



Informatica® Intelligent Cloud Services  
April 2024

# Secure Agent Services

Informatica Intelligent Cloud Services Secure Agent Services  
April 2024

© Copyright Informatica LLC 2021, 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](mailto: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: 2024-04-05

# Table of Contents

<b>Preface</b> .....	<b>6</b>
Informatica Resources. ....	6
Informatica Documentation. ....	6
Informatica Intelligent Cloud Services web site. ....	6
Informatica Intelligent Cloud Services Communities. ....	6
Informatica Intelligent Cloud Services Marketplace. ....	6
Data Integration connector documentation. ....	7
Informatica Knowledge Base. ....	7
Informatica Intelligent Cloud Services Trust Center. ....	7
Informatica Global Customer Support. ....	7
<b>Chapter 1: Secure Agent services</b> .....	<b>8</b>
Setting custom environment variables. ....	10
<b>Chapter 2: API Microgateway Service</b> .....	<b>11</b>
Editing the API Microgateway Service properties. ....	12
Enabling the API Microgateway Service in a Secure Agent or a Secure Agent group. ....	13
<b>Chapter 3: CMI Streaming Agent</b> .....	<b>14</b>
CMI Streaming Agent properties. ....	14
<b>Chapter 4: Common Integration Components</b> .....	<b>17</b>
Common Integration Components properties. ....	17
<b>Chapter 5: Database Ingestion service</b> .....	<b>20</b>
Database Ingestion service properties. ....	20
Database Ingestion Agent environment variables. ....	24
<b>Chapter 6: Data Integration Server</b> .....	<b>25</b>
Data Integration Server resiliency. ....	25
Data Integration Server properties. ....	26
Creating the OSProfileUserMappingFile. ....	29
Setting the OSProfileScriptForTaskExecution. ....	30
Data Integration Server upgrades. ....	31
<b>Chapter 7: Elastic Server</b> .....	<b>33</b>
Elastic Server properties. ....	33
Elastic Server concurrency. ....	35
<b>Chapter 8: File Integration Service</b> .....	<b>37</b>

<b>Chapter 9: GitRepoConnectApp.....</b>	<b>38</b>
Local repository base directory. . . . .	38
GitRepoConnectApp properties. . . . .	39
<b>Chapter 10: Mass Ingestion (Files).....</b>	<b>41</b>
<b>Chapter 11: Metadata Foundation Application.....</b>	<b>45</b>
Metadata Foundation Application properties. . . . .	45
<b>Chapter 12: Metadata Platform Service.....</b>	<b>50</b>
Metadata Platform Service properties. . . . .	50
<b>Chapter 13: Process Server.....</b>	<b>56</b>
Process Server properties. . . . .	56
Default connection database properties. . . . .	63
Logging levels. . . . .	63
Configuring a separate logging data source . . . . .	63
Process Server sizing recommendations. . . . .	64
Communication with the Secure Agent. . . . .	67
Secure Agent configurations for Process Server. . . . .	67
Deploy to a single Secure Agent. . . . .	68
Deploy to a Secure Agent group. . . . .	69
Prerequisites for PostgreSQL database installation and upgrade. . . . .	72
Managing the PostgreSQL database on Windows. . . . .	72
Backing up the PostgreSQL database on Windows. . . . .	73
Restoring the PostgreSQL database on Windows. . . . .	73
Resetting the PostgreSQL database on Windows. . . . .	73
Starting the PostgreSQL server on Windows. . . . .	73
Stopping the PostgreSQL server on Windows. . . . .	74
Getting the PostgreSQL server status on Windows. . . . .	74
Vacuuming the PostgreSQL database on Windows. . . . .	74
Reindexing the PostgreSQL database on Windows. . . . .	74
Resetting transaction logs on Windows. . . . .	75
Managing the PostgreSQL database on Linux. . . . .	75
Backing up the PostgreSQL database on Linux. . . . .	76
Restoring the PostgreSQL database on Linux. . . . .	76
Resetting the PostgreSQL database on Linux. . . . .	76
Starting the PostgreSQL server on Linux. . . . .	77
Stopping the PostgreSQL server on Linux. . . . .	77
Getting the PostgreSQL server status on Linux. . . . .	77
Vacuuming the PostgreSQL database on Linux. . . . .	77
Reindexing the PostgreSQL database on Linux. . . . .	78

Resetting transaction logs on Linux. . . . .	78
Upgrading the PostgreSQL database. . . . .	78
Upgrading the PostgreSQL database using the replication technique. . . . .	79
PostgreSQL configuration files. . . . .	79
Configuring PostgreSQL log rotation. . . . .	80
Configuring public certificates and private keys for Process Server. . . . .	80
Configuring thread pool profile to improve throughput. . . . .	82
Overriding properties in the platform.yaml file. . . . .	84
Creating a custom user-platform.yaml file. . . . .	84
Troubleshooting. . . . .	85
<b>Chapter 14: SecretManagerApp. . . . .</b>	<b>86</b>
<b>Chapter 15: Configuring Secure Agent service properties. . . . .</b>	<b>87</b>
<b>Index. . . . .</b>	<b>89</b>

# Preface

Use *Secure Agent Services* to learn about the microservices that the Informatica Intelligent Cloud Services™ Secure Agent uses for data processing. Learn how to configure service properties.

## 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](mailto: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](mailto: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

## Secure Agent services

Secure Agent services are pluggable microservices that the Secure Agent uses for data processing. For example, the Secure Agent uses the Data Integration Server to run data integration jobs and Process Server to run application integration and process orchestration jobs. Each Secure Agent service runs independently of the other services that run on the agent.

The independent services architecture provides the following benefits:

- The Secure Agent does not restart when you add a connector or package.
- Services are not impacted when another service restarts. For example, process orchestration jobs continue to run when the Data Integration Server restarts.
- Downtime during upgrades is minimized. The upgrade process installs a new version of the Secure Agent, updates connector packages, and applies configuration changes for the Data Integration Server and Database Ingestion agent service. To minimize downtime, the old agent remains available and continues to run data integration jobs during the upgrade. The new version of the Secure Agent runs jobs that start after the upgrade process completes.

The services that run on a Secure Agent vary based on your licenses and the Informatica Intelligent Cloud Services that are enabled for the Secure Agent group.

The following table describes the Secure Agent services that can run on an agent and the Informatica Intelligent Cloud Services that use them:

Secure Agent service	Description	Used by...
API Microgateway Service	Manages Application Integration processes that run on the Secure Agent.	Application Integration, API Manager
B2B Processor	Runs B2B Gateway inbound and outbound process flows. <b>Note:</b> Do not change the values of the service properties unless Informatica Global Customer Support instructs you to do so.	B2B Gateway
CIH Processor	Runs Cloud Integration Hub publications and subscriptions for organizations that use a private publication repository.	Cloud Integration Hub
CMI Streaming Agent	Runs streaming ingestion jobs in the Mass Ingestion service.	Mass Ingestion service
Common Integration Components	Runs the shell scripts or batch commands in a Command Task step of a taskflow.	Data Integration
Database Ingestion	Runs application ingestion and database ingestion jobs in the Mass Ingestion service.	Mass Ingestion service



Secure Agent service	Description	Used by...
Data Integration Server	Runs data integration jobs such as mapping, task, and taskflow instances.	B2B Gateway, Cloud Integration Hub, Data Accelerator for Azure, Data Integration Data Profiling
Domain Management App	Connects on-premises CDI-PC domains with Informatica Intelligent Cloud Services and handles backend domain update tasks.	Cloud Data Integration for PowerCenter (CDI-PC)
EDC Search Agent	Discovers Enterprise Data Catalog data assets for Data Accelerator for Azure and for data catalog discovery in Data Integration. <b>Note:</b> Do not change the values of the service properties unless Informatica Global Customer Support instructs you to do so.	Data Accelerator for Azure, Data Integration
Elastic Server	Manages an advanced cluster and the jobs that run on the cluster.	Data Integration
File Integration Service	Uses file transfer protocols such as HTTPS, AS2, and SFTP to receive files from a remote server or to send files to a remote server, or both.	B2B Gateway, Data Integration
GitRepoConnectApp	Manages communication between Informatica Intelligent Cloud Services and the source control repository when your organization uses an on-premises source control repository.	All Informatica Intelligent Cloud Services that use source control
Mass Ingestion	Runs file ingestion tasks and file listener jobs. <b>Note:</b> Do not change the values of the service properties unless Informatica Global Customer Support instructs you to do so.	Mass Ingestion service
Metadata Foundation Application	Extracts metadata from the configured source systems in your organization, and uploads the extracted metadata to Metadata Command Center through the Secure Agent.	Metadata Command Center
Metadata Platform Service	Performs profiling activities for the jobs that you run in Metadata Command Center. <b>Note:</b> Profiling fails if there is no active Metadata Platform Service present in the runtime environment of Metadata Command Center.	Metadata Command Center
OI Data Collector	Runs the Operational Insights data collectors that collect the operational data and domain-related metadata from PowerCenter, Data Engineering Integration, and Data Quality. <b>Note:</b> Do not change the values of the service properties unless Informatica Global Customer Support instructs you to do so.	Operational Insights

Secure Agent service	Description	Used by...
Process Server	Runs application integration processes, connectors, and connections.	Application Integration, Application Integration Console
SecretManagerApp	Manages communication between Informatica Intelligent Cloud Services and your secrets manager when your organization uses an external secrets manager like AWS Secrets Manager or Azure Key Vault.	Data Integration

Each Secure Agent service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings. You might need to configure a service or change the service properties to optimize performance or if you are instructed to do so by Informatica Global Customer Support. You configure a Secure Agent service independently from other services that run on the agent.

## Setting custom environment variables

You can customize your environment by adding scripts or variables to the `custom_env_settings.sh` script.

If you need to set custom environment variables for any of the services, add them to a script file named `custom_env_settings.sh` and place this file in the directory where the Secure Agent is installed.

For example, the following script ensures that your custom variables are automatically set up after you upgrade the agent:

```
$ pwd
/apps/cloudagent/apps/Data_Integration_Server/65.0.3.1/.lcm
$ ls lcm-env.sh
lcm-env.sh
```

## CHAPTER 2

# API Microgateway Service

The API Microgateway Service manages Application Integration processes that run on the organization's on-premises Secure Agent. Use the API Microgateway Service to expose managed APIs as API Microgateway proxies.

