



Informatica® Data Integration - Free & PayGo
April 2023

Runtime Environments

© Copyright Informatica LLC 2022, 2023

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: 2023-04-04

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: Runtime environments.....	 7
 Chapter 2: Hosted Agent.....	 8
 Chapter 3: Secure Agent groups.....	 10
Secure Agent groups with multiple agents.	10
Service assignment for Secure Agent groups.	11
Service assignment guidelines.	12
Enabling or disabling Secure Agent services for a Secure Agent group.	12
Enabling or disabling services and connectors for a Secure Agent group.	12
Working with Secure Agent groups.	13
Adding a Secure Agent to a group.	14
Adding a new Secure Agent to an existing group.	15
Removing a Secure Agent from a group.	15
Viewing Secure Agent group dependencies.	16
 Chapter 4: Secure Agents.....	 17
Working with Secure Agents.	17
Stopping and starting services on a Secure Agent.	20
Guidelines for stopping and starting Secure Agent services.	21
Stopping a Secure Agent service.	21
Starting a Secure Agent service.	21
Configuring agent blackout periods.	22
Overriding the blackout file name and directory.	23
Blackout file structure.	23
Renaming a Secure Agent.	24
Deleting a Secure Agent.	25
Upgrading a Secure Agent.	25
Secure Agent data encryption.	25

Changing the data encryption key on Windows.	26
Changing the data encryption key on Linux.	27
Secure Agent Manager.	28
Using a proxy server for the Secure Agent.	28
Configuring a proxy to exclude non-proxy hosts.	29
Stopping and restarting the Secure Agent on Windows.	29
Starting and stopping the Secure Agent on Linux.	29
Troubleshooting a Secure Agent.	30
Secure Agent errors.	31
Chapter 5: Secure Agent installation.	32
Secure Agent installation on Windows.	32
Secure Agent requirements on Windows.	32
Downloading and installing the Secure Agent on Windows.	33
Configure the proxy settings on Windows.	35
Configure a login for a Windows Secure Agent Service.	35
Uninstalling the Secure Agent on Windows.	36
Secure Agent installation on Linux.	36
Secure Agent requirements on Linux	37
Downloading and installing the Secure Agent on Linux.	38
Configure the proxy settings on Linux.	39
Uninstalling the Secure Agent on Linux.	39
Index.	40

Preface

Use *Runtime Environments* to learn how to create and configure runtime environments to use with Data Integration. Learn how to use the Informatica Intelligent Cloud Services Hosted Agent, download and install Secure Agents, create and configure Secure Agent groups, and troubleshoot Secure Agents.

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, go to <https://status.informatica.com/> and click **SUBSCRIBE TO UPDATES**. You can then 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 Customer Support Center by telephone or online.

For online support, click **Submit Support Request** in Informatica Intelligent Cloud Services. You can also use Online Support to log a case. Online Support requires a login. You can request a login at <https://network.informatica.com/welcome>.

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

Runtime environments

A runtime environment is the execution platform that runs Informatica Intelligent Cloud Services assets such as tasks and taskflows. 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 all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services.

You can set up runtime environments in the following ways:

Use the Informatica Cloud Hosted Agent.

When you use the Hosted Agent, you run tasks within the Informatica Cloud hosting facility. Informatica maintains the Hosted Agent runtime environment and agents. For more information about the Informatica Cloud Hosted Agent, see [Chapter 2, “Hosted Agent” on page 8](#).

Create one or more Secure Agent groups.

You can download and install one or more Secure Agents to run within your network or in a cloud computing services environment such as Amazon Web Services, Google Cloud, or Microsoft Azure. You can install one Secure Agent on each physical or virtual machine.

When you install a Secure Agent, it is added to its own group by default. You can add multiple agents to one Secure Agent group. For more information about Secure Agent groups, see [Chapter 3, “Secure Agent groups” on page 10](#).

When you configure a connection or some types of tasks, you specify the runtime environment to use. The runtime environment determines which agent runs the tasks at run time. If the runtime environment is the Hosted Agent, the Hosted Agent runs the tasks. If the runtime environment is a Secure Agent group, any available agent in the group can run the tasks.

CHAPTER 2

Hosted Agent

The Hosted Agent can run data loader and mapping 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 data loader and mapping tasks that use the following connectors:

- Amazon Redshift V2 Connector
- Amazon S3 V2 Connector
- Box Connector
- Coupa Connector
- Cvent Connector
- Databricks Delta Connector
- Eloqua Bulk API Connector
- Google Analytics Connector
- Google Big Query V2 Connector
- Google Cloud Spanner Connector
- Google Cloud Storage V2 Connector
- JIRA Connector
- Marketo V3 Connector
- Microsoft Azure Blob Storage V3 Connector
- Microsoft Azure Data Lake Storage Gen2 Connector
- Microsoft Azure SQL Data Warehouse V3 Connector
- Microsoft CDM Folders V2 Connector
- Microsoft Dynamics 365 for Operations Connector
- Microsoft Dynamics 365 for Sales Connector
- NetSuite Connector
- Microsoft SQL Server Connector
- MongoDB Connector
- MySQL Connector
- OData Connector
- Oracle Connector
- PostgreSQL Connector

- Salesforce Connector
- Salesforce Marketing Cloud Connector
- ServiceNow Connector
- Shopify Connector
- Snowflake Cloud Data Warehouse V2 Connector
- Stripe Connector
- SuccessFactors ODATA 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.

CHAPTER 3

Secure Agent groups

Use a Secure Agent group as the runtime environment when you need to access data on-premises or when you want to access data in a cloud computing services environment without using the Hosted Agent. When you select a Secure Agent group as the runtime environment for a connection or task, a Secure Agent within the group runs the tasks.

Create Secure Agent groups to accomplish the following goals:

Prevent the activities of one department from affecting another department.

To prevent the activities of one department from impacting a different department, create separate Secure Agent groups for each department. For example, users in the sales department run 10 times as many tasks as users in the finance department, but the finance tasks are more time critical. To prevent the sales tasks from impacting the finance tasks, create separate Secure Agent groups for each department. Then assign the sales tasks to one runtime environment and the finance tasks to the other runtime environment.

Separate tasks by environment.

You can create different Secure Agent groups for test and production environments. When you configure a connection, you can associate it with the test or production database by choosing the appropriate Secure Agent group as the runtime environment.

When you create a Secure Agent group, all users in the organization can select the Secure Agent group as the runtime environment.

You can add and remove Secure Agents from a group. You can also add multiple agents to a Secure Agent group.

If you need to access output files on the Secure Agent machine, you can view the **All Jobs** page in Monitor or the **My Jobs** page in Data Integration to determine where a task ran.

Secure Agent groups with multiple agents

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

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

Balance the workload across machines.

