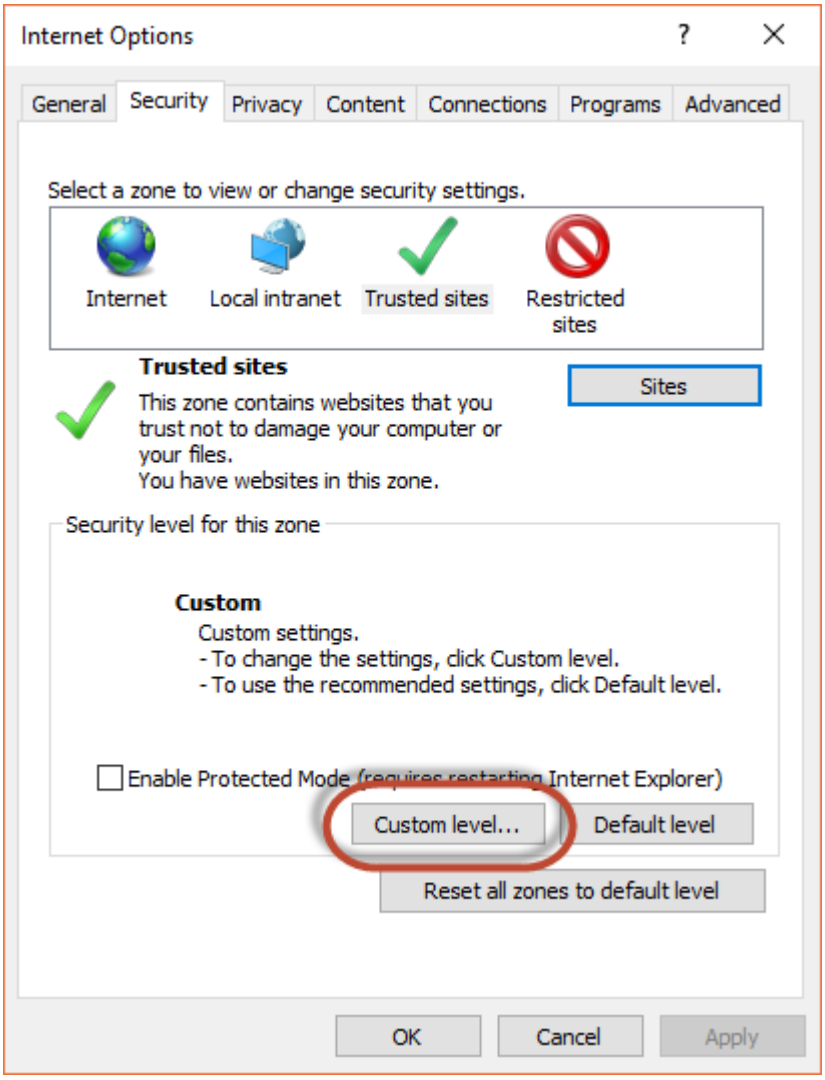
4. In the **Trusted Sites** dialog box, add the Informatica Intelligent Cloud Services domain to the zone, and click **Add**.