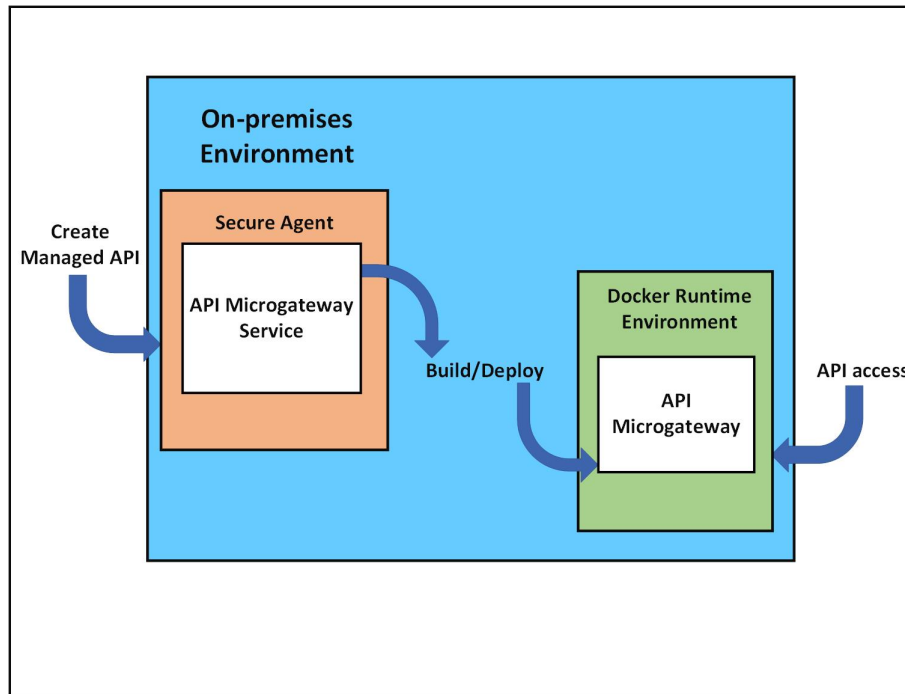
You can use the following methods to control access to managed APIs that you publish with the API Microgateway Service:

- IP filtering policy
- Rate limit policy
- Basic authentication or OAuth 2.0 authentication

The API Microgateway Service provides REST APIs to create and deploy API Microgateway proxies. API consumers access the managed APIs deployed as API Microgateway proxies on the organization's on-premises environment. The Application Integration processes expose REST Service URL and SOAP Service URL endpoints.

Use the API Microgateway Service to build an API Microgateway proxy to an API endpoint to manage. The API Microgateway Service builds an API Microgateway as an immutable Docker image on the organization's Secure Agent machine. You then use the API Microgateway Service to deploy the Docker image in a container on the Secure Agent Docker runtime environment for API access. The API Microgateway applies the API access policies that you configure before forwarding the requests to Application Integration endpoints.

The following diagram shows the API Microgateway Service and API Microgateway components exposing a managed API in the on-premises environment:



The Secure Agent Docker runtime environment hosts the Docker images using the blue-green deployment strategy to provide zero downtime during updates of the API Microgateway component.

## Editing the API Microgateway Service properties

Edit the API Microgateway Service properties in Administrator.

The following image shows the API Microgateway Service properties you can edit in the **System Configuration Details** area:

▼ System Configuration Details

---

Service:

Type:

Type	Name	Value
AGENT_RUNTIME_SETTINGS	project-name	'project1'
AGENT_RUNTIME_SETTINGS	docker-registry-name	'info.agent.apimgw'
DOCKER_CONTAINER_SETTINGS	blue	<a href="#">http-port: '16090'</a> <a href="#">https-port: '16095'</a>
DOCKER_CONTAINER_SETTINGS	green	<a href="#">http-port: '17090'</a> <a href="#">https-port: '17095'</a>
DOCKER_CONTAINER_SETTINGS	haproxy	<a href="#">http-port: '6090'</a> <a href="#">https-port: '6095'</a>

The following table describes the API Microgateway Service configurations:

Type	Name	Description
AGENT_RUNTIME_SETTINGS	project-name	Name of the project that stores the API configurations. You can change the name as per requirement, for example when you create a new project. <b>Note:</b> Project name must not contain the characters /or /0. If a project name includes restricted characters, the project creation fails.
AGENT_RUNTIME_SETTINGS	docker-registry-name	Name of the local Docker registry that contains all the named and tagged API Microgateway Docker images on the Secure Agent machine. <b>Note:</b> Docker image and tag names must not contain the following characters: - _ , . If a Docker image or tag name includes restricted characters, the image build fails.
DOCKER_CONTAINER_SETTINGS	blue	First Docker image container that deploys on the Secure Agent machine, alternates with green. You can change the following ports of the blue container: - http-port. The default value is: 16090 - https-port. The default value is: 16095
DOCKER_CONTAINER_SETTINGS	green	Second Docker image container that deploys on the Secure Agent machine, alternates with blue. You can change the following ports of the green container: - http-port. The default value is: 17090 - https-port. The default value is: 17095
DOCKER_CONTAINER_SETTINGS	haproxy	Router of the Docker image containers on the Secure Agent machine. Switches traffic between blue and green containers. You can change the following ports of the haproxy container: - http-port. The default value is: 6090 - https-port. The default value is: 6095

**Note:** To stop the API Microgateway, stop all three Docker image containers.

## Enabling the API Microgateway Service in a Secure Agent or a Secure Agent group

If you want to change the Secure Agent that runs the API Microgateway Service, enable the API Microgateway Service for a Secure Agent or a Secure Agent group in Administrator. When you enable API Microgateway Service for a Secure Agent group, it is enabled for all the Secure Agents in the group and for any Secure Agent that you later add to the group.

1. Navigate to the **Runtime Environments** page and select **Enable or Disable Services, Connectors** from the **Actions** menu of a Secure Agent or a Secure Agent group.  
The **Enable/Disable Components in Agent** window appears.
2. Select **API Microgateway** from the list of services and click **Save**.  
API Microgateway Service is enabled for the Secure Agent or the Secure Agent group.

## CHAPTER 3

# CMI Streaming Agent

Use the CMI Streaming Agent to define and deploy streaming ingestion tasks. You configure streaming ingestion tasks in the Mass Ingestion service.

A CMI Streaming Agent runs on an on-premise system and works in conjunction with the Mass Ingestion Streaming service. In an on-premise system, the CMI Streaming Agent runs the jobs deployed by Mass Ingestion Streaming. The agent provides status and statistics updates of each job.

On Linux, the CMI Streaming Agent does not start if the agent installation directory name contains a space. The agent returns a connection timeout status. After a few restart attempts, the agent goes into the error state.

**Note:** Prior to Spring 2020 April release of Informatica Intelligent Cloud Services Mass Ingestion service, CMI Streaming Agent was called Streaming Ingestion Agent.

## CMI Streaming Agent properties

To change or optimize the behavior of the CMI Streaming Agent, configure agent properties for your run-time environment. Configure CMI Streaming Agent properties in the **System Configuration Details** area when you edit a Secure Agent.

You can configure Engine, Agent, and Script properties of a CMI Streaming Agent.

The following image shows some of the CMI Streaming Agent properties:

▼ **System Configuration Details**

Service:	CMI Streaming Agent ▼	
Type:	All Types ▼	
Type	Name	Value
Engine	MaxLogFileSize	'5MB'
Engine	LogLevel	'DEBUG'
Agent	DataflowPullInterval	60
Agent	JVM	'-Xms256M -Xmx256M'
Agent	LogLevel	'DEBUG'
Agent	MaxLogFileSize	'10MB'
Agent	MaxNumberOfBackups	5
Scripts	LogLevel	'DEBUG'
Scripts	MaxFileSize	'5MB'
Scripts	MaxBackupIndex	5

You can configure the following CMI Streaming Agent properties:

Type	Property Name	Description
Engine	MaxLogFileSize	The maximum size of the log file that the engine can create. Default is 5 MB.
Engine	LogLevel	The log level for the engine.
Agent	DataflowPullInterval	The time interval after which the agent checks for updates in the task. Default is 60 seconds.
Agent	JVM	List of JVM properties for the agent. For example: [-Xms256M -Xmx256M]
Agent	LogLevel	The log level for the agent.
Agent	MaxLogFileSize	Maximum size of the log files that an agent can create. Default is 10 MB.

Type	Property Name	Description
Agent	MaxNumberOfBackups	Maximum number of backup log files for the agent. Default is 5.
Scripts	LogLevel	The log level of the scripts.
Scripts	MaxFileSize	The maximum file size after which the log rolls over and creates a new file. Default is 10 MB.
Scripts	MaxBackupIndex	Maximum number of backup files maintained after rolling over. Default is 5.



## CHAPTER 4

# Common Integration Components

The Common Integration Components service is the Secure Agent service that runs the commands specified in a Command Task step of a taskflow.

To view and configure the Common Integration Components service, you must have the license for the Common Integration Components service and command executor package.

You can optimize the performance of the Common Integration Components service by configuring some of its service properties. You can change service properties when you edit the Secure Agent.

All the requests that Common Integration Components service processes are logged in the following directory:

```
<Secure Agent installation directory>\apps\Common_Integration_Components\logs\<version>
```

You can view the log file for each command task in the following directory:

```
<Secure Agent installation directory>\apps\Common_Integration_Components\logs\command  
\<Command_job ID>
```

In a serverless runtime environment, the Secure Agent pushes the log file for each command task to Amazon S3.

## Common Integration Components properties

To change or optimize the behavior of the Common Integration Components service, configure its properties in the **System Configuration Details** section when you edit a Secure Agent.

The following image shows some of the Common Integration Components service properties:

### ▼ System Configuration Details

Service:

Type:

Type	Name
Tomcat	NetworkTimeoutPeriod
Tomcat	JRE_OPTS
Platform	LCM_JRE_OPTS
SYSTEM_CFG	HTTP_CONNECTION_TIMEOUT_SECONDS
SYSTEM_CFG	HTTP_SOCKET_TIMEOUT_SECONDS
COMMAND_CFG	MaximumConcurrentJobs

You can configure the following Common Integration Components service properties:

Type	Name	Description
Tomcat	JRE_OPTS	JRE VM options for the Apache Tomcat process.
Platform	LCM_JRE_OPTS	JRE options to start, stop, or get the status of the Apache Tomcat process. <b>Note:</b> Do not change the value of this property unless Informatica Global Customer Support instructs you to do so.
SYSTEM_CFG	HTTP_CONNECTION_TIMEOUT_SECONDS	The maximum amount of time, in seconds, that the Secure Agent waits to set up an HTTP connection to communicate with Informatica Intelligent Cloud Services. Default is 60. <b>Note:</b> Do not change the value of this property unless Informatica Global Customer Support instructs you to do so.
SYSTEM_CFG	HTTP_SOCKET_TIMEOUT_SECONDS	The maximum amount of idle time, in seconds, during the data packet transfer over an HTTP connection between the Secure Agent and Informatica Intelligent Cloud Services. Default is 60. <b>Note:</b> Do not change the value of this property unless Informatica Global Customer Support instructs you to do so.

Type	Name	Description
COMMAND_CFG	MaximumConcurrentJobs	<p>The maximum number of concurrent command tasks that can be executed by a single Secure Agent.</p> <p>The default value is 10 for each Secure Agent in a Secure Agent group.</p> <p>For example, if there are 3 Secure Agents in a Secure Agent group, the maximum number of concurrent command tasks that the service can handle is 30.</p> <p>Any command execution requests beyond the maximum limit are queued and are executed when a Secure Agent is available.</p>
<p><b>Note:</b> Do not change the values of other Common Integration Components service properties unless Informatica Global Customer Support instructs you to do so.</p>		

## CHAPTER 5

# Database Ingestion service

Mass Ingestion Applications and Mass Ingestion Databases use the Database Ingestion agent service to run ingestion jobs.