Add multiple agents to a group to balance the distribution of tasks across machines. When the runtime environment is a Secure Agent group with multiple agents, the group dispatches tasks and background processes such as metadata calls to the available agents in a round-robin fashion.

Improve scalability for connections and tasks.

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

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

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

Service assignment for Secure Agent groups

If your organization uses multiple services, demand on a Secure Agent group can be high. To reduce the potential demand on a Secure Agent group, you can enable and disable specific Secure Agent services for the group.

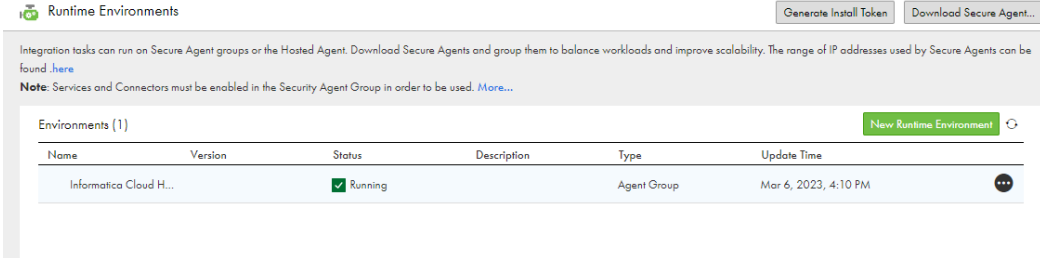
Enable Secure Agent services when you want the agents in the group to run the connections, tasks, processes, or product features associated with a service or set of services. When you enable a Secure Agent service, the service starts on each agent in the Secure Agent group.

Disable Secure Agent services when you do not want the agents in the group to run the connections, tasks, processes, or product features associated with a service or set of services. When you disable a Secure Agent service, the service stops on each agent in the Secure Agent group. Any connection, task, process, or product feature that uses the Secure Agent group as the runtime environment no longer runs.

You can also enable or disable Secure Agent services for individual Secure Agents within the Secure Agent group. For more information, see [“Stopping and starting services on a Secure Agent” on page 20](#).

For more information about Secure Agent services, see *Secure Agent Services*.

Enable or disable services and connectors for a Secure Agent group on the **Runtime Environments** page:



The screenshot shows the 'Runtime Environments' page. At the top, there are buttons for 'Generate Install Token' and 'Download Secure Agent...'. Below these, a note states: 'Integration tasks can run on Secure Agent groups or the Hosted Agent. Download Secure Agents and group them to balance workloads and improve scalability. The range of IP addresses used by Secure Agents can be found [here](#). Note: Services and Connectors must be enabled in the Security Agent Group in order to be used. [More...](#)'

The main section is titled 'Environments (1)' and contains a table with the following data:

Name	Version	Status	Description	Type	Update Time
Informatica Cloud H...		Running		Agent Group	Mar 6, 2023, 4:10 PM

There is a 'New Runtime Environment' button and a refresh icon at the top right of the table. A menu icon (three dots) is visible at the bottom right of the table row.

After you make service assignments for a Secure Agent group, you might add or remove agents. When you add a Secure Agent to a group, the agent inherits the service assignments of the group that you add it to.

Service assignment guidelines

Use the following guidelines when you enable and disable services or Secure Agent services for a Secure Agent group:

- Before you disable a service, verify that no connection, task, or process that uses the group as the runtime environment requires the service.

If a connection, task, or process has a Secure Agent group selected as the runtime environment and you disable a required service, the task or process cannot run. For example, the connection for a mapping source uses runtime environment RuntimeEnv1. If you disable Data Integration Server on RuntimeEnv1, the mapping task fails at run time.

- Do not disable a service to temporarily stop the service on a Secure Agent. For information about temporarily stopping a service on a Secure Agent, see [“Stopping and starting services on a Secure Agent” on page 20](#).

Enabling or disabling Secure Agent services for a Secure Agent group

If your organization does not have the Runtime Environments Selection license, you can enable or disable Secure Agent services for Secure Agent groups. When you disable a Secure Agent service, the service can no longer run on any agent in the Secure Agent group.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group and select **Enable or Disable Services**.
A list of all the services for the Secure Agent group is displayed.
3. Choose the services to enable or disable.
For more information, see the *Secure Agent Services* guide.
4. Click **OK**.
The changes affect every Secure Agent in the group.

Enabling or disabling services and connectors for a Secure Agent group

If your organization has the Runtime Environment Selections license, you can enable or disable Informatica Intelligent Cloud Services and connectors for a Secure Agent group. By default, all services and connectors are disabled in newly-created Secure Agent groups. Enable the services and connections you want to run on the group.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group and select **Enable or Disable Services and Connectors**.
A dialog box listing all the services and connectors for the Secure Agent group is displayed.
3. On the **Services** tab, choose the Informatica Intelligent Cloud Services to enable or disable.
Certain services may be listed in the **Additional Services** tab.
4. On the **Connectors** tab, choose the connectors to enable or disable.
5. On the **Additional Services** tab, select the Secure Agent services to enable or disable.

For example, if your organization uses source control, and you want to disable it on your Secure Agent group, disable the GitRepoConnectApp service.

The services that appear in this list vary based on your licenses. You might not see any services listed here.

6. Click **OK**.

The changes affect every Secure Agent in the group.

Working with Secure Agent groups

Create Secure Agent groups on the **Runtime Environments** page. After you create a Secure Agent group, you can rename or delete the group and add and remove Secure Agents.

Tip: Click the refresh icon next to **New Runtime Environment** to refresh the page before performing any actions on Secure Agent groups.

You can complete the following tasks:

Create a Secure Agent group.

To create a Secure Agent group, click **New Runtime Environment** and enter a name and optionally a description for the group. After you create a group, you can add Secure Agents to the group.

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

Rename a Secure Agent group.

To rename a Secure Agent group, expand the Actions menu, select **Edit Environment Properties**, and enter a new name for the group. Update the description if necessary. Informatica Intelligent Cloud Services updates the group name in all services that use the group.

Enable or disable Secure Agent services for a Secure Agent group.

To enable or disable Secure Agent services for a Secure Agent group, expand the Actions menu, select **Enable or Disable Services**, and select the services to enable or disable. You can enable or disable any service that your organization uses.

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

Add Secure Agents to a group.

To add Secure Agents to a group, expand the Actions menu and select **Add or Remove Secure Agents**. You can add any agent that is in the Unassigned Agents group on the **Runtime Environments** page.

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

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

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

Remove Secure Agents from a group.

To remove Secure Agents from a group, expand the Actions menu and select **Add or Remove Secure Agents**. When you remove an agent from a group, Informatica Intelligent Cloud Services adds it to a group named "Unassigned Agents."

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

Delete a Secure Agent group.