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

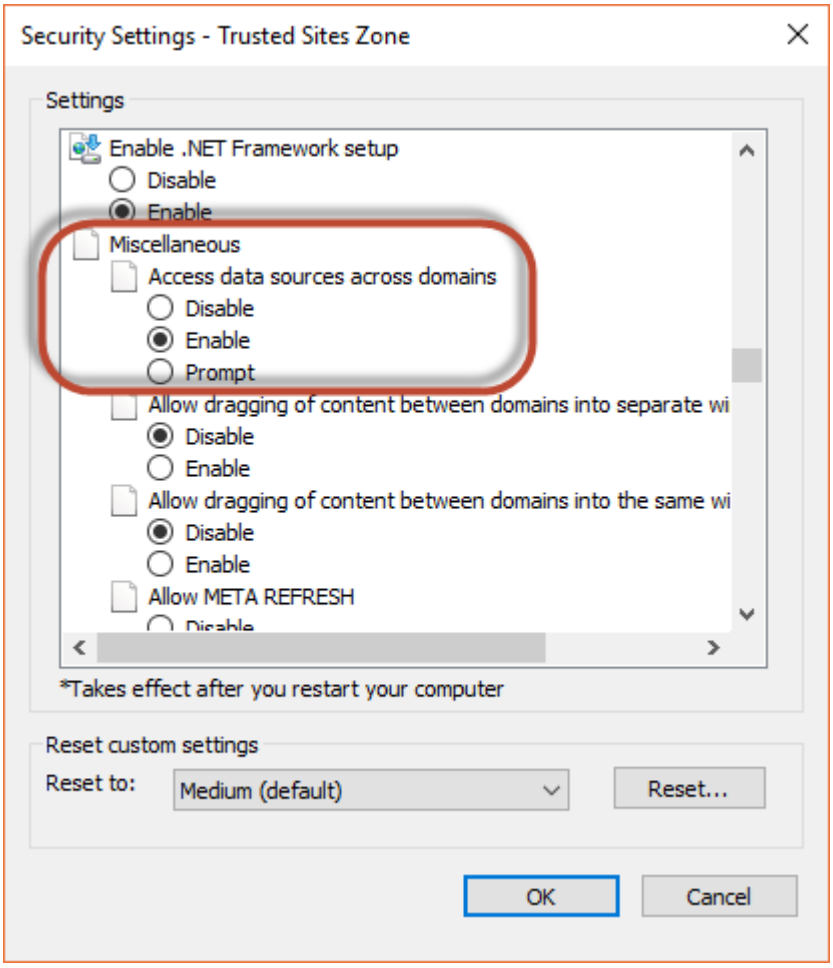


5. Click **Close**.

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

Runtime environment configuration

A runtime environment is the execution platform for running tasks. You must have at least one runtime environment in each organization so that users in the organization can run 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 can create and access a runtime environment in the following ways:

Use the Informatica Cloud Hosted Agent.

This is the simplest and quickest option. The Hosted Agent is included with every installation of Data Integration.

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's nothing to install.

The Hosted Agent can run mapping, synchronization, 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.

Configure a runtime environment on the cloud.

This is the second simplest method. The installation wizard does all the work behind the scenes to set up and configure a Secure Agent on AWS, Google Cloud, or Microsoft Azure.

Note: Configuring a runtime environment on the cloud creates a virtual machine on the cloud platform, which can incur additional costs.

Download and install a Secure Agent.

When you need to access data on-premises or when you want to access SaaS data without using the Hosted Agent, you can download and install a Secure Agent manually.

Download and install a runtime environment manually when you need to perform any of the following tasks:

- Run the agent on Windows.
- Install the agent on a local machine or a VM on a cloud platform other than AWS, Google Cloud, or Microsoft Azure.
- Access data sources that are behind a firewall.
- Run tasks that can't run on other runtime environment types. For example, Data Ingestion and Replication tasks must run on a local 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.

Configure a 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.

For more information about configuring a serverless runtime environment, see *Runtime Environments* in the Administrator help.

Hosted Agent

The Hosted Agent can run synchronization, mapping, and replication tasks that use certain connectors.

Informatica Intelligent Cloud Services manages the Hosted Agent runtime environment, so you cannot add, delete, or configure a Hosted Agent.

The Hosted Agent can run synchronization, mapping, and replication tasks that use the following connectors:

- Amazon Athena Connector
- Amazon Aurora Connector
- Amazon Redshift Connector
- Amazon Redshift V2 Connector
- Amazon S3 Connector
- Amazon S3 V2 Connector
- Box Connector
- Box Oauth Connector
- Cloud Integration Hub
- Concur V2 Connector
- Coupa Connector
- Coupa V2 Connector
- Cvent Connector
- Databricks Delta Connector
- DB2 Warehouse on Cloud Connector
- Eloqua Bulk API Connector
- Google Analytics Connector
- Google Big Query Connector
- Google Big Query V2 Connector
- Google Cloud Storage Connector

- Google Cloud Storage V2 Connector
- JIRA Connector
- Marketo V3 Connector
- Microsoft Azure Blob Storage V2 Connector
- Microsoft Azure Blob Storage V3 Connector
- Microsoft Azure Cosmos DB SQL API Connector
- Microsoft Azure Data Lake Storage Gen1 V2 Connector
- Microsoft Azure Data Lake Storage Gen1 V3 Connector
- Microsoft Azure Data Lake Storage Gen2 Connector
- Microsoft Azure SQL Data Warehouse V2 Connector
- Microsoft Azure SQL Data Warehouse V3 Connector
- Microsoft Azure Synapse SQL Connector
- Microsoft CDM Folders V2 Connector
- Microsoft Dynamics 365 for Operations Connector
- Microsoft Dynamics 365 for Sales Connector
- Microsoft Fabric Data Warehouse Connector
- Microsoft Fabric Lakehouse Connector
- Microsoft Fabric OneLake Connector
- Microsoft SQL Server Connector
- MySQL Connector
- NetSuite Connector
- OData Connector
- Oracle Connector
- PostgreSQL Connector
- REST V2 Connector
- Salesforce Connector
- Salesforce Marketing Cloud Connector
- Salesforce Oauth Connector
- ServiceNow Connector
- Snowflake Cloud Data Warehouse V2 Connector
- SuccessFactors ODATA Connector
- UltiPro Connector
- Workday V2 Connector
- Xactly Connector
- Zendesk V2 Connector
- Zuora AQuA Connector

Note: The Hosted Agent support is specific to connectors. For more information, see the help for the relevant connector.

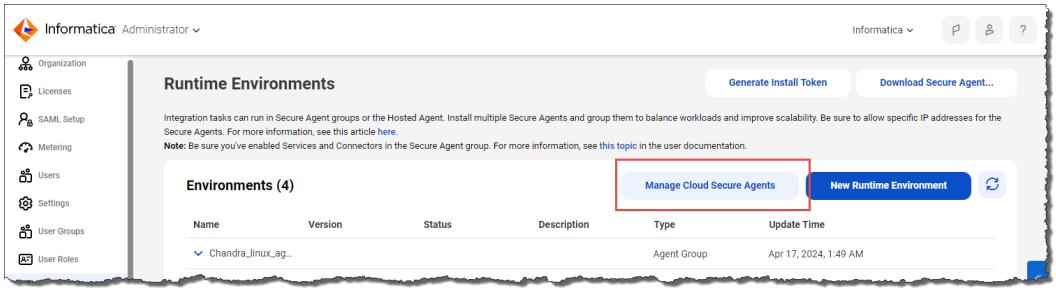
Runtime environment configuration in a cloud environment

You can install and run a Secure Agent on AWS, Google Cloud, or Microsoft Azure.