After you download the Secure Agent to your runtime environment and enable the Database Ingestion service, the Database Ingestion packages are pushed to the on-premises system where the Secure Agent runs. You can then optionally configure properties for the Database Ingestion service that runs on the Secure Agent.

## Database Ingestion service properties

To change or optimize the behavior of the Database Ingestion service that your Secure Agent group uses, configure Database Ingestion properties for your runtime environment.

To configure the properties, open your runtime environment and click **Edit**. Under **System Configuration Details**, select the **Database Ingestion** service and the **DBMI\_AGENT\_CONFIG** type.

The following table describes the Database Ingestion agent service properties:

Property	Description
maxTaskUnits	<p>The maximum number of application ingestion task units and database ingestion task units that can run concurrently on an on-premises machine where the Secure Agent is running.</p> <p>Task units are not related to the capacity and availability of your hardware or software. You can configure maxTaskUnits to precisely control CPU usage. Valid values are 1 to 2000000000 (2 billion).</p> <p>To calculate a reasonable number of task units for your Secure Agent machine, Informatica recommends that you divide the number of cores by 3 or 4. For example, if you have an 8-core machine, you could set this property to 2. Then monitor CPU usage and adjust the property value as needed to tune performance.</p> <p>During initial load processing, this property determines the number of tables that can be unloaded simultaneously. Remaining tables are queued and start unload processing when resources become available.  <b>Note:</b> A single job can process many tables. The total number of tables that can be processed is limited only by available memory. On the average, 25 MB of RAM is required per table for an initial load task based on a 1 KB row size.</p> <p>During incremental load processing, this property determines the number of application ingestion and database ingestion jobs that can run simultaneously.</p> <p>Setting this property to a value greater than the number of cores on the Secure Agent machine can increase parallelism for task execution but also cause performance bottlenecks at task execution time.</p>
serviceLogRetentionPeriod	<p>The number of days to retain each internal Database Ingestion service log file after the last update is written to the file. When this retention period elapses, the log file is deleted. The default value is 7 days.</p> <p>Service logs are retained on the Secure Agent host where they are created: &lt;infaagent&gt;/apps/Database_Ingestion/logs.</p> <p><b>Note:</b> This property is applicable to both Mass Ingestion Applications and Mass Ingestion Databases.</p>
taskLogRetentionPeriod	<p>The number of days to retain each job log file after the last update is written to the file. When this retention period elapses, the log file is deleted. The default value is 7 days.</p>

Property	Description
ociPath	<p>For Oracle sources and targets, the path to the Oracle Call Interface (OCI) directory that contains the oci.dll or libclntsh.so file. By default, Oracle uses \$ORACLE_HOME/lib on Linux or %ORACLE_HOME%\bin on Windows. The OCI library is used by database ingestion CDC tasks to connect to Oracle.</p> <p>For a DBMI agent that is running, this value is appended to the PATH environment variable value on Windows or to the LD_LIBRARY_PATH environment variable value on Linux. This property is not required if you already included the OCI path in the PATH or LD_LIBRARY_PATH environment variable.</p> <p><b>Note:</b> This property is applicable only to Mass Ingestion Databases.</p>
serviceUrl	<p>The URL that the Database Ingestion service uses to connect to the Informatica Intelligent Cloud Services cloud.</p> <p><b>Note:</b> This property is applicable to both Mass Ingestion Applications and Mass Ingestion Databases.</p>
logLevel	<p>The level of detail to include in the logs that the Database Ingestion service produces. Options are:</p> <ul style="list-style-type: none"> <li>- TRACE</li> <li>- DEBUG</li> <li>- INFO</li> <li>- WARN</li> <li>- ERROR</li> </ul> <p>The default value is TRACE.</p> <p><b>Note:</b> This property is applicable to both Mass Ingestion Applications and Mass Ingestion Databases.</p>
taskExecutionHeapSize	<p>The maximum heap size, in gigabytes, for the Task Execution service. This value, in conjunction with maxTaskUnits property, affects the number of concurrent application ingestion and database ingestion tasks that can run on a Secure Agent. Try increasing the heap size to run more tasks concurrently. Enter this value followed by "g" for gigabytes, for example, '9g'. The default value is '8g'.</p> <p><b>Note:</b> This property is applicable to both Mass Ingestion Applications and Mass Ingestion Databases.</p>
useProxy	<p>Set this property to true to enable the DBMI Agent to go through a proxy when connecting to or writing data to targets. The DBMI Agent then uses the proxy settings from the Secure Agent proxy configuration. By default, proxy settings are not used.</p> <p><b>Note:</b> This property is applicable to both Mass Ingestion Applications and Mass Ingestion Databases.</p>
intermediateStorageDirectory	<p>For incremental load and combined initial and incremental load jobs, the local root directory under which intermediate files that contain data are stored when the <b>Enable Persistent Storage</b> option is selected in the associated task definitions.</p> <p><b>Note:</b> This property is applicable only to Mass Ingestion Databases.</p>

Property	Description
storageBackupDirectory	<p>For incremental load and combined initial and incremental load jobs, the path to the directory that stores backup files when the <b>Enable Persistent Storage</b> option is selected in the associated task definitions.</p> <p><b>Note:</b> This property is applicable only to Mass Ingestion Databases.</p>
storageProperties	<p>For incremental load and combined initial and incremental load jobs, a comma-separated list of key=value pairs that is used when the <b>Enable Persistent Storage</b> option is selected in the associated task definitions. Specify this property only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> This property is applicable only to Mass Ingestion Databases.</p>
task_container.jvm.allowExceptionForInvalidEncodedData	<p>If you receive transliteration errors that report invalid encoding to UTF-8, and you do not want to repair or correct the source data, set this property to false so that database ingestion jobs do not fail when trying to unload the data from the source. With this setting, the Database Ingestion service passes an equivalent Java property to the DataDirect JDBC driver to prevent the exception from occurring. After you set this property, you must restart the Database Ingestion service.</p> <p><b>Note:</b> This property is applicable only to Mass Ingestion Databases.</p>

# Database Ingestion Agent environment variables

To change or optimize the behavior of the Database Ingestion Agent, define the following environment variables:

Environment Variable	Description
DBMI_REPLACE_UNSUPPORTED_CHARS	<p>For Microsoft Azure Synapse Analytics targets, controls whether an application ingestion job or database ingestion job replaces characters in character data that the target cannot process correctly. To enable character replacement, set this environment variable to true.</p> <pre>DBMI_REPLACE_UNSUPPORTED_CHARS=true</pre> <p>Mass Ingestion Applications or Mass Ingestion Databases then uses the character that is specified in the DBMI_UNSUPPORTED_CHARS_REPLACEMENT environment variable to replace unsupported characters.</p>
DBMI_UNSUPPORTED_CHARS_REPLACEMENT	<p>If the DBMI_REPLACE_UNSUPPORTED_CHARS environment variable is set to true, specifies the character that replaces the characters in source data that a Microsoft Azure Synapse Analytics target cannot process correctly.</p> <p>Default value: ? (question mark)</p> <p><b>Note:</b> Define this environment variable only for Mass Ingestion Databases.</p>
DBMI_WRITER_CONN_POOL_SIZE	<p>Indicates the number of connections that an application ingestion job or database ingestion job uses to propagate the change data to the target. The default value is 8. Valid values are 4 through 8.</p>
DBMI_WRITER_RETRIES_MAX_COUNT	<p>If a network issue occurs while a database ingestion job is loading source data to an Amazon S3 or Microsoft Azure Data Lake Storage Gen2 target, indicates the maximum number of times that the database ingestion job retries a request to continue the initial load or incremental load. If all of the retries fail, the job fails.</p> <p>The default value is 5.</p>
DBMI_WRITER_RETRIES_INTERVAL_IN_MILLIS	<p>Specifies the time interval, in milliseconds, that a database ingestion job waits before retrying the request to continue the initial load or incremental load to an Amazon S3 or Microsoft Azure Data Lake Storage Gen2 target if a network issue occurs.</p> <p>The default value is 1000.</p>

**Note:** After you define or change an environment variable, restart the Database Ingestion Agent for the changes to take effect.



## CHAPTER 6

# Data Integration Server

The Data Integration Server is the Secure Agent service that runs data integration jobs such as mapping, task, and taskflow instances.

If an advanced cluster processes data logic in a mapping in advanced mode, the Data Integration Server defers the advanced cluster subtask to the Elastic Server.

You can optimize performance of the Data Integration Server by configuring some of its service properties. For example, you might want to change the network resiliency settings or the connection timeout period for the Secure Agent. You can change service properties when you edit the Secure Agent.

## Data Integration Server resiliency

During temporary network issues, data integration tasks can continue to run while the Secure Agent tries to reestablish a connection. You can configure network resiliency properties for the Data Integration Server.

The following Data Integration Server properties determine how the Secure Agent tries to reestablish a connection:

### **NetworkTimeoutPeriod**

Determines the length of time that the Secure Agent tries to reestablish communication with Informatica Intelligent Cloud Services. If communication is not established at the end of the time period, data integration tasks that were in progress stop running. The default value is 300 seconds.

### **NetworkRetryInterval**

Determines the frequency with which the Secure Agent tries to contact Informatica Intelligent Cloud Services within the specified timeout period. The default value is five seconds.

For example, with the default settings, if the network is down, the Secure Agent tries to reestablish communication with Informatica Intelligent Cloud Services for 300 seconds. During the 300-second period, the Secure Agent tries to contact Informatica Intelligent Cloud Services every five seconds. If the Secure Agent reestablishes communication within the 300-second period, data integration tasks that are in progress are not affected. If the Secure Agent is unable to reestablish communication within the 300-second period, the Secure Agent stops all data integration tasks that are in progress.

# Data Integration Server properties

To change or optimize behavior of the Data Integration Server, configure the Data Integration Server properties. Configure Data Integration Server properties in the **System Configuration Details** area when you edit a Secure Agent.

The following image shows some of the Data Integration Server properties:

▼ System Configuration Details

---

Service:

Type:

Type	Name	Value
Tomcat	NetworkTimeoutPeriod	300
Tomcat	NetworkRetryInterval	5
Tomcat JRE	INFA_SSL	
Tomcat JRE	INFA_MEMORY	'-Xms32m -Xmx512m -XX:MaxPermSize=128m'
Tomcat JRE	JRE_OPTS	'-Xrs'
Tomcat JRE	JAVA_LIBS	
Tomcat Log4j	log4j_rootLogger	'INFO, tomcatLog'
Tomcat Log4j	log4j_appender_tomcatLog	'org.apache.log4j.FileAppender'
Tomcat Log4j	log4j_appender_tomcatLog_layout	'org.apache.log4j.PatternLayout'
Tomcat Log4j	log4j_appender_tomcatLog_layout_ConversionPattern	'%d %d{z} %p [%c] - %m%n'

You can configure the following Data Integration Server properties:

Type	Name	Description
Tomcat	NetworkTimeoutPeriod	Amount of time, in seconds, that the Secure Agent tries to reestablish communication with Informatica Intelligent Cloud Services. Default is 300.
Tomcat	NetworkRetryInterval	Frequency, in seconds, in which the Secure Agent tries to contact Informatica Intelligent Cloud Services within the specified timeout period. Default is 5.
Tomcat	INFA_DTM_STAGING_ENABLED_CONNECTORS	Applies to certain Cloud Data Warehouse connectors. Enables the Data Integration Server to optimize staging target data in a local flat file before loading the data to the target. To optimize staging, set this property to the plugin ID of the connector. For more information, see the help for the appropriate connector.