To delete Secure Agent group, expand the Actions menu and select **Delete**. You can delete a Secure Agent group if it does not contain any Secure Agents.

Share or unshare a Secure Agent group.

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

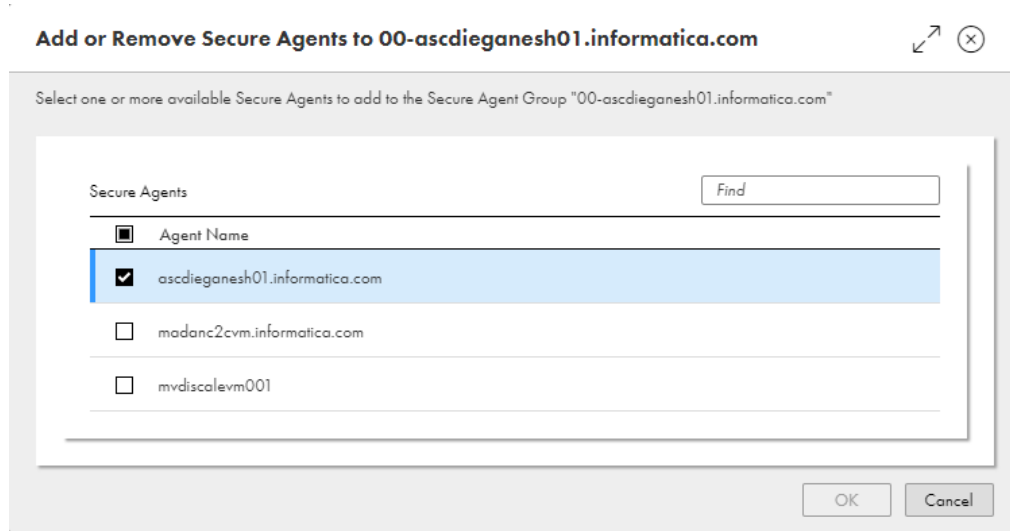
Adding a Secure Agent to a group

You can add any available Secure Agent to a Secure Agent group. Available agents appear in the "Unassigned Agents" group on the **Runtime Environments** page. You cannot add a Secure Agent to a group if the agent has already been added to another group.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group, and select **Add or Remove Secure Agents**.
3. In the **Secure Agents** list, enable the checkbox for the Secure Agents that you want to add to the group.

If the agent you want isn't listed, that means it is currently assigned to another group. You must remove an agent from a group before you can add it to a different group.

If there are many agents in the list, use the **Find** box to quickly locate an agent.



4. Click **OK**.

Adding a new Secure Agent to an existing group

You can add a Secure Agent to an existing Secure Agent group when you install the agent. To add a Secure Agent to an existing group, add the `InfaAgent.GroupName` property to the `infaagent.ini` file before you register the agent.

1. Install the Secure Agent.
2. On Windows, when you are prompted to register the agent, open Windows Services and stop the agent. On Linux, when the installation program finishes, do not start the agent.
3. Open `<Secure Agent installation directory>/apps/agentcore/conf/infaagent.ini` in a text editor.
4. Add the following property and save the file:
`InfaAgent.GroupName=<Secure Agent group name>`
5. Start the agent.
6. Register the agent.

Informatica Intelligent Cloud Services adds the Secure Agent to the group you specify in the `InfaAgent.GroupName` property instead of a new group.

Removing a Secure Agent from a group

You can remove an agent from a Secure Agent group if the group is not used in a connection or task. If the group is used in a connection or task, you can remove an agent if it is not the only agent in the group. When you remove a Secure Agent from a group, Informatica Intelligent Cloud Services adds it to a group named "Unassigned Agents."

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent group, and select **Add or Remove Secure Agents**.
3. In the list of **Secure Agents**, clear the check mark next to the agents that you want to remove from the group.

4. Click **OK**.

The Secure Agents that were removed appear in the "Unassigned Agents" group on the **Runtime Environments** page.

Viewing Secure Agent group dependencies

You can view object dependencies for Secure Agent groups.

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

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

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

USWPF3201 Dependencies

Uses



Used By

Used By (2)

↕

⌵

🔍

<input type="checkbox"/>	Name	Type	Location	Updated By	Status
<input type="checkbox"/>	 FF_USWPF3201	Connection		herry.smith	
<input type="checkbox"/>	 MappingTask2	Mapping Task	Default	herry.smith	Valid

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

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

CHAPTER 4

Secure Agents

The Informatica Cloud Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. When the Secure Agent runs a task, it connects to the Informatica Cloud hosting facility to access task information. It connects directly and securely to sources and targets, transfers data between them, orchestrates the flow of tasks, runs processes, and performs any additional task requirement.

If the Secure Agent loses connectivity to Informatica Intelligent Cloud Services, it tries to reestablish connectivity to continue the task. If it cannot reestablish connectivity, the task fails.

The Secure Agent uses pluggable microservices for data processing. For example, the Data Integration Server runs all data integration jobs and the Common Integration Components service runs the commands specified in a Command Task step of a taskflow. Each Secure Agent service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings. For more information about Secure Agent services, see *Secure Agent Services*.

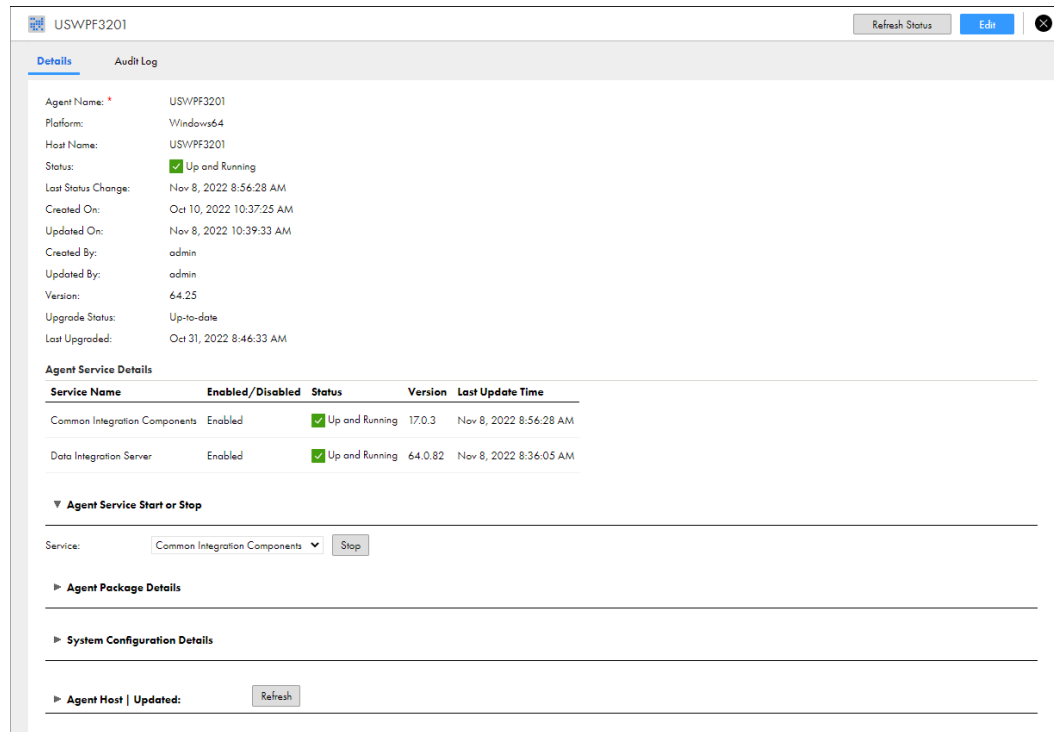
You can install and run one Secure Agent on a physical or virtual machine. After you install a Secure Agent, all users in the organization share the Secure Agent. You can configure the Secure Agent properties and move it to a different Secure Agent group. To improve scalability, you can also add multiple agents to a Secure Agent group.