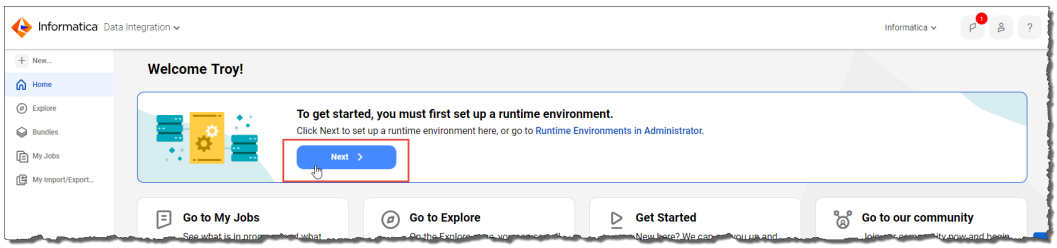
Install a Secure Agent in the following ways based on your cloud environment:

- If you choose AWS, you're redirected to the AWS Marketplace to continue the installation.
- If you choose Google Cloud, you log in using your Google credentials and then enter the Secure Agent configuration details.
- If you choose Microsoft Azure, you log in using your Azure credentials and then enter the Secure Agent configuration details.

You can install a Secure Agent in a cloud environment on the **Runtime Environments** page in Administrator. Click **Manage Cloud Secure Agents** to open the installer, as shown in the following image:



If your organization uses the unified **Home** page and your organization doesn't have any runtime environments, you can also install a Secure Agent in a cloud environment by clicking **Next** in the **To get started, you must first set up a runtime environment** panel, as shown in the following image:



Installing in AWS

The Secure Agent installer can help you create a runtime environment on Amazon Web Services (AWS). The runtime environment you create is a Secure Agent group that contains one Secure Agent.

When you create a runtime environment on AWS, you create a new stack where the Secure Agent is deployed. You can create the stack in a new or existing virtual private cloud (VPC). The installer creates an Amazon Elastic Compute Cloud (EC2) instance within the VPC.

To create a runtime environment, you must have a subscription with AWS that includes create, modify, and delete privileges for the following resource types:

- AWS CloudFormation template. The AWS CloudFormation template supports the following regions: ap-southeast-2, eu-west-2, eu-central-1, us-west-2.
- EC2 instances

- Elastic IP addresses
- Elastic network interfaces
- Internet gateways
- Route tables
- Security groups
- Subnets
- VPCs

You must also have read and launch permissions for machine images and AWS CloudFormation templates.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Manage Cloud Secure Agents**.
3. Click **New Cloud Secure Agent**.
4. Select **Amazon Web Services**.
5. Click **Next**.
6. On the **Environment Configuration** page, copy the install token.

   The install token is valid for 24 hours and can't be reused.
7. Choose whether to create the runtime environment on an existing or new VPC.
8. Click **Continue Configuration in AWS**.

   The AWS **Sign in** screen opens in a new browser tab.
9. Sign in to your AWS account.

   The **Quick create stack** page opens.
10. In the **Stack name** area, enter a stack name.
11. In the **Parameters** area, under **Network Configuration**, configure the following properties based on whether you're using an existing VPC or a new VPC.
    - For an existing VPC, configure the following properties:

Property	Value
VPC ID	Select the ID for the VPC where you want to deploy the Secure Agent.
Subnet ID	Enter or select a subnet within the VPC.
Allowed Remote Access CIDR	Enter the CIDR block that specifies the IP addresses where the Secure Agent can be installed. CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses. It configures a network rule to allow remote access to the Secure Agent. The "/x" portion of the address determines how many IP addresses are available in the subnet, for example: 108.124.81.10/32

- For a new VPC, configure the following properties:

Property	Value
Availability Zones	Select the availability zone for your region.
VPC CIDR	Enter the CIDR block that specifies the IP addresses where you want to create the VPC.
Subnet CIDR	Enter the CIDR block that specifies the IP addresses for the subnet in the availability zone that you selected.
Allowed Remote Access CIDR	Enter the CIDR block that specifies the IP addresses where the Secure Agent can be installed.

12. Under **Amazon EC2 Configuration**, configure the following properties:

Property	Value
Key Pair Name	Enter the name of an existing EC2 key pair to enable external access to the EC2 instance. Corresponding key pair files are required for SSH access to the server.
Instance Type	Select the instance type for the EC2 instance or accept the default. Default is m5.xlarge.
Enable Elastic IP Addressing	Choose whether to assign elastic IP addresses to the EC2 instance or accept the default. Default is no.