Type	Name	Description
Tomcat	INFA_DTM_RDR_STAGING_ENABLED_CONNECTORS	<p>Applies to certain Cloud Data Warehouse connectors.</p> <p>Enables the Data Integration Server to optimize the staging of source data in a local flat file after reading the data from the source.</p> <p>To optimise staging, set this property to the plugin ID of the connector.</p> <p>For more information, see the help for the appropriate connector.</p>
Tomcat	INFA_DTM_LKP_STAGING_ENABLED_CONNECTORS	<p>Applies to certain Cloud Data Warehouse connectors.</p> <p>Enables the Data Integration Server to optimize the staging of lookup data in a local flat file after reading the data from the lookup object.</p> <p>To optimize staging, set this property to the plugin ID of the connector.</p> <p>For more information, see the help for the appropriate connector.</p>
Tomcat JRE	JRE_OPTS	JRE VM options for the Apache Tomcat process.
Tomcat JRE	INFA_MEMORY	JRE VM options that are set for virtual machine memory for the Apache Tomcat process.
DTM	AgentConnectionTimeout	Number of seconds that the Secure Agent communication requests to wait before it times out. Default is 5.
DTM	JVMOption1 - JVMOption5	<p>JVM options that configure advanced properties for the Data Integration Server such as the maximum and minimum JVM heap size, the maximum record size for Intelligent Structure Discovery, or proxy settings for certain connectors. For example, to change the maximum JVM heap size from the default value of 512 MB to 2048 MB, you might set JVMOption1 to <code>'-Xmx2048m'</code>.</p> <p>By default, you can configure up to five advanced properties using JVMOption1 through JVMOption5. To configure additional properties, you can add custom DTM properties for the Data Integration Server named JVMOption6, JVMOption7, etc. Ensure that the option numbers are sequential and that you do not skip numbers.</p> <p>For information about the JVM options that you can set, see the Data Integration help, the help for the appropriate connector, or the <a href="#">Knowledge Base</a> on Informatica Network.</p>

Type	Name	Description
OS_PROFILE	EnableOSProfileForTaskExecution	<p>Enables or disables the OS Profile functionality. Values are true or false. Default is false.</p> <p><b>Note:</b> The OS Profile functionality is only available in Linux.</p> <p>By default, tasks run with the same operating user as the Secure Agent. When you enable the OS Profile functionality, you can run tasks with a different operating system user.</p> <p>For example, you have different departments using the same Informatica Intelligent Cloud Services installation and you need isolation.</p> <p><b>Tip:</b> You can view the name of the OS Profile user in the session log for completed tasks.</p>
OS_PROFILE	FailTasksForMissingOsProfileMapping	<p>If the OS Profile functionality is enabled, this property fails a task if the mapping to the operating system user for a given task is missing. Values are true or false. Default is true.</p> <p>Set this property to false to not fail the task in this scenario and instead run the task with the Secure Agent's operating system user.</p>
OS_PROFILE	ShareSystemDirectories	<p>Shares the system directories that were created for the Secure Agent user with the operating system user. Values are true or false. Default is false.</p> <p>Enable sharing if you want to share information such as user parameters. However, for improved isolation and reduced possibility of errors, don't share these directories.</p> <p>The default behavior creates new system directories for the operating system user under <code>Data_Integration_Server/data/osprofiles_filesystem/&lt;profile_name&gt;</code></p> <p>The system directories save mapping information, sessions logs, and user parameters.</p>
OS_PROFILE	OSProfileUserMappingFile	<p>Location of the YAML file that contains mapping information between the Secure Agent user or location and the operating system user.</p> <p>Changes to the mapping file apply automatically, without needing to restart the Secure Agent.</p> <p>For more information about this property, see <a href="#">"Creating the OSProfileUserMappingFile" on page 29.</a></p>

Type	Name	Description
OS_PROFILE	OSProfileScriptForTaskExecution	Location of the script file that will be used for task execution. For more information about this property, see <a href="#">"Setting the OSProfileScriptForTaskExecution" on page 30.</a>
<p><b>Note:</b> Do not change the values of other Data Integration Server properties unless Informatica Global Customer Support instructs you to do so.</p>		

## Creating the OSProfileUserMappingFile

When defining OS\_PROFILE properties, you need to create a YAML file that contains mapping information between the Secure Agent user or location and the operating system user. This is set in the OSProfileUserMappingFile property in the Data Integration Server service.

Create a YAML file using the following example as a template:

```
- profileName: userprofile1
  profileType: USER
  systemNames:
  - osp_idmc_1
  osMapping:
    osUser: osprofileuser1
    pmVariables:
      PMRootDir: /home/osprofileuser1/pmdata
      PMSessionLogDir: /mnt/shared/Vadi/osprofile
      PMBadFileDir: /home/osprofileuser1/pmbadfile
      PMCacheDir: /home/osprofileuser1/pmcache
      PMTargetFileDir: /home/osprofileuser1/pmtrgtfile
      PMSourceFileDir: /home/osprofileuser1/pmsrcfile
      PmExtProcDir: /home/osprofileuser1/pmextproc
      PMTempDir: /home/osprofileuser1/pmtemp
      PMLookupFileDir: /home/osprofileuser1/pmlookupfile
      PMStorageDir: /data/agent/userparam
- profileName: userprofile2
  profileType: USER
  systemNames:
  - osp_idmc_2
  osMapping:
    osUser: osprofileuser2
- profileName: locationprofile1
  profileType: LOCATION
  systemNames:
  - osprofilefoldertest1
  - osprofiletestfolder2
  osMapping:
    osUser: osprofileuser1
- profileName: locationprofile2
  profileType: LOCATION
  systemNames:
  - osprofilefoldertest1\test
  - osprofiletestfolder\test
  osMapping:
    osUser: osprofileuser2
```

The following table describes each property in the YAML file:

Property	Description
profileName	Name of the profile. Must be unique. This property is required.
profileType	Describes whether this mapping is based on the Secure Agent user or location. Valid values are USER or LOCATION. <b>Note:</b> If both User and Location profile types are specified for the same task, then User has the higher precedence.
systemNames	This section contains a list of Informatica Intelligent Cloud Services (IICS) system names. - If profileType = USER, then the system names are a list of IICS users. - If profileType = LOCATION, then the system names are a list of IICS location names. Use the absolute path for every location.
osMapping	This section contains a mapping to the operating system.
osUser	The operating system user.
pmVariables	A list of the PM variables to override. The following variables can be overridden: - PMRootDir - PMSessionLogDir - PMBadFileDir - PMCacheDir - PMTargetFileDir - PMSourceFileDir - PmExtProcDir - PMTempDir - PMLookupFileDir <b>Note:</b> The override directories must be accessible by both Secure Agent and operating system users. To ensure this, add both the Secure Agent and operating system users to the profile OS user group.

## Setting the OSProfileScriptForTaskExecution

When defining OS\_PROFILE properties, you need to define a script that will be used for task execution. This is set in the OSProfileScriptForTaskExecution property in the Data Integration Server service.

Choose one of the following methods to create your OS profile script:

- Configure the `pmimpprocess` executable. This is the recommended method because it is more secure.
- Use the default script provided by Informatica.

Use the following table to help you decide which method to use:

Method	Advantage	Disadvantage
Use <code>pmimpprocess</code> (recommended)	More secure, with the one time sticky bit set as root.	More difficult to customize, as <code>pmimpprocess</code> is an executable. The sole purpose of this executable is to switch users.
Use default script	Easily customizable. For example, you need to configure Kerberos.	Requires the Secure Agent user to be able to <code>sudo</code> , which means adding the user to <code>/etc/sudoer</code> . Once this is done, the user assumes near root-user privileges, which is less secure.

## Configuring the pmimpprocess

To configure the OS profile script using `pmimpprocess`, perform the following steps:

1. Locate the `pmimpprocess` process in the following location:  

```
<Secure Agent installation directory>/downloads/package-  
ICSAGENTruntime.<latest_version>/package/ICS/main/bin/rdtm
```
2. Copy `pmimpprocess` to the Secure Agent.  
For example:  

```
<Secure Agent installation directory>/infaagent/apps/Data_Integration_Server/ext/  
pmimpprocess
```
3. Run the following command to change the permissions of `pmimpprocess`:  

```
chmod 755 pmimpprocess
```
4. Log in as the root user or sudo as root.
5. Run the following command to change the ownership and access permissions of `pmimpprocess`:  

```
chown root:root pmimpprocess  
chmod u+s pmimpprocess
```
6. Enter the location of `pmimpprocess` for the value of the `OSProfileScriptForTaskExecution` property in ["Data Integration Server properties" on page 26](#).  
For example:  

```
/home/agent/infaagent/apps/Data_Integration_Server/ext/pmimpprocess
```

## Using the default script

If you prefer to use the script method, locate the script in the following location:

```
Data_Integration_Server/ext/infa-osprofile-dtm.sh
```

**Note:** The script method is intended for advanced technical users only.

The following illustration shows the default script:

```
#!/bin/sh  
input_args="$@"  
env_var_file=$(mktemp)  
chmod +r "${env_var_file}"  
printenv | sed 's/\([^=]*\)=(.*)/export \1="\2"/'>"${env_var_file}"  
echo "sudo su - ${ENV_INFA_DTM_OSPROFILE_USER} -c . ${env_var_file}; cd ${PWD}; ${  
{input_args}" >/tmp/xx  
sudo su - ${ENV_INFA_DTM_OSPROFILE_USER} -c ". ${env_var_file}; cd ${PWD}; ${input_args}"  
exit_code=$?  
rm "${env_var_file}"  
exit "${exit_code}"
```

Update the script as appropriate to meet your needs.

# Data Integration Server upgrades

The Data Integration Server upgrades automatically when a new version is available.

Data Integration Server upgrades are automatic and don't require any user intervention. When an upgrade is available, a new version of the Data Integration Server starts up and the old version stops after processing all jobs. If there are long-running jobs such as CDC continuous extraction jobs, the upgrade process terminates the job on the old version of the Data Integration Server and restarts them as new jobs on the upgraded version.

When this happens, the original job shows as a failed status with the following message on the My Jobs page:

```
Job stopped for Data Integration Server upgrade and will resume as a new job on the upgraded service.
```

The original job is replaced by a new job with a different instance name.

For more information about configuring mapping tasks for CDC continuous extraction, see the help for the appropriate connector in the online help.



# CHAPTER 7

## Elastic Server

The Elastic Server is the Secure Agent service that manages an advanced cluster and the jobs that run on the cluster.

You can configure service properties to specify details about the cloud platform that hosts the advanced cluster, such as the cluster operator role and the Secure Agent role in an AWS environment. You can also configure properties to specify access to parameter files, the level of detail that the Elastic Server writes to log files, and concurrency settings.

For more information about advanced clusters, see *Advanced Clusters*.

## Elastic Server properties

To change the behavior of the Elastic Server, configure the Elastic Server properties in the **System Configuration Details** area when you edit a Secure Agent.