Working with Secure Agents

After you create a Secure Agent, you might need to perform management tasks such as viewing and configuring agent properties, checking the host information, viewing audit logs, or refreshing the agent status. You can also delete a Secure Agent if it is no longer used.

You perform most management tasks for Secure Agents on the agent details page. To access the agent details page, click a Secure Agent on the **Runtime Environments** page.

The following image shows the agent details page:



You can complete the following tasks:

View the Secure Agent details.

View details such as the host name, the current status, the last date and time that the agent was updated, and the agent version.

The Secure Agent can have any of the following statuses:

Status	Description
Agent Core is not running.	The Secure Agent is not available, but one or more of the services is running.
Not all the services are running.	The Secure Agent is available, but one or more of the services is not available.
Agent Core Upgrading	The Secure Agent is upgrading to a new version.
Stopped	The Secure Agent is not available.
Up and Running	The Secure Agent and all of the services that the agent runs are available.

View the Secure Agent service details.

View details for Secure Agent services that run on the Secure Agent such as the service name, status, version, and last update time.

A Secure Agent service can have any of the following statuses:

Status	Description
Error	The process failed.
Restarting Due to Error	The service is starting due to a failure.
Shutting Down	The service is shutting down.
Standby	The service is running, but it is not compatible with Informatica Intelligent Cloud Services.
Starting Up	The service is starting up.
Stopped	The service is not available.
Up and Running	The service is running.
User Stopped	The service was stopped by a user.
Warning	The service is running, but it cannot accept work.

The version number changes each time you modify the service. The Secure Agent retains the directories for the old version of the service for seven days. For example, if you update the `NetworkTimeoutPeriod` for version 55.0.2 of the Data Integration Server, the agent increments the version number to 55.0.3 and creates the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/55.0.3.1
```

It deletes the `<Secure Agent installation directory>/apps/Data_Integration_Server/55.0.2.x` directories after seven days.

Stop and start Secure Agent services.

Stop and start the services that run on a Secure Agent to perform troubleshooting, optimize resources on the agent machine, or make service configuration changes. When you stop or start a Secure Agent service, other services that run on the agent are not affected.

View the Secure Agent package details.

Expand the **Agent Package Details** section to see the name and version number for the packages in each service that runs on the Secure Agent. You can filter the packages by service.

View and edit Secure Agent service properties.

Expand the **System Configuration Details** section to see the Secure Agent service properties. You can filter the properties by service and type.

To configure the properties, click **Edit**. You can configure properties for each service that runs on the Secure Agent. You can also add and remove custom properties, which are used by connectors. For more information about Secure Agent services and service properties, see *Secure Agent Services*. For more information about custom properties, see the help for the appropriate connector.

View the Secure Agent host properties.

Expand the **Agent Host** section to see information about the machine that hosts the Secure Agent. For example, you can view the machine name, operating system, and available disk space.

To refresh the information, click **Refresh**. The last date and time that the information was refreshed appears next to the **Agent Host | Updated** heading.

View the Audit Log.

To view audit information such as start and stop times, server connections, and upgrade messages, click **Audit Log**.

Refresh the Secure Agent status.

To refresh the status of the Secure Agent, click **Refresh Status** in the upper right corner of the page.

To view the status on Linux, you can also navigate to the following directory:

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

Then run one of the following commands:

```
./consoleAgentManager.sh getstatus  
./consoleAgentManager.sh updatestatus
```

Stopping and starting services on a Secure Agent

By default, each Secure Agent in an organization runs all microservices that are used for data processing in the organization. You can stop and start the microservices to perform troubleshooting, optimize resources on the agent machine, or make configuration changes. When you stop or start a Secure Agent microservice, other microservices that run on the agent are not affected.

The microservices that you stop and start on a Secure Agent are the Secure Agent services, which are different from the Informatica Intelligent Cloud Services. For example, the Data Integration Server runs data integration tasks such as data loader tasks and mapping tasks. For more information about Secure Agent services, see *Secure Agent Services*.

You might need to stop and restart a Secure Agent service to troubleshoot issues with a specific Secure Agent service. For example, if a Secure Agent service shows an error state, you can stop the service, troubleshoot the problem, and then restart the service.

Each time you start and restart a service, the Secure Agent creates a new subdirectory for the service-related files. For example, if the Secure Agent uses version 64.0.38 of the Data Integration Server, the Secure Agent installation directory contains the following subdirectory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/64.0.38.1
```