13. Under **Informatica Intelligent Data Management Cloud (IDMC) Account Details**, configure the following properties:

Property	Value
IDMC POD Master URL	Accept the default value for the IDMC POD Master URL. This is the URL that you use to access Informatica Intelligent Cloud Services. **Warning:** Changing this URL can result in stack deployment failure.
IDMC User Name	Enter your Informatica Intelligent Cloud Services user name.
IDMC User Token	Paste the install token that you copied. If you forgot to copy the install token, you can switch back to Informatica Intelligent Cloud Services and generate a new one.
Secure Agent Group Name	Accept the default value for the Secure Agent group name. This is the name of the runtime environment that you're creating.

14. Click **Create stack**.

    It takes a few minutes to create the stack. Be sure to monitor the stack creation and address any issues that might occur. For more information about troubleshooting CloudFormation stacks, see the AWS documentation.

When the stack is created successfully, the EC2 Instance status changes from CREATE_IN_PROGRESS to CREATE_COMPLETE.

15. In Informatica Intelligent Cloud Services, on the **Environment Configuration** page, click **Finish**.

    IICS creates your runtime environment and displays it on the **Runtime Environments** page.

    Tip: To see the progress of your pending Secure Agents, click **Manage Cloud Secure Agents** on the **Runtime Environments** page. The status appears at the top of the page.

It takes a few minutes for the Secure Agent services to start. When the Secure Agent is ready to use, the status changes from "Pending Environment Set Up" to "Up and Running." You might need to refresh the page to see the updated status.

Installing in Google Cloud

The Secure Agent installer can create a runtime environment on Google Cloud for you, based on just a few properties that you enter on the configuration page.

Note: You must have a subscription with Google Cloud that includes permissions to deploy resources.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Manage Cloud Secure Agents**.
3. Select **Google Cloud Platform**.
4. Click **Next**.
5. Select the Google account to use.
6. Enter the following properties:

Property	Description
Project	A project defines how Informatica Intelligent Cloud Services interacts with Google services and what resources it uses. Select your Google Cloud project from the drop-down list. **Note:** If you don't have a project, exit the installation wizard and create your project on Google Cloud. You can't create a project from within Informatica Intelligent Cloud Services.
Secure Agent Name	Enter a name for your Secure Agent. The name needs to conform to the following rules: - The name can be up to 43 characters long, with a combination of letters, numbers, and hyphens. - The first character must be a lowercase letter. - The last character can't be a hyphen. - All letters must be lowercase. By default, the runtime environment uses the same name as the agent.
Region	Select the region to deploy the Secure Agent. Choose a region that's appropriate for your organization and your customers.
Machine Type	Select the machine type for your virtual machine. If you're not familiar with Google machine types, start with a size with at least 4 cores and 16 GB of memory.
Virtual Network	Specify whether to use an existing virtual network based on your Google subscription or create a new virtual network. A virtual network uses hardware and software to emulate a physical network.

Property	Description
Virtual Network Name	Select an existing virtual network or enter the name for a new virtual network.
Subnet	Select the subnet to use or enter a name for a new subnet.
Subnet Address	Select the subnet address that includes all the resources or enter a new subnet address. Subnet addressing allows a system made up of multiple networks to share the same Internet address.

7. Select the **I acknowledge this action will incur costs in Google Cloud Platform** check box to acknowledge that costs will be incurred on your Google account.
8. Click **Create**.
   Informatica Intelligent Cloud Services creates your runtime environment and displays it on the **Runtime Environments** page.

Troubleshooting connection issues on Google Cloud

The firewall in Google Cloud can block access to your VM. If this occurs, add a firewall rule to allow RDP and SSH access to your VM instances.

When Google Cloud blocks access, the runtime environment fails to start with the following error:

```
Connection Failed. We are unable to connect to the VM on port 22.
```

1. In the Google Cloud console, go to the **Firewall Rules** page.
2. Click **Create firewall rule**.
3. Create a firewall rule with the following settings:

Setting	Value
Name	Enter a name for the firewall rule. For example: `allow-ingress-from-iap(<name>)`
Direction of traffic	Ingress
Action on match	allow
Target	All instances in the network
Source filter	IP ranges
Source IP ranges	35.235.240.0/20
Protocols and ports	Select **TCP** and enter `22,3389` to allow both RDP and SSH.

4. Click **Create**.

Installing in Azure

The Secure Agent installer can configure a runtime environment on Microsoft Azure. Note that running data integration tasks on Azure incurs costs based on the workload and the VM size.