The following image shows the Elastic Server properties:

Type	Name	Value	Sensitive
PARAMFILE_CFG	parameterfile_access_flag	'true'	<input type="checkbox"/>
PARAMFILE_CFG	parameterfile_access_directory	'/\$AGENT_HOME/apps/data/userparameters, /\$AGENT_HOME/apps/Data_Integration_Server/data/userparameters'	<input type="checkbox"/>
LOG4J_CFG	log4l_app_log_level	'INFO'	<input type="checkbox"/>
AWS_CFG	agent_role_external_id_key		<input type="checkbox"/>
AWS_CFG	privileged_role_arn_key	<input type="text" value="arn:aws:iam::&lt;account id&gt;:role/cluster_operator_role"/>	<input type="checkbox"/>
AWS_CFG	role_session_duration_secs_key		<input type="checkbox"/>
AWS_CFG	aws_regional_endpoint_enabled	'false'	<input type="checkbox"/>
AZURE_CFG	azure_agent_role_identity_client_id		<input type="checkbox"/>
CONCURRENCY_CFG	allow_queuing	'true'	<input type="checkbox"/>
CONCURRENCY_CFG	max_concurrent_jobs		<input type="checkbox"/>

You can configure the following Elastic Server properties:

Type	Name	Description
PARAMFILE_CFG	parameterfile_access_flag	Indicates whether developers can download parameter files that are stored on the Secure Agent machine. Default is 'true.'
PARAMFILE_CFG	parameterfile_access_directory	List of directories on the Secure Agent machine that allow parameter file download. Developers can download parameter files from any of the specified directories or subdirectories. Default is '\$AGENT_HOME/apps/data/userparameters, \$AGENT_HOME/apps/Data_Integration_Server/data/userparameters.'
LOG4J_CFG	log4j_app_log_level	Level of detail that the Elastic Server writes to log files. Enter the logging level as a string, such as 'INFO.'  As the logging level increases, the messages that the Elastic Server writes to log files include the messages in the prior logging levels. For example, if the logging level is INFO, the log contains FATAL, ERROR, WARNING, and INFO code messages.  The following values are valid: <ul style="list-style-type: none"> <li>- FATAL. Includes nonrecoverable system failures that cause the service to shut down or become unavailable.</li> <li>- ERROR. Includes connection failures, failures to save or retrieve metadata, and service errors.</li> <li>- WARNING. Includes recoverable system failures or warnings.</li> <li>- INFO. Includes system and service change messages.</li> <li>- TRACE. Logs user request failures.</li> <li>- DEBUG. Logs user request logs.</li> </ul>
AWS_CFG	agent_role_external_id_key	External ID that the Secure Agent specifies when the agent attempts to assume the cluster operator role. Required if you configure an external ID in the trust relationship of the cluster operator role.  This property takes effect only in an AWS environment.
AWS_CFG	privileged_role_arn_key	ARN of the cluster operator role.  Required when you set up separate cluster operator and Secure Agent roles in an AWS environment.  This property takes effect only in an AWS environment.
AWS_CFG	role_session_duration_secs_key	Session duration of the AWS AssumeRole API in seconds. By default, the session duration is 1800 seconds (30 minutes).  Overrides the maximum CLI/API session duration that is configured for the cluster operator role. If the session duration configured for the Elastic Server is longer than session duration for the cluster operator role, the Secure Agent might fail to assume the cluster operator role.  This property takes effect only in an AWS environment.

Type	Name	Description
AZURE_CFG	azure_agent_role_identity_client_id	Client ID of the managed identity <code>agent_identity</code> . Required when <code>agent_identity</code> is a user-assigned managed identity and the Secure Agent machine has at least one other managed identity. This property takes effect only in an Azure environment.
CONCURRENCY_CFG	allow_queuing	Indicates whether the Elastic Server queues Spark tasks. Default is true.
CONCURRENCY_CFG	max_concurrent_jobs	Maximum number of concurrent Spark tasks that the Elastic Server can process.

## Elastic Server concurrency

The Elastic Server can process Spark tasks concurrently and queue additional Spark tasks. You can configure concurrency properties to enable or disable queuing and set the maximum number of concurrent Spark tasks.

The following Elastic Server properties define queuing and concurrency:

### **allow\_queuing**

Allows the Elastic Server to queue Spark tasks. The default value is set to true.

If this property is set to false, the Elastic Server processes all submitted Spark tasks concurrently. If you set the maximum number of concurrent tasks on the Elastic Server to a value that is higher than the default concurrency, increase the Java heap size accordingly. Otherwise, the Secure Agent process might crash.

The Elastic Server processes data preview and SQL ELT optimization jobs immediately without queuing them.

### **max\_concurrent\_jobs**

Maximum number of concurrent Spark tasks that the Elastic Server can process. When the Elastic Server reaches the maximum number of concurrent Spark tasks, additional Spark tasks can be queued.

By default, the maximum number of concurrent Spark tasks depends on the cloud platform. The Elastic Server uses the following defaults for fully-managed and self-service clusters:

- 500 concurrent Spark tasks per 2 GB of Java heap space on AWS
- 375 concurrent Spark tasks per 2 GB of Java heap space on Google Cloud
- 250 concurrent Spark tasks per 2 GB of Java heap space on Microsoft Azure

A local cluster can run 15 concurrent Spark tasks, and the concurrency can't be changed.

Note that the Java heap size is set to 2 GB by default. If you set the maximum number of concurrent tasks to a value that is higher than the default, increase the Java heap size using the default ratios.

For example, if you want to run 500 concurrent Spark tasks on Microsoft Azure, increase the Java heap size to 4 GB. If the Java heap size remains at 2 GB, the Elastic Server will process a maximum of 250 concurrent Spark tasks and the remaining 250 Spark tasks can be queued.

The Elastic Server uses an upper bound of 1,000 Spark tasks per 2 GB of Java heap space. If you set the maximum number of concurrent tasks to a value that is higher than 1,000 without increasing the Java heap size above 2 GB, the Elastic Server fails to start.

For more information about Secure Agent machine sizing, see *Data Integration Performance Tuning*.

## CHAPTER 8

# File Integration Service

Use the File Integration Service to transfer files between your organization and remote file servers.

The File Integration Service is a Secure Agent service that the agent uses to run advanced file transfer protocols such as AS2.

You must configure file servers before your organization can receive files from remote partners. Configure your organization's file server associated with the File Integration Service on the File Servers page in Administrator. Configuration includes properties such as file server details, encryption methods, and allowed file types.

To stop or start the File Integration Service, you stop or start the file server that uses the service.

For information about configuring file servers, see *File Servers*.

To use the File Integration Service, your organization must have the appropriate license. To configure the File Integration Service, you must be assigned the Admin role.

## CHAPTER 9

# GitRepoConnectApp

When your organization uses an on-premises source control repository, the GitRepoConnectApp service manages the communication between Informatica Intelligent Cloud Services and the source control repository.

The Secure Agent uses the GitRepoConnectApp service when it creates the local copy of the remote source control repository on the Secure Agent machine. It also uses the service to get information about source control operations from the remote repository.

## Local repository base directory

If your source control repository is on-premises, the Secure Agent creates a local copy of the repository branch that stores Informatica Intelligent Cloud Services assets. You can configure the local repository location on the Secure Agent machine.

By default, the Secure Agent creates the local repository in the following directory:

```
<Secure Agent installation directory>/apps/GitRepoConnectApp/<base directory>/<client URL>/<organization ID>/<branch>/<remote repository name>
```

In this file path, the base directory is controlled by the **git\_local\_repository\_path** property of the GitRepoConnectApp service.

By default, **git\_local\_repository\_path** is set to `../data/git_repository/`. Therefore, the Secure Agent creates the local Git repository in the following directory:

```
<Secure Agent installation directory>/apps/GitRepoConnectApp/data/git_repository/<client URL>/<organization ID>/<branch>/<remote repository name>
```

You can change the base directory by editing the **git\_local\_repository\_path** property. For example, if you set this property to `../MYREPO/PROD`, the Secure Agent creates the local Git repository in the following directory:

```
<Secure Agent installation directory>/apps/GitRepoConnectApp/MYREPO/PROD/<client URL>/<organization ID>/<branch>/<remote repository name>
```

To specify a base directory that contains a backslash character (`\`), escape it with another backslash character.

Use the following guidelines when you set the `git_local_repository_path` property:

- If you omit the parent directory (..) when you set this property, the Secure Agent creates a subdirectory for the version of the GitRepoConnectApp service. The local copy of the repository is then stored in the following directory:

```
<Secure Agent installation directory>/apps/GitRepoConnectApp/<GitRepoConnectApp version>/  
<base directory>/<client URL>/<organization ID>/<branch>/<remote repository name>
```

In this case, the Secure Agent creates a new local repository directory each time the GitRepoConnectApp service is updated, which can consume large amounts of disk space on the Secure Agent machine.

- Do not configure this property in such a way that the local repository directory is shared by multiple agents. Each Secure Agent machine must have its own local copy of the repository.

## GitRepoConnectApp properties

To change or optimize behavior of the GitRepoConnectApp service, configure the service properties. Configure the service properties in the **System Configuration Details** area when you edit a Secure Agent.

The following image shows the GitRepoConnectApp properties:

▼ System Configuration Details

---

Service:

Type:

Type	Name	Value
LOG4J	rootLogger	'INFO'
GIT_REPO_CONNECT_APP_CONF	host	'localhost'
GIT_REPO_CONNECT_APP_CONF	address	'127.0.0.1'
GIT_REPO_CONNECT_APP_CONF	git_local_repository_path	'../data/git_repository/'
GIT_REPO_CONNECT_APP_CONF	JVM_MIN_MEMORY	'32m'
GIT_REPO_CONNECT_APP_CONF	JVM_MAX_MEMORY	'256m'

You can configure the following service properties:

Type	Name	Description
GIT_REPO_CONNECT_APP_CONF	git_local_repository_path	<p>Base directory for the local Git repository on the Secure Agent machine.</p> <p>The base directory is created in the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/GitRepoConnectApp/</pre> <p>Default is <code>../data/git_repository/</code>. Therefore, the Secure Agent creates the local Git repository in the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/GitRepoConnectApp/data/git_repository/&lt;client URL&gt;/&lt;organization ID&gt;/&lt;branch&gt;/&lt;remote repository name&gt;</pre>
GIT_REPO_CONNECT_APP_CONF	JVM_MIN_MEMORY	<p>Amount of memory allocated for the GitRepoConnectApp service when the service starts.</p> <p>Default is 32 MB.</p>
GIT_REPO_CONNECT_APP_CONF	JVM_MAX_MEMORY	<p>Maximum memory allocated for the GitRepoConnectApp service.</p> <p>Default is 256 MB.</p>
<p><b>Note:</b> Do not change the values of other GitRepoConnectApp properties unless Informatica Global Customer Support instructs you to do so.</p>		



## CHAPTER 10

# Mass Ingestion (Files)

To change or optimize the behavior of Mass Ingestion Files that your Secure Agent group uses, configure Mass Ingestion properties for your runtime environment in Administrator.