When you stop and restart the Data Integration Server, the Secure Agent creates the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/64.0.38.2
```

The Secure Agent does not delete the `.../64.0.38.1` directory.

Guidelines for stopping and starting Secure Agent services

Use the following guidelines when you stop and start services on a Secure Agent:

- Use caution when you stop Secure Agent services because this can cause job failures.

When you stop a Secure Agent service, any job that requires the service and is currently running on the agent stops. If there are no other agents in the group, the job can no longer run. If there are other agents in the group, you can restart the job and it will run on a different agent.

- Do not stop and start services to reserve a Secure Agent group for certain types of jobs.

If you want to reserve a Secure Agent group for certain types of jobs, you can enable the required services for the Secure Agent group and disable other services. For more information about enabling and disabling services for a Secure Agent group, see [“Service assignment for Secure Agent groups” on page 11](#).

Stopping a Secure Agent service

You can stop a Secure Agent service that is in the "Up and Running" or "Error" state. Stopping a Secure Agent service stops all versions of the service that are running. After a service stops, you can start the latest version of the service.

Note: If you stop a Secure Agent service and then restart the Secure Agent, the service remains stopped until you start it.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click the name of the Secure Agent.
Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
3. Click the **Details** tab.
4. In the **Agent Service Start or Stop** area, select the service that you want to stop.
5. Click **Stop**.

The Secure Agent service stops, and Informatica Intelligent Cloud Services adds an entry in the audit log indicating that the service was stopped by a user.

Starting a Secure Agent service

You can start a Secure Agent service that is in the "Stopped" state. Starting a Secure Agent service starts the latest version of the service.

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click the name of the Secure Agent.
Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
3. Click the **Details** tab.
4. In the **Agent Service Start or Stop** area, select the service that you want to start.
5. Click **Start**.

Informatica Intelligent Cloud Services attempts to start the Secure Agent service. After the service starts, the status changes to "Up and Running." If the Secure Agent service fails to start, check the audit log to find the cause of the error.

Configuring agent blackout periods

You can configure blackout periods for a Secure Agent. Blackout periods prevent data integration jobs from running on the agent during a certain period. Configure an agent blackout period to configure specific hours, days, or intervals in which no data integration jobs can run on the agent.

Agent blackout periods stop the Data Integration Server service from running jobs on a Secure Agent during the blackout period. They do not prevent other types of jobs from running on the agent. Configure an agent blackout period in the following circumstances:

- The Data Integration Server is the only service enabled on the agent and you want to stop all data integration jobs from running during a certain period.
- The Secure Agent runs multiple services and you want to stop only the data integration jobs from running during a certain period.

Note: The agent blackout period is different than the schedule blackout period for the organization. During an organization's schedule blackout period, no jobs can run on any agent. For more information about schedule blackout periods, see *Organization Administration*.

To configure a blackout period on a Secure Agent, you must create a blackout file. The blackout file is an XML file that specifies the repeat frequency, start date, and end date for each blackout period.

For example, the following blackout file contains two blackout periods: one blackout period from July 27, 2021, 5:00 AM through July 28, 2021, 11:00 PM and a second blackout period that repeats on Fridays from 2:00-4:00 PM:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
  <BlackoutWindow>
    <RepeatFrequency>OneTime</RepeatFrequency>
    <Start>2021-07-27 5:00:00</Start>
    <End>2021-07-28 23:00:00</End>
  </BlackoutWindow>
  <BlackoutWindow>
    <RepeatFrequency>Friday</RepeatFrequency>
    <Start>14:00:00</Start>
    <End>16:00:00</End>
  </BlackoutWindow>
</BlackoutWindows>
```

To configure one or more blackout periods, create a file named "blackoutWindows.dat" in the following directory on the Secure Agent machine:

```
<Secure Agent Installation Directory>\apps\Data_Integration_Server\conf\
```

If the Secure Agent is in a Secure Agent group, copy the blackout file to the ... \conf\ directory on each agent machine in the group.

If you want to use a different file name and directory, you can override the file name and file path.

After you create a blackout file, restart the Data Integration Server service on the Secure Agent so that the blackout periods take effect.

Overriding the blackout file name and directory

You can override the blackout file name and directory by setting the BlackoutWindowsFile Tomcat custom property for the Data Integration Server.

Set the following custom property for the Data Integration Server on the agent details page:

Service	Type	Name	Value
Data Integration Server	Tomcat	BlackoutWindowsFile	File path and file name for the blackout file. For example: C:/AgentBlackouts/Agent001Blackouts.dat Note: Use forward slashes (/) in the file path on both Windows and UNIX machines because the Secure Agent interprets backslashes (\) as escape characters. The file path must be accessible by the Secure Agent.

For more information about configuring custom properties for a Secure Agent service, see *Secure Agent Services*.

Blackout file structure

The blackout file is an XML file that contains elements that define each blackout period and the frequency, start time, and end time for each blackout period.