Note: You need a Microsoft Azure subscription with permissions that allow you to deploy resources. If admin consent is enabled at your organization, reach out to the Azure administrator for app consent approvals. For more information about admin consent requests, see the Microsoft documentation.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Manage Cloud Secure Agents**.
3. Click **New Cloud Secure Agent**.
4. Select **Microsoft Azure**.
5. Click **Next**.
6. Select the Microsoft account to use.
7. Enter the following properties:

Property	Description
Subscription	Select your Microsoft Azure subscription. The subscription must include permissions to deploy the following resources: - Network security group - Virtual network (including subnet) - Network interface - Public IP address - OS disk - Virtual machine Be sure to grant permission to the Hyperscalar Azure Integration App when prompted. **Note:** If you do not have an Azure subscription, exit the installer and sign up for one with Microsoft. You cannot sign up from within Informatica Intelligent Cloud Services.
Resource Group	A resource group is a container that holds related resources for your runtime environment. Informatica Intelligent Cloud Services uses one resource group for each Secure Agent to simplify management of the VM resources for that agent. You typically create new resource groups, but you can use any existing group that is empty. **Tip:** Use the same or similar name as the Secure Agent to more easily identify which resource group belongs with each agent.
Resource Group Name	Name of the resource group. Enter the name of a new group or select an existing group. Ensure that any existing resource group is empty, otherwise this message appears*: "API Input validation failed."*
Location	Select the region to deploy the Secure Agent. Choose the Azure region that's appropriate for your organization and your customers. Not every resource is available in every region.
VM Name	Enter a name for the virtual machine (VM) that will be created.
VM User Name	Enter your name as the virtual machine user.
VM Password	Enter a password to access the virtual machine.

Property	Description
Secure Agent Name	Enter a name for your Secure Agent. By default, the runtime environment has the same name as the agent. **Tip:** Use the same or similar name as the resource group, to more easily identify which resource group belongs with each agent.
VM Size	Select a size for your virtual machine. If you are unfamiliar with Azure image sizing, start with a size with at least 4 cores and 16 GB of memory. Note that your Azure hourly charges are affected by the VM size.
Virtual Network	Select an existing virtual network based on your Microsoft Azure subscription and location or create a new virtual network.
Virtual Network Name	Select an existing virtual network or enter the name for a new virtual network. When you select an existing virtual network, this associates the newly created VM with the existing VNet.
Virtual Network Address	Select an existing virtual network address or enter a new address.
Subnet Name	Select the subnet to use or enter a name for a new subnet. The subnet holds all the Azure resources that are deployed to the virtual network.
Subnet Address	Select the subnet address that includes all the resources or enter a new subnet address. Subnet addressing allows a system made up of multiple networks to share the same Internet address.
CIDR IP Address Range	Enter the CIDR IP address range. CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses. It configures a network rule to allow remote access to the Secure Agent. The "/x" portion of the address determines how many IP addresses are available in the subnet, for example: 108.124.81.10/32

Tip: For more information, refer to "Explore Azure Virtual Networks" in the Microsoft documentation.

8. Click **Create**. Administrator creates your runtime environment and displays it on the **Runtime Environments** page.

   Tip: To see the progress of your pending Secure Agents, click **Manage Cloud Secure Agents** on the **Runtime Environments** page. The status appears at the top of the page.

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.

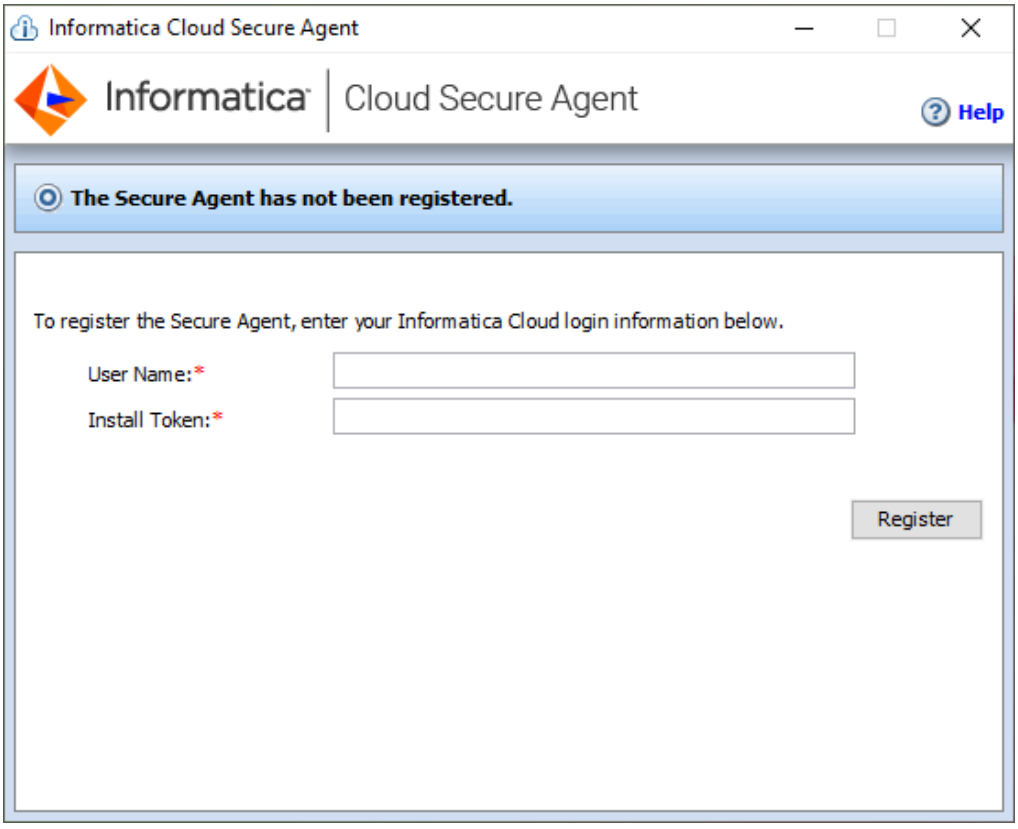
Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine. If any other Secure Agent exists, you must uninstall it.