You can configure the following properties:

Type	Name	Description
AGENT_RUNTIME_SETTINGS	file-listener-snapshot-dir	A directory where the snapshots of a new file listener components are added. You can add the following directory paths: <ul style="list-style-type: none"><li>- A path relative to the <code>MassIngestionRuntime</code> directory. For example, <code>../data/monitor</code>.</li><li>- The absolute path. For example, <code>&lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/monitor</code> where <i>Secure agent installation directory</i> is the name of the directory where the secure agent is installed.</li></ul> <b>Note:</b> Use the snapshot directory shared with all agents when multiple Secure Agents are present in a group.
AGENT_RUNTIME_SETTINGS	mi-task-workspace-dir	A directory in the agent that file ingestion tasks use as an intermediate staging area when transferring files to a target. The directory is a custom location in the agent. The path can be a shared location, mounted location, or a location apart from the default location in the agent.
AGENT_RUNTIME_SETTINGS	mi-task-project-dir	A directory where the file ingestion task stores the project files. The directory is a custom location in the agent. The path can be a shared location, mounted location, or a location apart from the default location in the agent.
AGENT_RUNTIME_SETTINGS	mi-task-logs-dir	A directory where the file ingestion task stores the task logs files. The directory is a custom location in the agent. The path can be a shared location, mounted location, or a location apart from the default location in the agent.

Type	Name	Description
AGENT_RUNTIME_SETTINGS	mi-task-quarantine-dir	A directory where the file ingestion task stores the infected files detected when you run a virus scan. The directory is a custom location in the agent. The path can be a shared location, mounted location, or a location apart from the default location in the agent. For example, <code>userdata\quarantine</code> <b>Note:</b> To automatically clean up the quarantine directory, set the agent property for the quarantine location to a system temporary files location such as <code>/tmp/informatica/fmi/quarantine</code> .
AGENT_RUNTIME_SETTINGS	agent-dedup-repository	The information about skipped duplicate files is saved in Informatica Intelligent Cloud Services (IICS). To save the skipped duplicate files information in the Secure Agent, set the property to <code>true</code> . Default is <code>false</code> . For more information about saving the skipped duplicate information, see the <i>Mass Ingestion Files</i> guide.
AGENT_RUNTIME_SETTINGS	mi-dedup-snapshot-dir	Enter the path to store the information about skipped duplicate files in the Secure Agent. Applies only when the <b>agent-dedup-repository</b> property is set to <code>true</code> .
AGENT_RUNTIME_SETTINGS	file-listener-max-pool-size	The maximum number of threads to execute the file listener. Default is 20.
AGENT_RUNTIME_SETTINGS	file-listener-core-pool-size	The total number of threads. Default is 20.
AGENT_RUNTIME_SETTINGS	fmi-task-max-pool-size	The maximum number of threads to execute the file ingestion task. Default is 50.
AGENT_RUNTIME_SETTINGS	fmi-task-core-pool-size	The initial or minimum number of threads. Default is 20.
AGENT_RUNTIME_SETTINGS	ftp-receive-socket-buffer-size	The buffer size for FTP inbound packets. Default is 16 bytes.
AGENT_RUNTIME_SETTINGS	ftp-send-socket-buffer-size	The buffer size for FTP outbound packets. Default is 16 bytes.
AGENT_RUNTIME_SETTINGS	http-client-timeout	The timeout duration in seconds for Agent requests to Informatica Intelligent Cloud Services. Default is 30 seconds.

Type	Name	Description
PGP_SETTINGS	public-keyring-path	The directory to store the public key ring. You can add the following directory paths: <ul style="list-style-type: none"> <li>- A path relative to the directory where mass ingestion is installed. For example, <code>../data/pubring.pkr</code> where <i>pubring.pkr</i> is the name of the file where you store the public key ring.</li> <li>- The absolute path. For example, <code>&lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/pubring.pkr</code> where <i>pubring.pkr</i> is the name of the file where you store the public key ring and <i>Secure agent installation directory</i> is the name of the directory where the agent is installed.</li> </ul>
PGP_SETTINGS	secret-keyring-path	The directory to store the secret key ring. You can add the following directory paths: <ul style="list-style-type: none"> <li>- A path relative to the directory where mass ingestion is installed. For example, <code>../data/secring.pkr</code> where <i>secring.pkr</i> is the name of the file where you store the secret key ring.</li> <li>- The absolute path. For example, <code>&lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/secring.pkr</code> where <i>secring.pkr</i> is the name of the file where you store the secret key ring and <i>Secure Agent installation directory</i> is the name of the directory where the agent is installed.</li> </ul>
JVM_SETTINGS	app-heap-size	The minimum and maximum heap sizes of the Mass Ingestion Files application. Default is <code>-Xms256m -Xmx2048m</code> .
JVM_SETTINGS	lcm-heap-size	The minimum and maximum heap sizes of life-cycle management scripts. Default is <code>-Xms32m -Xmx128m</code> .

You can configure the following properties in the **Custom Configuration Details** area when you edit a Secure Agent:

Type	Name	Description
AGENT_RUNTIME_SETTINGS	ComplexFileDisableWriteChecksum	Set the value to <b>True</b> to ignore the <code>crc</code> file. The job runs successfully with Hadoop Files V2 as source and Snowflake Cloud Data Warehouse V2 as the target.

#### Guidelines to specify the folder path

A folder path can be a shared location, mounted location, or a location apart from the default location in the Secure Agent.

The following table lists the use of slashes around the source folder path:

Source	Folder Path
Windows	<folder path> For example, C:\temp
Linux	/<folder path>/ For example, /root/path
Windows shared location	<folder path> with additional slashes (\) For example, the path \\INV12B2B01\Shared\path, is specified as \\.\.\INV12B2B01\Shared\path

# CHAPTER 11

## Metadata Foundation Application

The Metadata Foundation Application service enables you to extract metadata from the configured source systems in your organization, and uploads the extracted metadata to Metadata Command Center through the Secure Agent

You can optimize the performance of the Metadata Foundation Application service by configuring some of its service properties.

### Metadata Foundation Application properties

To change or optimize the behavior of the Metadata Foundation Application service, configure its properties in the **System Configuration Details** section when you edit a Secure Agent.

The following image shows some of the Metadata Foundation Application service properties:

**System Configuration Details**

Service:

Type:

Type	Name
APP_CFG	mfa_maxParallelTasks
APP_CFG	mfa_agentMaxRetryAttempts
APP_CFG	mfa_agentInitialBackoffInterval
APP_CFG	mfa_agentMaxBackoffInterval
APP_CFG	mfa_agentShutdownWaitTimeMillis
APP_CFG	mfa_JVM_ARGS
PLUGIN_CFG	plugin_JVM_ARGS

You can configure the following Metadata Foundation Application service properties:

Type	Name	Description	Sample Value	Default Value
APP_CFG	mfa_maxParallelTasks	Number of concurrent running tasks in the Secure Agent.	5	4
APP_CFG	mfa_agentMaxRetryAttempts	-	3	5
APP_CFG	mfa_agentInitialBackoffInterval	-	500	100
APP_CFG	mfa_agentMaxBackoffInterval	-	20000	35000
APP_CFG	mfa_agentShutdownWaitTimeMillis	-	30000	60000
APP_CFG	mfa_JVM_ARGS	Option to add debug parameters or modify the JVM memory configuration parameters.	agentlib:jdwp=transport=dt_socket,address=8084,server=y,suspend=y	-
PLUGIN_CFG	plugin_JVM_ARGS	Option to add debug parameters or modify the JVM memory configuration parameters.	agentlib:jdwp=transport=dt_socket,address=8083,server=y,suspend=y	-
TRANSFER_SVC_CFG	transfer_svc_JVM_ARGS	Option to add debug parameters or modify the JVM memory configuration parameters.	agentlib:jdwp=transport=dt_socket,address=8085,server=y,suspend=y	-
TRANSFER_SVC_CFG	transfer_svc_batchSize	Number of content files that can be processed in a batch.  Use this option to optimize the generation of CSV files that are uploaded using the upload service.	4	1

Type	Name	Description	Sample Value	Default Value
TRANSFER_SVC_CFG	transfer_svc_stagingMaxRetry	Number of retries in case of failure while staging the content.	5	3
TRANSFER_SVC_CFG	transfer_svc_parallelTaskExecutorsSize	Number of concurrent running tasks.	5	4
TRANSFER_SVC_CFG	transfer_svc_contentBatchExecutorsSize	Number of concurrent content uploads using the upload service.	5	4
TRANSFER_SVC_CFG	transfer_svc_stagingBatchExecutorsSize	Number of concurrent content staging tasks.	5	4
TRANSFER_SVC_CFG	transfer_svc_contentWorkersBean	Transfer service beans that do the staging, ingestion and log transfer. To disable staging, specify only ingest and log transfer.	ingestion,log	ingestion,staging,log
TRANSFER_SVC_CFG	transfer_svc_ingestionMaxRetry	Number of retries for upload and bulk ingestion in case of failure.	5	3
TRANSFER_SVC_CFG	transfer_svc_contentMaxRetentionTimeInMin	Option to retain or delete the metadata extraction results after upload. The default behavior is to delete the results.	600	0

Type	Name	Description	Sample Value	Default Value
TRANSFER_SVC_CFG	transfer_svc_postDriverCompletionMaxWaitTimeInSec	Number of seconds after which long running or unresponsive ingestion tasks will be terminated. The default behavior is to not terminate any long running or unresponsive ingestion task.	10	-1
APP_LOG4J	name	Common property for all Secure Agent applications.	AppLogPropertiesConfig	AppLogPropertiesConfigXmx2048m
APP_LOG4J	rootLogger_level	Common property for all Secure Agent applications.	warn	info
APP_LOG4J	rootLogger_appenderRefs	Common property for all Secure Agent applications.	applog	applog
APP_LOG4J	rootLogger_appenderRefs_applog_ref	Common property for all Secure Agent applications.	LOGFILE	LOGFILE
APP_LOG4J	appenders	Common property for all Secure Agent applications.	applog	applog
APP_LOG4J	appender_applog_type	Common property for all Secure Agent applications.	RollingFile	RollingFile
APP_LOG4J	appender_applog_name	Common property for all Secure Agent applications.	LOGFILE	LOGFILE
APP_LOG4J	appender_applog_filePattern	Common property for all Secure Agent applications.	%d{MM-dd-yy-HH-mm-ss}-%i	%d{MM-dd-yy-HH-mm-ss}-%i



Type	Name	Description	Sample Value	Default Value
APP_LOG4J	appender_applog_layout_type	Common property for all Secure Agent applications.	PatternLayout	PatternLayout
APP_LOG4J	appender_applog_layout_pattern	Common property for all Secure Agent applications.	%d %d{z} %p [%c] - %m%n	%d %d{z} %p [%c] - %m%n
APP_LOG4J	appender_applog_policies_type	Common property for all Secure Agent applications.	Policies	Policies
APP_LOG4J	appender_applog_policies_size_type	Common property for all Secure Agent applications.	SizeBasedTriggeringPolicy	SizeBasedTriggeringPolicy
APP_LOG4J	appender_applog_policies_size_size	Common property for all Secure Agent applications.	5MB	10MB
APP_LOG4J	appender_applog_strategy_type	Common property for all Secure Agent applications.	DefaultRolloverStrategy	DefaultRolloverStrategy
APP_LOG4J	appender_applog_strategy_max	Common property for all Secure Agent applications.	5	5
APP_LOGBACK	logback_log_file_pattern	Common property for all Secure Agent applications.	{yyyy-ww}	{yyyy-ww}
APP_LOGBACK	logback_log_max_file_size	Common property for all Secure Agent applications.	5MB	10MB
APP_LOGBACK	logback_log_max_history	Common property for all Secure Agent applications.	20	10
APP_LOGBACK	logback_root_level	Common property for all Secure Agent applications.	DEBUG	INFO

## CHAPTER 12

# Metadata Platform Service

The Metadata Platform Service enables you to perform profiling activities for the jobs that you run in Metadata Command Center. Profiling fails if there is no active Metadata Platform Service present in the runtime environment of Metadata Command Center.