The blackout file has the following structure:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
  <BlackoutWindow>
    <RepeatFrequency></RepeatFrequency>
    <Start></Start>
    <End></End>
  </BlackoutWindow>
  <BlackoutWindow>
    <RepeatFrequency></RepeatFrequency>
    <Start></Start>
    <End></End>
  </BlackoutWindow>
  ...
</BlackoutWindows>
```

The file contains the following elements:

Element	Required/Optional	Description
BlackoutWindows	Required	Contains a BlackoutWindow element for each blackout period. Must contain one or more BlackoutWindow elements.
BlackoutWindow	Required	Defines one blackout period. Must contain one RepeatFrequency element, one Start element, and one End element.

Element	Required/ Optional	Description
RepeatFrequency	Required	Repeat frequency for the blackout period. Must contain one of the following values: <ul style="list-style-type: none"> - OneTime - Daily - Weekdays - Sunday - Monday - Tuesday - Wednesday - Thursday - Friday - Saturday
Start	Required	Blackout period start time in the format yyyy-mm-dd hh24:mi:ss. For example, 2019-07-25 10:26:55. The time zone is the Secure Agent time zone.
End	Required	Blackout period end time in the format yyyy-mm-dd hh24:mi:ss. For example, 2019-07-26 11:45:00. The time zone is the Secure Agent time zone.

Do not enclose element values in quotation marks.

Renaming a Secure Agent

By default, the name of a Secure Agent is the same as the name of the machine where you installed the agent. You can change the agent name.

- On the **Runtime Environments** page, click the name of the Secure Agent.
Note: You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
- Click the **Details** tab.
- In the upper right corner, click **Edit**.
- Enter a new name in the **Agent Name** field.
Note: If you use multi-byte characters in the Secure Agent name and the agent is in a cloud-hosted environment, verify that the environment also supports these characters.
- Click **Save**.

Deleting a Secure Agent

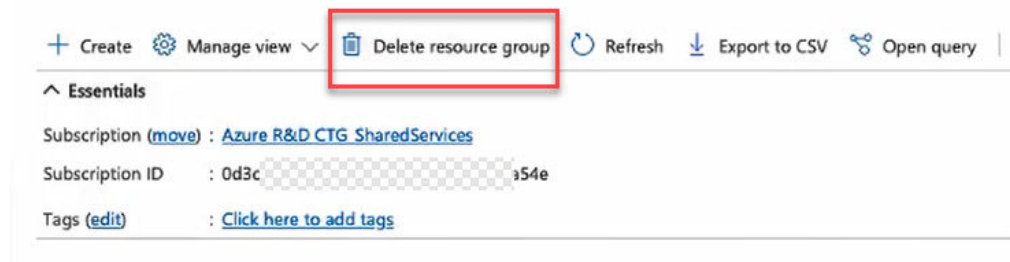
Delete a Secure Agent if you no longer need it to run tasks. Delete a Secure Agent on the **Runtime Environments** page.

Note: You cannot delete a Secure Agent if it is used in a connection or a task. For example, if the Secure Agent is the only agent in a group, and the group is used as the runtime environment for a connection or task, you cannot delete the agent.

1. In Administrator, select **Runtime Environments**.
2. Expand the Actions menu for the Secure Agent and select **Delete Secure Agent**.

If the Secure Agent is running, a warning message appears. Stopping an active Secure Agent prevents scheduled tasks associated with the Secure Agent from running. Ignore the warning if you do not need the Secure Agent.

3. From the Azure console, delete the resource group belonging to Secure Agent.



It is important to delete the resource group, otherwise the virtual machine may be left in a running state, incurring charges.

If you no longer need the Secure Agent, uninstall the Secure Agent after you delete it.

Upgrading a Secure Agent

The Secure Agent upgrades automatically the first time that you access a new Informatica Intelligent Cloud Services release. The upgrade process installs a new version of the Secure Agent, updates connector packages, and applies configuration changes for the microservices that run on the agent. You do not need to upgrade the Secure Agent manually.

Note: A Secure Agent can upgrade only if the agent version is the current major release and the agent is running. For example, the new major release upgrades the Secure Agent to version 65.x. To be upgraded, an agent must be version 64.x and must be running.

Secure Agent data encryption

The Secure Agent encrypts sensitive data that is stored in the Secure Agent directory. You can change the key that it is used to encrypt this data.

When you install a Secure Agent, some of the files in the Secure Agent directory contain sensitive data such as agent credentials, agent proxy credentials, and JDK keystore passwords. If you store connections on the

Secure Agent, files on the Secure Agent machine also store the connection credentials. This information is encrypted using a key that is unique to the Secure Agent.

The encryption key uses some machine-specific information. This prevents an attacker from copying the Secure Agent directory from one machine to a different machine and starting the agent on that machine.

By default, the encryption key is generated using the following properties:

- Operating system of the Secure Agent machine
- Machine architecture, for example, 32-bit, 64-bit, or 64-bit ARM
- Host name of the machine
- Hardware MAC address

You can prevent some of these properties from being used to generate the encryption key. For example, if you plan to back up the agent on one machine and restore it on a different machine, you might want to exclude the host name and hardware MAC address. You can also add other properties to make the encryption even more secure. For example, if the Secure Agent is installed on Amazon Web Services, you might add the instance ID or the AMI ID.

You can change the encryption key at any time. To do this, you use the `consoleAgentManager rotateDeviceKey` command.

The command performs the following actions:

- Re-encrypts the `infaagent.ini` and `proxy.ini` files.
- Re-encrypts the connection master key.
- Forces the redeployment of the Secure Agent services on the next startup.

After you run the command, you must also configure the following environment variables:

Environment variable	Description
<code>INFA_AGENT_EXCLUDE_SEC_PROPS</code>	Specifies the properties to exclude. Set the value to the same values you excluded in the <code>rotateDeviceKey</code> command.
<code>INFA_AGENT_ADDITIONAL_SEC_PROPS</code>	Specifies the properties to add. Set the value to the same values you added in the <code>rotateDeviceKey</code> command.

Changing the data encryption key on Windows

To change the Secure Agent data encryption key, use the `consoleAgentManager rotateDeviceKey` command.

Back up the Secure Agent installation directory before you change the data encryption key.

The user account you use to change the encryption key must have privileges to delete files in the Secure Agent installation directory and its subdirectories.

Note: During upgrade, there can be two versions of the Data Integration Server running within the maintenance window. Do not change the encryption key until the upgrade has completed and the newer version of the Data Integration Server is the only version that is running.

1. Stop the Secure Agent.
2. Open a command prompt as an administrator, and navigate to the following directory:

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

3. Run the following command:

```
consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<excluded security
properties> INFA_AGENT_ADDITIONAL_SEC_PROPS=<additional security properties>
```

You can exclude the following properties: `OS_TYPE`, `OS_ARCH`, `HOSTNAME`, and `HWD_MAC_ADDR`. Separate multiple properties with a comma.

Additional properties can be any key=value pair. For example, `instanceId=<AWS instance ID>`, `amiId=<AWS AMI ID>`. Separate multiple properties with a comma.

For example, to exclude the Secure Agent machine hostname and hardware MAC address from the encryption key and include the AWS instance ID, run the following command:

```
consoleAgentManager rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR
INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS instance ID>
```

4. When the command completes successfully, if you excluded security properties, create the system environment variable `INFA_AGENT_EXCLUDE_SEC_PROPS`, and set the value to the same values that you set in the `rotateDeviceKey` command.
5. If you added security properties, create the system environment variable `INFA_AGENT_ADDITIONAL_SEC_PROPS`, and set the value to the same values that you set in the `rotateDeviceKey` command.
6. Restart the machine.
7. If the Secure Agent doesn't start automatically, restart the Secure Agent.

Changing the data encryption key on Linux

To change the Secure Agent data encryption key, use the `consoleAgentManager rotateDeviceKey` command.

Back up the Secure Agent installation directory before you change the data encryption key.

Note: During upgrade, there can be two versions of the Data Integration Server running within the maintenance window. Do not change the encryption key until the upgrade has completed and the newer version of the Data Integration Server is the only version that is running.

1. Stop the Secure Agent.
2. Navigate to the following directory:

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

3. Run the following command:

```
./consoleAgentManager.sh rotateDeviceKey INFA_AGENT_EXCLUDE_SEC_PROPS=<excluded security
properties> INFA_AGENT_ADDITIONAL_SEC_PROPS=<additional security properties>
```

You can exclude the following properties: `OS_TYPE`, `OS_ARCH`, `HOSTNAME`, and `HWD_MAC_ADDR`. Separate multiple properties with a comma.

Additional properties can be any key=value pair. For example, `instanceId=<AWS instance ID>`, `amiId=<AWS AMI ID>`. Separate multiple properties with a comma.

For example, to exclude the Secure Agent machine hostname and hardware MAC address from the encryption key and include the AWS instance ID, run the following command:

```
./consoleAgentManager.sh rotateDeviceKey
INFA_AGENT_EXCLUDE_SEC_PROPS=HOSTNAME,HWD_MAC_ADDR
INFA_AGENT_ADDITIONAL_SEC_PROPS=instanceId=<AWS instance ID>
```

4. When the command completes successfully, if you excluded security properties, create the environment variable `INFA_AGENT_EXCLUDE_SEC_PROPS` in the source bash profile, and set the value to the same values that you set in the `rotateDeviceKey` command.

5. If you added security properties, create the environment variable `INFA_AGENT_ADDITIONAL_SEC_PROPS` in the source bash profile, and set the value to the same values that you set in the `rotateDeviceKey` command.
6. Restart the Secure Agent.

Secure Agent Manager

When you install the Secure Agent on Windows, you also install the Informatica Cloud Secure Agent Manager. The Secure Agent runs as a Windows service. You can launch the Secure Agent Manager from the Windows Start menu or the desktop icon.

Use the Secure Agent Manager to perform the following tasks:

- View the status of the Secure Agent and the services that the Secure Agent runs.
- Stop and restart the Secure Agent.
- Configure Windows settings such as proxy settings and a Windows Secure Agent service login.

The Secure Agent Manager displays the status of the Secure Agent and the services that the Secure Agent runs. If the Secure Agent or one of the services that the Secure Agent runs is not starting or not running, the Secure Agent Manager displays an alert message and a link that you can click to view details.

When you close the Secure Agent Manager, it minimizes to the Windows taskbar for quick access. Closing the Secure Agent Manager does not stop the Secure Agent. When the Secure Agent Manager is minimized, you can view the Secure Agent status by hovering over the Secure Agent Manager icon.

Using a proxy server for the Secure Agent

A proxy server allows indirect connection to network services for security and performance reasons. For example, you can use a proxy server to get through a firewall, and some proxies provide caching mechanisms.

When you configure a proxy server for the Informatica Cloud Secure Agent, you define the minimum required settings in the Secure Agent Manager. Informatica Intelligent Cloud Services updates the following file and adds other properties that you can edit manually:

`<Secure Agent installation directory>/apps/agentcore/conf/proxy.ini`

The following code shows the default contents of `proxy.ini`:

```
InfaAgent.ProxyPassword=ZU8KjIzgtVrVmFRMUPzPMw\=\=  
InfaAgent.ProxyNtDomain=  
InfaAgent.ProxyHost=foo.bar.com  
InfaAgent.ProxyPasswordEncrypted=true  
InfaAgent.NonProxyHost=localhost|127.*|[\:\:1]  
InfaAgent.ProxyUser=  
InfaAgent.ProxyPort=12345  
InfaAgent.AuthenticationOrder=
```

When you configure a proxy server for the Informatica Cloud Secure Agent, you can set `InfaAgent.NonProxyHost` to exclude certain IP addresses and host names from the proxy.

Configuring a proxy to exclude non-proxy hosts

In the `proxy.ini` file, set the property `InfaAgent.NonProxyHost` to exclude IP addresses or host names. By default, Informatica Intelligent Cloud Services adds `localhost` as the value for `InfaAgent.NonProxyHost` when you initially configure the proxy server.

1. Open `<Secure Agent installation directory>/apps/agentcore/conf/proxy.ini`.
2. Update the value for `InfaAgent.NonProxyHost` to specify the IP addresses or host names that you want to exclude.

For example:

- Local IP addresses:

```
InfaAgent.NonProxyHost=localhost|127.0.0.1|123.432.
```

- Host names:

```
InfaAgent.NonProxyHost=localhost|127.0.0.1|.foo.com
```

Note: You can combine a list of host names and IP addresses using the pipe character (`|`) as a delimiter. You can also enter a wildcard to the left for host names or to the right for IP addresses.

3. Restart the Secure Agent so that the changes take effect.

Stopping and restarting the Secure Agent on Windows

The Secure Agent Manager displays the Secure Agent status. You can use the Secure Agent Manager to stop or restart the Secure Agent.

Launch the Secure Agent Manager from the Windows **Start** menu. If the Secure Agent Manager is active, you can click the Informatica Cloud Secure Agent Manager icon in the Windows taskbar notification area to open the Secure Agent Manager.

To stop the Secure Agent from the Secure Agent Manager, click **Stop**. To restart the Secure Agent, click **Restart**. The Secure Agent Manager displays a message when the action is complete.

When you close the Secure Agent Manager, it minimizes to the Windows taskbar notification tray. Closing the Secure Agent Manager does not stop the Secure Agent.

Starting and stopping the Secure Agent on Linux

After you download the Secure Agent program files on a Linux machine, you can run the Secure Agent as a Linux process. Manually start the Secure Agent process on Linux.

1. From the command line, navigate to the following directory:

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

```
./infaagent.sh startup
```

3. To stop the Secure Agent, enter the following command:

```
./infaagent.sh shutdown
```

You can view the Secure Agent status from Informatica Intelligent Cloud Services or from a Linux command line.

Troubleshooting a Secure Agent

I installed the Secure Agent, but I want to install another on a different machine. How do I do that?

On the new machine, use your login to connect to Informatica Intelligent Cloud Services. Then, download and install the Secure Agent.

Why does my Secure Agent always display "Agent Core Upgrading" in Administrator?

On the **Runtime Environments** page in Administrator, the status of an agent always displays "Agent Core Upgrading". You see the following message in the `agentcore.log` file:

```
2022-10-11 17:02:57,560 GMT tid="21" tn="Agent Core State Machine Thread" ERROR
[com.informatica.saas.infaagent.agentcore.AgentCoreStateMachine] - Authentication failed
due to IO error: [cannot decrypt null or empty string].
```

This issue occurs when the agent missed one or more previous major upgrades. For example, you stopped an agent that was on version 62.x and the current version is 65.x when you restart it. The automatic upgrade only supports upgrading from the previous major version, 64.x. Since your version is older than version 64.x, the automatic upgrade fails.

To resolve the issue, either reregister or reinstall the Secure Agent.

You can see the agent version in the Details tab of a Secure Agent:

Details		Audit Log
Agent Name:	*	asCDIEHQILABS01
Platform:		Linux64
Host Name:		asCDIEHQILABS01
Status:		✓ Up and Running
Last Status Change:		Mar 1, 2023 10:14:27 AM
Created On:		Feb 6, 2023 10:23:46 AM
Updated On:		Mar 1, 2023 1:24:07 PM
Created By:		admin
Updated By:		agent
Version:		65.04
Upgrade Status:		Up-to-date
Last Upgraded:		Feb 15, 2023 7:29:53 AM

Secure Agent errors

I started the Secure Agent, but the status is inactive.

The Secure Agent might take a few minutes to start. The status refreshes every 5 seconds. If the Secure Agent does not become active, complete the following tasks:

- If your organization uses a proxy server to access the internet, verify that the proxy settings are set correctly.
- View the details in infaagent.log in the directory where you installed the Secure Agent.

The Secure Agent did not install or start correctly.

If the Secure Agent does not install or start correctly, complete the following tasks:

1. View the installation details in infaagent.log in the directory where you installed the Secure Agent.
2. View the application logs in the Event Viewer for a Secure Agent that runs on Windows.
3. From the Azure console, delete the resource group belonging to Secure Agent.

One of my services shows an error status after I restarted the service successfully.

If a service fails with an error status, the error status for the service might continue to display in the Agent Service Details after the service starts up successfully. The error stays on the page until an internal job that cleans up obsolete messages runs. You can ignore the error.

I am trying to uninstall the Secure Agent, but the Secure Agent status still shows "Up and Running."

When you uninstall the Secure Agent without first stopping the Secure Agent, the Agent Core and other services might continue to run for several minutes. To avoid this issue, stop the Secure Agent before you uninstall it.

After you uninstall the Secure Agent, delete the resource group belonging to that agent through the Azure portal. This shuts down the virtual machine, preventing further charges.

CHAPTER 5

Secure Agent installation

You can install a Secure Agent on Windows or Linux. You can also uninstall a Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Installation and uninstallation instructions vary based on your operating system.

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 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.

You can find the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs in [this Knowledge Base article](#) on Informatica Network or by clicking 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 there is, you must uninstall it.

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 Secure Agent Manager 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 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 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.

Uninstalling the Secure Agent on Windows

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. Click **Start > All Programs > Informatica Cloud Secure Agent > Uninstall Informatica Cloud Secure Agent**.

The Secure Agent uninstaller launches.

2. Click **Uninstall**.
3. When the uninstall completes, click **Done**.
4. Delete any remaining files in the installation directory.

After you uninstall the Secure Agent, delete all files and directories associated with the Secure Agent installation.

Note: Uninstalling the Secure Agent does not delete log files from the Secure Agent directory. If you want to reinstall a Secure Agent on the machine, you must delete all files and directories associated with the Secure Agent installation or reinstallation will fail. If you want to save the log files, copy them to a different directory, and then delete the Secure Agent installation directory.

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.
- Don't install more than one Secure Agent on the same machine.
- Don't install the Secure Agent on any node within the Informatica domain.

For more information about Secure Agent requirements, see this article:

<https://knowledge.informatica.com/s/article/526096>

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 environment variable `LD_LIBRARY_PATH` is set to the following location: `<Secure Agent installation directory>/apps/Data_Integration_Server/<version>/ICS/main/bin/rdtm`
- The account that you use to install the Secure Agent must have access to all remote directories that contain flat source 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.

You can find the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs in [this Knowledge Base article](#) on Informatica Network or by clicking 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.

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. You can update the proxy server settings defined for the Secure Agent from the command line.

To configure the proxy server settings for the Secure Agent on a Linux machine, use a shell command that updates the `proxy.ini` file. Contact the network administrator to determine the proxy settings.

1. Navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```
2. To update the `proxy.ini` file, enter the following command:

```
./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name>  
<proxy password>
```
3. Restart the Secure Agent.

Uninstalling the Secure Agent on Linux

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. From the command line, navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```
2. Stop the Secure Agent Linux process by entering the following command:

```
./infaagent shutdown
```
3. To uninstall the Secure Agent, run `rm -rf` on the directory where you installed the Secure Agent to remove Secure Agent files.

INDEX

A

allowlist

- Secure Agent domains [33, 37](#)
- Secure Agent IP addresses [33, 37](#)

B

blackout period

- configuring for a Secure Agent [22](#)
- overriding Secure Agent blackout file [23](#)
- Secure Agent blackout file structure [23](#)

C

Cloud Application Integration community

URL [5](#)

Cloud Developer community

URL [5](#)

D

Data Integration community

URL [5](#)

directories

configuring Secure Agent login to access [35](#)

F

firewall

configuration [33, 37](#)

H

Hosted Agent

description [8](#)

I

Informatica Global Customer Support

contact information [6](#)

Informatica Intelligent Cloud Services

web site [5](#)

L

Linux

- configuring proxy settings [39](#)
- starting and stopping the Secure Agent [29](#)

Linux (*continued*)

uninstalling the Secure Agent [39](#)

M

maintenance outages [6](#)

O

object dependencies

viewing for Secure Agent groups [16](#)

P

POD

how to identify [33, 37](#)

proxy settings

configuring on Linux [39](#)

configuring on Windows [29, 35](#)

R

requirements

Secure Agent [32, 37](#)

runtime environments

Hosted Agent [8](#)

enabling and disabling services [11, 12](#)

enabling and disabling services and connectors [12](#)

installing Secure Agents [32](#)

overview [7](#)

Secure Agent groups [10](#)

service assignment guidelines [12](#)

S

Secure Agent

troubleshooting [30](#)

Secure Agent connectors

enabling and disabling [12](#)

Secure Agent groups

adding and removing Secure Agents [13](#)

adding new agents to existing groups [15](#)

adding Secure Agents [14](#)

creating [13](#)

deleting [13](#)

enabling and disabling services [11–13](#)

enabling and disabling services and connectors [12](#)

overview [10](#)

removing Secure Agents [15](#)

renaming [13](#)

service assignment guidelines [12](#)

- Secure Agent groups (*continued*)
 - viewing dependencies [16](#)
- Secure Agent Manager
 - launching [32](#)
 - stopping and restarting the Secure Agent [29](#)
 - using [28](#)
- Secure Agent services
 - enabling and disabling [11](#), [12](#)
- Secure Agents
 - adding to Secure Agent groups [14](#)
 - blackout file structure [23](#)
 - changing the data encryption key on Linux [27](#)
 - changing the data encryption key on Windows [26](#)
 - communication port [33](#), [37](#)
 - configuring a Windows service login [35](#)
 - configuring blackout periods [22](#)
 - data encryption [25](#)
 - deleting [25](#)
 - domains allowlist [33](#), [37](#)
 - guidelines for starting and stopping services [21](#)
 - installing [32](#)
 - installing on Linux [38](#)
 - installing on Windows [33](#)
 - IP address allowlist [33](#), [37](#)
 - load balancing [10](#)
 - overriding blackout file [23](#)
 - overview [17](#)
 - permissions on Linux [37](#)
 - permissions on Windows [33](#)
 - registering on Linux [38](#)
 - registering on Windows [33](#)
 - removing from Secure Agent groups [15](#)
 - renaming [24](#)
 - requirements on Linux [37](#)
 - requirements on Windows [32](#)
 - rotateDeviceKey command [25](#)
 - scalability [10](#)
 - Secure Agent groups [10](#)

- Secure Agents (*continued*)
 - Secure Agent Manager [28](#)
 - starting a service [21](#)
 - starting and stopping on Linux [29](#)
 - starting and stopping services [20](#)
 - starting on Windows [32](#)
 - stopping a service [21](#)
 - stopping and restarting on Windows [29](#)
 - uninstalling on Linux [39](#)
 - uninstalling on Windows [36](#)
 - upgrading [25](#)
 - view details, refresh status [17](#)
- status
 - Informatica Intelligent Cloud Services [6](#)
- system status [6](#)

T

- troubleshooting
 - Secure Agent [30](#)
- trust site
 - description [6](#)

U

- upgrade notifications [6](#)

W

- web site [5](#)
- Windows
 - configuring proxy settings [29](#), [35](#)
- Windows service
 - configuring Secure Agent login [35](#)