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 4

Connection configuration

When you create a connection, it's available to your Data Integration organization.

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 help.

Configuring a connection

You can configure a connection on the **Connections** page, in a wizard as you configure a task or taskflow, or in the Mapping Designer as you configure a mapping.

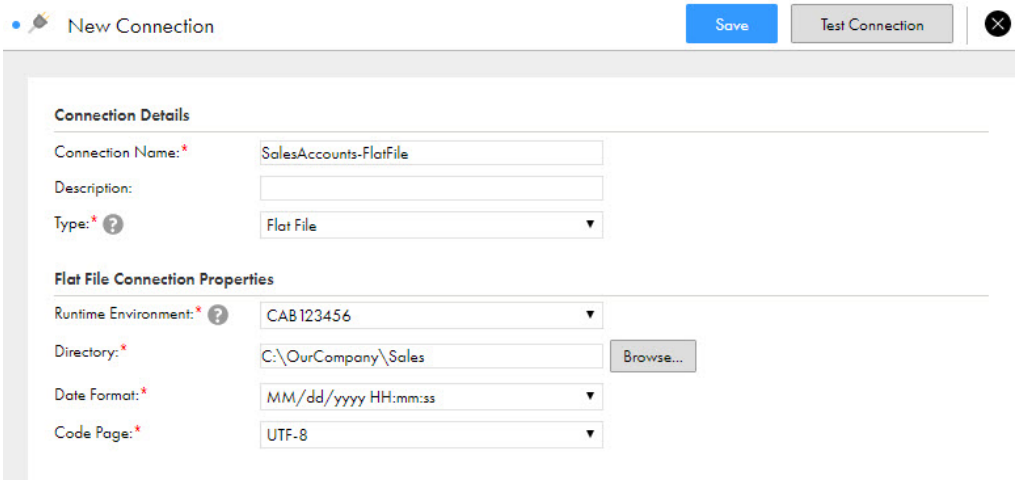
To access the **Connections** page, in Administrator, select **Connections**.

1. Configure the following connection details:

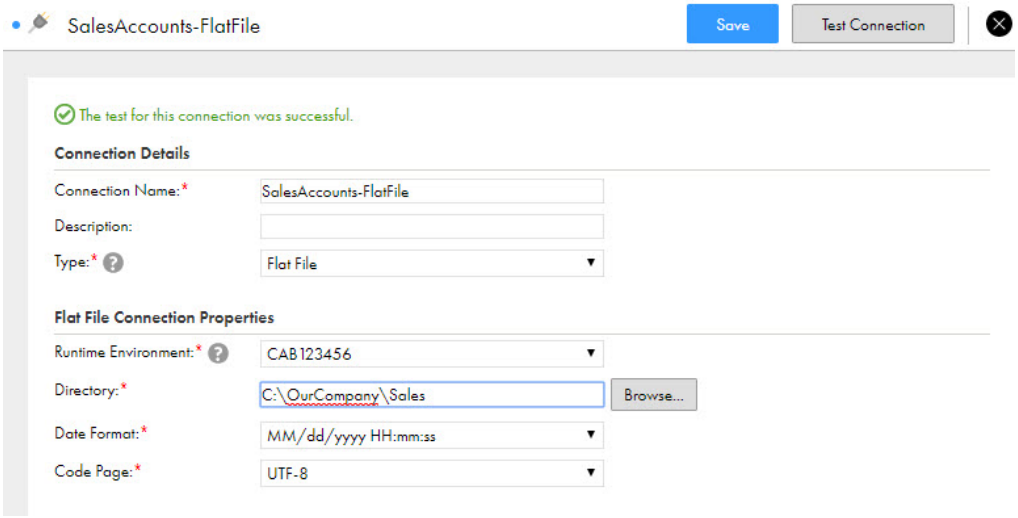
Connection detail	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Maximum length is 100 characters. Connection names are not case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



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



If a database connection fails, contact the database administrator.

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

Object search and selection

When you select a connection in a Data Integration mapping or task, you can search for the object or objects that you want to use.

When you search for an object, the **Select Object** dialog box displays the 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**.

Note: For some connection types, you must select the schema associated with the object in the **Packages** pane before you can view and select objects. You can search for the schema to use.

For synchronization and mapping tasks, use object search when the connection responds slowly.

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
CDC	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.