You can optimize the performance of the Metadata Platform Service by configuring some of its service properties.

## Metadata Platform Service properties

To change or optimize the behavior of the Metadata Platform Service, configure its properties in the **System Configuration Details** section when you edit a Secure Agent.

The following image shows some of the Metadata Platform Service properties:

### ▼ System Configuration Details

Service:	Metadata Platform Service	▼
Type:	All Types	▼
Type	Name	Value
APP_CFG	mps_maxParallelTasks	4
APP_CFG	mps_agentMaxRetryAttempts	5
APP_CFG	mps_agentInitialBackoffInterval	100
APP_CFG	mps_agentMaxBackoffInterval	35000
APP_CFG	mps_agentShutdownWaitTimeMillis	60000
APP_CFG	mps_profileResultRetention	false
APP_CFG	mps_maxDeploymentBatchSize	100

You can configure the following Metadata Platform Service properties:

Type	Name	Description	Sample Value	Default Value
APP_CFG	mps_maxParallelTasks	The maximum number of batch profiling sub tasks that can run at the same time.	3	4
APP_CFG	mps_agentMaxRetryAttempts	-	3	5
APP_CFG	mps_agentInitialBackoffInterval	-	500	100
APP_CFG	mps_agentMaxBackoffInterval	-	20000	35000
APP_CFG	mps_agentShutdownWaitTimeMillis	-	30000	60000
APP_CFG	mps_profileResultRetention	-	false	false
APP_CFG	mps_maxDeploymentBatchSize	The maximum number of objects that a batch profiling sub-task can contain.	50	100 <b>Note:</b> The value of the deployment batch size parameter should be 1 or greater than 1.
APP_CFG	mps_metadataComputeProfile	Defines the load type.	-	'Small:core.DataElement=1000;Medium:core.DataElement-10000;'
APP_CFG	mps_previewFileRetentionInDays	The maximum number of days when files associated with a catalog source job for the profiling capability are stored. For example, Data Preview results.	5	7
APP_CFG	mps_JVM_ARGS	Option to add debug parameters or modify the JVM memory configuration parameters.	-Xms32m -Xmx512m	-

Type	Name	Description	Sample Value	Default Value
TRANSFER_SVC_CFG	transfer_svc_batchSize	Number of content files that can be processed in a batch.  Use this option to optimize the generation of CSV files that are uploaded using the upload service.	4	1
TRANSFER_SVC_CFG	transfer_svc_stagingMaxRetry	Number of retries in case of failure while staging the content.	5	3
TRANSFER_SVC_CFG	transfer_svc_parallelTaskExecutorsSize	Number of concurrent running tasks.	5	4
TRANSFER_SVC_CFG	transfer_svc_contentBatchExecutorsSize	Number of concurrent content uploads using the upload service.	5	4
TRANSFER_SVC_CFG	transfer_svc_stagingBatchExecutorsSize	Number of concurrent content staging tasks.	5	4
TRANSFER_SVC_CFG	transfer_svc_contentWorkersBean	Transfer service beans that do the staging, ingestion and log transfer.  To disable staging, specify only ingest and log transfer.	ingestion,log	ingestion,staging,log
TRANSFER_SVC_CFG	transfer_svc_ingestionMaxRetry	Number of retries for upload and bulk ingestion in case of failure.	5	3

Type	Name	Description	Sample Value	Default Value
TRANSFER_SVC_CFG	transfer_svc_contentMaxRetentionMin	Option to retain or delete the metadata extraction results after upload. The default behavior is to delete the results.	600	0
TRANSFER_SVC_CFG	transfer_svc_postDriverCompletionMaxWaitTimeInSec	Number of seconds after which long running or unresponsive ingestion tasks will be terminated. The default behavior is to not terminate any long running or unresponsive ingestion task.	10	-1
APP_LOG4J	name	Common property for all Secure Agent applications.	AppLogPropertiesConfig	AppLogPropertiesConfig
APP_LOG4J	rootLogger_level	Common property for all Secure Agent applications.	warn	info
APP_LOG4J	rootLogger_appenderRefs	Common property for all Secure Agent applications.	applog	applog
APP_LOG4J	rootLogger_appenderRefs_applog_ref	Common property for all Secure Agent applications.	LOGFILE	LOGFILE
APP_LOG4J	appenders	Common property for all Secure Agent applications.	applog	applog
APP_LOG4J	appender_applog_type	Common property for all Secure Agent applications.	RollingFile	RollingFile

Type	Name	Description	Sample Value	Default Value
APP_LOG4J	appender_applog_name	Common property for all Secure Agent applications.	LOGFILE	LOGFILE
APP_LOG4J	appender_applog_filePattern	Common property for all Secure Agent applications.	%d{MM-dd-yy-HH-mm-ss}-%i	%d{MM-dd-yy-HH-mm-ss}-%i
APP_LOG4J	appender_applog_layout_type	Common property for all Secure Agent applications.	PatternLayout	PatternLayout
APP_LOG4J	appender_applog_layout_pattern	Common property for all Secure Agent applications.	%d %d{z} %p [%c] - %m%n	%d %d{z} %p [%c] - %m%n
APP_LOG4J	appender_applog_policies_type	Common property for all Secure Agent applications.	Policies	Policies
APP_LOG4J	appender_applog_policies_size_type	Common property for all Secure Agent applications.	SizeBasedTriggeringPolicy	SizeBasedTriggeringPolicy
APP_LOG4J	appender_applog_policies_size_size	Common property for all Secure Agent applications.	5MB	10MB
APP_LOG4J	appender_applog_strategy_type	Common property for all Secure Agent applications.	DefaultRolloverStrategy	DefaultRolloverStrategy
APP_LOG4J	appender_applog_strategy_max	Common property for all Secure Agent applications.	5	5
APP_LOGBACK	logback_log_file_pattern	Common property for all Secure Agent applications.	{yyyy-ww}	{yyyy-ww}
APP_LOGBACK	logback_log_max_file_size	Common property for all Secure Agent applications.	5MB	10MB

Type	Name	Description	Sample Value	Default Value
APP_LOGBACK	logback_log_max_history	Common property for all Secure Agent applications.	20	10
APP_LOGBACK	logback_root_level	Common property for all Secure Agent applications.	DEBUG	INFO

## CHAPTER 13

# Process Server

Process Server is the Secure Agent service that executes Application Integration processes, connectors, and connections.

When you deploy Application Integration assets to the Secure Agent, you deploy them to Process Server. When you run an asset, Process Server executes it.

The PostgreSQL database comes with the Process Server service of the Secure Agent and stores the metadata that Process Server collects and generates.

Find the PostgreSQL directory in the following location on your system:

```
<Secure Agent installation directory>\apps\process-engine\data\PostGreSql
```

Informatica includes a PostgreSQL database with the Process Server package. However, you can also connect a different PostgreSQL database version to the Process Server. You can also migrate the existing cluster database dump to the PostgreSQL database. For more information, see *Configure* in the [How-To library](#) section on the documentation portal.

## Process Server properties

To change or optimize the behavior of Process Server, configure Process Server properties. You can configure the server, Secure Agent group, Java Virtual Machine, connector, database, and logging properties.

The following image shows some Process Server properties:



server	host-name	'localhost'
server	shutdown-port	7005
server	key-alias	'localhost'
server	key-store	'../conf/ae.keystore'
server	key-store-password	'password'
server	trust-store	'../conf/ae.cacerts'
server	trust-store-password	'changeit'
server	ldap-enabled-realm	false
server	ldap-properties	<ul style="list-style-type: none"> <li>- key: connectionURL</li> <li>  value: ldap://\$ {host_name}:10389</li> <li>- key: connectionName</li> <li>  value: uid=admin,ou=system</li> <li>- key: connectionPassword</li> <li>  value: \$ {pe_ldap_password}</li> <li>- key: authentication</li> <li>  value: simple</li> <li>- key: userBase</li> <li>  value: ou=people,DC-\$ {host_name},DC=informatica,DC=com</li> <li>- key: userSearch</li> <li>  value: (uid={01})</li> <li>- key: roleBase</li> <li>  value: ou=groups,DC-\$ {host_name},DC=informatica,DC=com</li> <li>- key: roleName</li> <li>  value: cn</li> <li>- key: roleSearch</li> <li>  value: (uniqueMember={01})</li> </ul>
server	ssl-enabled-protocols	'TLSv1.2'
server	ephemeral-DH-key-size	2048
server	use-secure-ciphers-only	true

You can configure the following server properties:

Name	Communication Method	Description
host-name	Secure Agent Channel	The host name of the Process Engine server.
shutdown-port	Secure Agent Channel	Process Server Tomcat shutdown port.
key-alias	HTTPS	The identifier of the keystore record that contains security keys for HTTPS communication.
key-store	HTTPS	<p>The path and file name of the key store file that Application Integration uses for HTTPS communication.</p> <p>When you install the Secure Agent, you can find the key store in the following default location:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/process-engine/conf/ae.keystore</pre> <p>You can also enter a relative path. For example, if the current working directory is the Secure Agent installation directory, enter the following value to point to the ae.keystore file:</p> <pre>../conf/ae.keystore</pre> <p><b>Note:</b> The file path can contain only forward slashes (/).</p>
key-store-password	HTTPS	The key store password. Default is <b>password</b> .