You can't use the following characters:

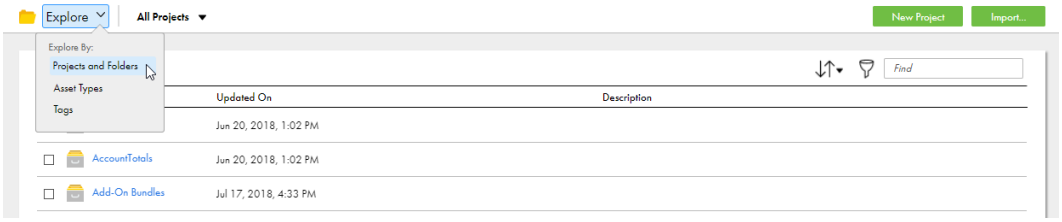
```
# ? ' | { } " ^ & [ ] / \
```

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

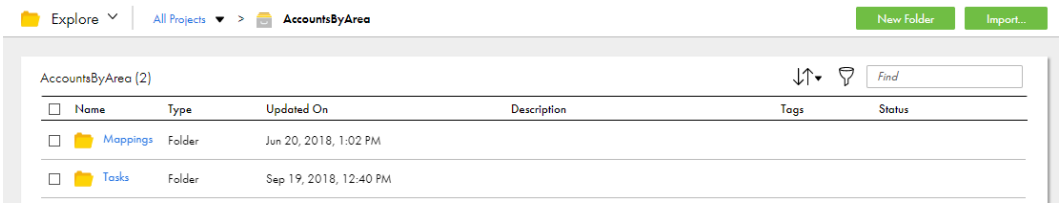
Creating projects and project folders

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**.



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

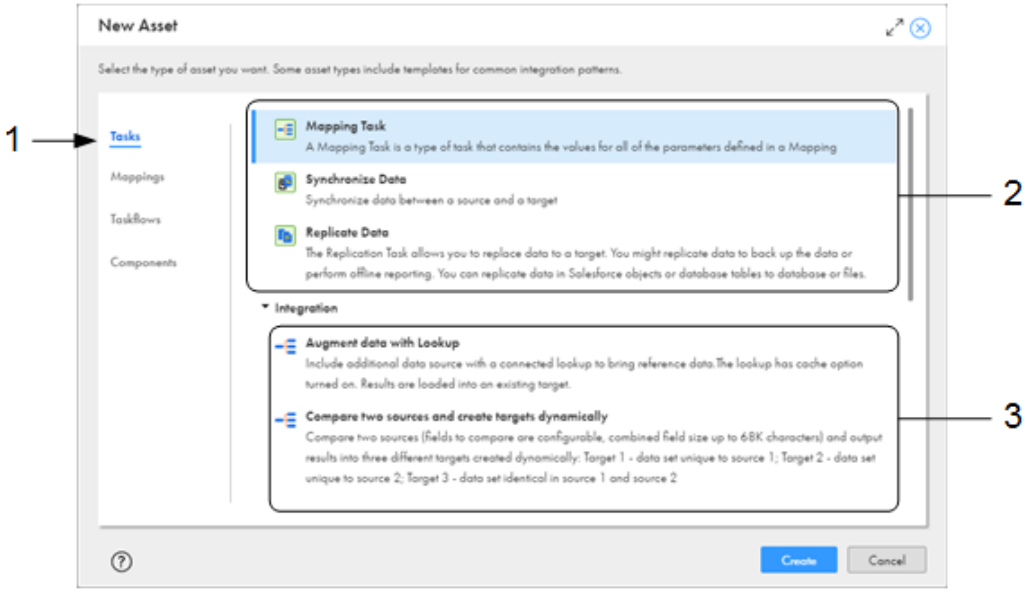
Create integration assets and assign them to projects.

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

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

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

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



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

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

- You can begin all asset names with an abbreviation of the asset type. For example, mapping names begin with m_ and mapping tasks begin with mt_.
- Within mappings, you can begin all Source transformation names with src_, all parameter names with p_, and so on.
- You can use names that explain the purpose of the object, For example, filter names begin with flt_.

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

For more information on working with assets, see *Asset Management*.

CHAPTER 6

Enabling source control

If your Informatica Intelligent Cloud Services organization is licensed to use source control, specify your source control repository user credentials in Informatica Intelligent Cloud Services.

Before your organization can use source control, the organization administrator must configure a link between the Informatica Intelligent Cloud Services organization and a GitHub, Azure DevOps, or Bitbucket source control repository.

If your organization has read/write access to the source control repository, you can add your projects and assets to the repository. Each time you check out the objects, make changes, and then check them in to the repository, the source control system creates a new version of the objects.

If your organization has read-only access to the source control repository, you can pull versions of projects and assets to your organization, but you cannot add new or updated objects to the repository.

For more information about source control, see *Asset Management*.

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**.

CHAPTER 7

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 8

Inviting users to join your organization

If you have an appropriate role, you can invite users to join your organization when you configure a runtime environment or primary cloud data warehouse. Invite users to join your organization so they can help you set up a runtime environment or connect to your cloud data warehouse.

To invite users to join your organization, click **Invite a friend or colleague to help you**. To invite users, you must have the Admin role, or you must have the Designer role and a custom role that has the "read role" and "create user" Administrator asset privileges. You must assign the user you invite the Admin or Designer role.

If you don't see the **Invite a friend or colleague to help you** option or you want to assign the user a different role, you can add a user on the **Users** page in Administrator. For more information, see *User Administration* in the Administrator help.

1. Click **Invite a friend or colleague to help you**.
2. Enter the first name, last name, email address, user name, and role for the person you want to invite.

   The user name must be unique within the organization. You cannot change the user name after you invite the user.

   You can assign the following roles:

   - Select **Administrator** to assign the user the Admin role.
   - Select **Designer** to assign the user the Designer role.
3. Click **OK**.

   The user you invite receives an email with a link to join your organization.

CHAPTER 9

Primary cloud data warehouse setup

You can configure a primary cloud data warehouse where you normally load data. When you do this, the mappings in SQL ELT mode that you create are automatically configured to load data to this target. You can still change the target if you wish.

You can configure a primary cloud data warehouse if your organization uses the unified **Home** page. The cloud data warehouse that you choose applies to the organization that you're currently logged into. If you have access to multiple organizations, you can configure a different primary cloud data warehouse for each organization and sub-organization.

The setup steps vary based on whether you've already configured a primary cloud data warehouse. If you've already configured one, you can change or unselect it.

Configuring a primary cloud data warehouse

Configure a primary cloud data warehouse from the **Home** page.

1. On the **Home** page, click **Yes, let's go** in the **Do you use a cloud data warehouse as your primary destination?** panel.
2. On the **Destination** page, select your cloud data warehouse type, for example, Snowflake Data Cloud or Databricks Delta, and click **Next**.
3. On the **Connect** page, select a connection, or click **New** and enter the connection properties.
4. Click **Connect**.

Changing or unselecting a primary cloud data warehouse

If you've already configured a primary cloud data warehouse, you can change or unselect it. Change or unselect a primary cloud data warehouse from the **Home** page.

1. On the **Home** page, click the cloud data warehouse type in the upper right corner and select **Change primary cloud data warehouse**.

2. If you want to change your primary cloud data warehouse, select **I have a primary cloud data warehouse**.
3. To change the cloud data warehouse type, complete the following steps:
    a. Click **Change** next to **Type**.
    b. On the **Destination** page, select the data warehouse type, and then click **Next**.
    c. On the **Connect** page, select a connection, or click **New** and enter the connection properties.
    d. Click **Connect**.
4. To change the connection, complete the following steps:
    a. Click **Change** next to **Connection**.
    b. On the **Connect** page, select a connection, or click **New** and enter the connection properties.
    c. Click **Connect**.
5. If you no longer wish to use a primary cloud data warehouse, select **I don't have a primary cloud data warehouse**, and click **Save**.

CHAPTER 10

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 23, 28
  Secure Agent IP addresses 23, 28
assets
  creating 36
  source control 37
Azure DevOps user credentials 37

B

Bitbucket user credentials 37

C

Cloud Application Integration community
  URL 5
cloud data warehouses
  changing the primary cloud data warehouse 40
  configuring a primary cloud data warehouse destination 40
  primary cloud data warehouse setup 40
  unselecting a primary cloud data warehouse 40
Cloud Developer community
  URL 5
connections
  configuring properties 32
  creating 32
  testing 32
creating
  assets 36
  folders 35
  projects 35

D

Data Integration community
  URL 5
directories
  configuring Secure Agent login to access 26

E

email addresses
  for notification 38

F

firewall
  configuration 23, 28
folders
  creating 35

G

getting started
  activities 7
  runtime environment configuration 13
GitHub user credentials 37

H

Hosted Agent
  description 14

I

Informatica Global Customer Support
  contact information 6
Informatica Intelligent Cloud Services
  web site 5
Internet Explorer 11
  requirements 8

L

Linux
  configuring proxy settings 30
lookups
  searching in a task wizard 33

M

maintenance outages 6

O

object search
  in a task wizard 33
organizations
  switching to another organization 42

P

passwords
  changing 38
POD
  how to identify 23, 28
Product Availability Matrix 8

profiles
editing 38
projects
creating 35
creating folders 35
source control 37
proxy settings
configuring on Linux 30
configuring on Windows 25

R

requirements
Internet Explorer 11 8
Product Availability Matrix 8
Secure Agent 23, 27
runtime environments
Hosted Agent 14
configuring 13, 16, 19, 21
installing in a cloud environment 16

S

search
for objects for a task wizard 33
Secure Agent Manager
launching 22
Secure Agents
communication port 23, 28
configuring a Windows service login 26
domains allowlist 23, 28
installing in a cloud environment 16
installing on Linux 28
installing on Windows 24
IP address allowlist 23, 28
permissions on Linux 28
permissions on Windows 23
registering on Linux 28
registering on Windows 24
requirements on Linux 27
requirements on Windows 23
starting on Windows 22
security questions
editing 38
source control
configuring access to the repository 37
sources
searching in a task wizard 33
status
Informatica Intelligent Cloud Services 6
sub-organizations
switching to another organization 42
system requirements 8
system status 6

T

targets
searching in a task wizard 33
time zones
changing user profile 38
trust site
description 6

U

upgrade notifications 6
user profiles
editing 38
users
adding, editing, and deleting 39
inviting 39

V

version control 37

W

web site 5
Windows
configuring proxy settings 25
Windows service
configuring Secure Agent login 26