Name	Communication Method	Description
trust-store	HTTPS	<p>The path and file name of the trust store file that Application Integration uses for HTTPS communication.</p> <p>When you install the Secure Agent, you can find the trust store in the default location:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/process-engine/conf/ae.cacerts</pre> <p>You can also enter a relative path. For example, if the current working directory is the Secure Agent installation directory, enter the following value to point to the ae.cacerts file:</p> <pre>../conf/ae.cacerts</pre> <p><b>Note:</b> The file path can contain only forward slashes (/).</p> <p>If you want to import public certificates for service endpoint authentication, place them in the following location:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/process-engine/conf/certs</pre>
trust-store-password	HTTPS	The trust store password. Default is <b>changeit</b> . You can change the password.
ldap-enabled-realm	HTTP/HTTPS	Set this property to <code>true</code> if you want to use an LDAP provider for authentication. Use the LDAP provider as a centralized form of authentication when you have clustered Secure Agents.
ldap-properties	HTTP/HTTPS	<p>The LDAP properties that you need to configure. Edit the existing properties to suit your LDAP provider.</p> <p><b>Note:</b> Your LDAP password does not appear on screen. The value of <code>\$ (pe.ldap.password)</code> is taken from the <code>PE_LDAP_PASSWORD</code> environment variable.</p>
ssl-enabled-protocols	HTTPS	The TLS protocol to use. The default protocol, TLSv1.2, is the most secure protocol. Change this value to an older version like TLSv1.0 or TLSv1.1 only if you face compatibility issues.
ephemeral-DH-key-size	HTTPS	The key length of the secure algorithm. Default is <b>2048</b> . Change this value only if you face compatibility issues.
use-secure-ciphers-only	HTTPS	Limits the set of ciphers used during a call to the endpoint to secure ciphers only. Default is <b>true</b> . Change this value to <code>false</code> only if you face compatibility issues.
fips-enabled	HTTPS	<p>Set this property to <code>true</code> to enable the Federal Information Processing Standard (FIPS) mode on a Secure Agent. When you enable the FIPS mode, Windows uses the FIPS validated cryptographic algorithms.</p> <p>Default is <b>false</b>.</p>

You can configure the following Secure Agent group ('cluster' on the UI) properties:

Name	Communication Method	Description
name	HTTP/HTTPS	The name of the Secure Agent group.
primary-node	HTTP/HTTPS	Set this property to <code>true</code> if you want the Secure Agent to be the master agent. When you select a master agent, you create a Secure Agent cluster. In a cluster, all Secure Agents share the PostgreSQL database of the master Secure Agent.
load-balance-url	HTTP/HTTPS	The load balancer URL that you can use to invoke the process deployed to the Secure Agent. Applicable if you have a load balancer.

You can configure the following Java Virtual Machine properties:

Name	Communication Method	Description
min-heap	Secure Agent Channel	The minimum heap memory that Process Server allocates to the Tomcat JVM.
max-heap	Secure Agent Channel	The maximum heap memory that Process Server allocates to the Tomcat JVM.
additional-properties	Secure Agent Channel	A custom system property that you can add to the Tomcat JVM set. For example, you can set the custom property - <code>Dsun.net.inetaddr.ttl=60</code>

You can configure the following connector properties:

Name	Communication Method	Description
http-port	HTTP	The HTTP port to which the Secure Agent sends data. The default port is 7080. For more information about the construction of REST and SOAP endpoint URLs, see the Application Integration help.
http-maxThreads	HTTP	The maximum number of connections that Process Server creates with Application Integration over HTTP.
http-connectionTimeout	HTTP	The maximum time, in milliseconds, that Process Server waits for an HTTP connection to reply.
https-port	HTTPS	The HTTPS port to which the Secure Agent sends data. The default port is 7443. For more information about the construction of REST and SOAP endpoint URLs, see the Application Integration help.
https-maxThreads	HTTPS	The maximum number of connections that Process Server creates with Application Integration over HTTPS.

Name	Communication Method	Description
https-connectionTimeout	HTTPS	The maximum time, in milliseconds, that Process Server waits for an HTTPS connection to reply.
secure-channel-maxThreads	Secure Agent Channel	The maximum number of connections that Process Server creates with Application Integration.
secure-channel-connectionTimeout	Secure Agent Channel	The maximum time, in milliseconds, that Process Server waits for a connection to reply.

You can configure the following database properties:

Name	Communication Method	Description
type	Secure Agent Channel	The database type that Process Server runs on. <b>Important:</b> Do not change this setting. The Application Integration Secure Agent does not support other databases.
driver	Secure Agent Channel	The database driver that Process Server runs on. <b>Important:</b> Do not change this setting. The Informatica Cloud Secure Agent does not support other databases.
URL	Secure Agent Channel	URL at which Process Server accesses the database. <b>Important:</b> Do not change this setting. The Informatica Cloud Secure Agent does not support other databases.
maxActive	Secure Agent Channel	The maximum number of active connections allocated to the Process Server database at the same time.
maxIdle	Secure Agent Channel	The maximum number of connections that can remain idle at a time in the Process Server database. Process Server releases connections if the number of idle connections crosses this number.
maxWait	Secure Agent Channel	The maximum time that the Process Server database waits for a connection if none are available.
connection-properties	Secure Agent Channel	Key-value pairs of database connection properties. Some keys are available by default. Do not delete the default keys. However, you can change the values of these keys. You can add other key-value pairs. For example, you can add the following key-value pair: key: autoReconnect value: true

If you created a separate logging data source and want to redirect the process logging from the existing database to the data source, configure the following properties:

Name	Communication Method	Description
logUrl	Secure Agent Channel	The URL at which the Process Server accesses the logging data source to redirect the process logging data. Default is <code>jdbc:postgresql://localhost:5432/activevos</code> .
logMaxActive	Secure Agent Channel	The logs for the maximum number of active connections allocated to the Process Server database at the same time. Default is <b>50</b> .
logMaxIdle	Secure Agent Channel	The logs for the maximum number of connections that remained idle at a time in the Process Server database. Default is <b>5</b> .
logMaxWait	Secure Agent Channel	The logs for the maximum time that the Process Server database waited for a connection if none was available. Default is <b>30000</b> .
logConnection-properties	Secure Agent Channel	The key-value pairs of the logging database connection properties. The following keys are available by default: <ul style="list-style-type: none"> <li>- key: <code>timeBetweenEvictionRunsMillis</code> value: <code>300000</code></li> <li>- key: <code>testOnBorrow</code> value: <code>true</code></li> <li>- key: <code>testWhileIdle</code> value: <code>true</code></li> </ul> <p>Do not delete the default keys. However, you can change the values of these keys.</p> <p>You can add other key-value pairs. For example, you can add the following key-value pair:</p> <ul style="list-style-type: none"> <li>- key: <code>autoReconnect</code> value: <code>true</code></li> </ul>

For more information about configuring a separate logging data source on a Secure Agent, see [“Configuring a separate logging data source” on page 63](#).

You can configure the following logging properties:

Name	Communication Method	Description
<code>org.apache.catalina.core.ContainerBase.Catalina_localhost_level</code>	Secure Agent Channel	The level of logging in the <code>localhost.log</code> file when you host Tomcat on a virtual machine. Default is <b>INFO</b> .
<code>org.apache.catalina.core.ContainerBase.Catalina_localhost_manager_level</code>	Secure Agent Channel	The level of logging in the <code>manager.log</code> file when you host Tomcat on a virtual machine. Default is <b>INFO</b> .

Name	Communication Method	Description
org_apache_catalina_core_ContainerBase_Catalina_localhost_host-manager_level	Secure Agent Channel	The level of logging in the <code>host-manager.log</code> file when you host Tomcat on a virtual machine. Default is <b>INFO</b> .
log4j2_root_level	Secure Agent Channel	The logging level of the ROOT logger. Default is <b>INFO</b> .
additional-logging	Secure Agent Channel	The name-level of logging pair for a specific class. Default is: <pre>- name: org.apache.camel.component.file.remote.S ftpOperations level: ERROR</pre>

You can configure the following custom properties in the **Custom Configuration Details** section:

Name	Type	Description
https-clientAuth	connectors	Set this property to <code>true</code> to enable mutual authentication after upgrading the Process Server. For more information about configuring this property, see <a href="#">"Enable mutual authentication for Process Server" on page 81</a> .
replication_upgrade	db	Set this property to <code>true</code> to enable the replication upgrade of the PostgreSQL database for a Secure Agent. For more information about configuring this property, see <a href="#">"Upgrading the PostgreSQL database using the replication technique" on page 79</a> .
ssl-implementation	server	Set this property to override the class name of the ssl implementation to be used in Tomcat. Default is <code>org.apache.tomcat.util.net.jsse.JSSEImplementation</code> .

After adding or editing a custom property, you must restart the Process Server for the change to take effect.

For more information about adding a custom property, see [Chapter 15, "Configuring Secure Agent service properties" on page 87](#).

## Default connection database properties

The following table describes the default keys that are available for the `connection-properties` database property:

Key	Description
<code>timeBetweenEvictionRuns</code>	The number of milliseconds that Process Server waits in-between runs of the idle object evictor thread.
<code>testOnBorrow</code> value	Process Server validates objects before borrowing objects from the pool. If Process Server cannot validate the object, it drops the object from the pool. Then, Process Server tries to borrow another object.
<code>testWhileIdle</code>	Process Server validates objects by the idle object evictor (if one exists). If Process Server cannot validate the object, it drops the object from the pool.
<code>validationQuery</code> value	The SQL query that validates connections from this pool before returning them to the caller. If you specify this property, the query must be an SQL SELECT statement that returns at least one row.

## Logging levels

The following table describes the levels that you can configure for Process Server **logging** properties:

Level	Description
SEVERE	Logs errors.
WARNING	Logs potentially harmful situations.
INFO	Logs informational events that show the high-level progress of the application.
CONFIG	Logs informational events in more detail than at the <code>INFO</code> level.
FINE	Logs fine-grained informational events that you can use to debug an application.
FINER	Logs fine-grained informational events in more detail than at the <code>FINE</code> level.
FINEST	Logs all events.

## Configuring a separate logging data source

You can configure a separate logging data source to redirect process logging from the existing database to the data source, and thereby reduce the load on the existing database.

To create a separate logging data source on a Secure Agent, perform the following steps:

1. Create an environment variable with the user name and password for the log database environment as follows:

```
PE_DB_LOG_USERNAME
```

```
PE_DB_LOG_PASSWORD
```

This step is optional. If you do not specify a separate environment variable for the log database, the default database user name and password, that is, `PE_DB_USERNAME` and `PE_DB_PASSWORD` are used.

- If you use a separate database or schema, execute the following DDL to create a structure for the AeProcessLogData table within that schema:

```
CREATE TABLE AeProcessLogData
(
    ProcessId BIGINT NOT NULL,
    SequenceId BIGINT NOT NULL,
    PlanId BIGINT NOT NULL,
    TenantContextId VARCHAR(32),
    LocationPath TEXT NOT NULL,
    InstanceLocationId INT NOT NULL,
    DefLocationId INT NOT NULL,
    CorrelationId INT NOT NULL,
    EventId INT NOT NULL,
    SessionId INT NOT NULL,
    SourceId INT NOT NULL,
    FaultName VARCHAR(255),
    AncillaryStr TEXT,
    AncillaryInt INT,
    EventTime BIGINT NOT NULL,
    DataDocument TEXT,
    PRIMARY KEY (ProcessId, SequenceId)
);
CREATE INDEX AeLogDataPidInsId ON AeProcessLogData(PlanId, ProcessId, InstanceLocationId);
```

- Configure the following logging data source properties in the Process Server properties:

- logUrl
- logMaxActive
- logMaxIdle
- logMaxWait
- logConnection-properties

For more information about configuring the logging data source properties, see [“Process Server properties” on page 56](#).

- Restart the Secure Agent for the change to take effect.

## Process Server sizing recommendations

Configure the Process Server service of the Secure Agent according to your workload.

Use the following sizing recommendations to optimize resources:

Recommendation	Small	Medium	Large
Process Count	75	175	350
Resource Cache (MB)	75	175	350
Work Manager Thread Pool Min	50	100	150
Work Manager Thread Pool Max	250	500	750



Recommendation	Small	Medium	Large
JVM Min Heap (MB)	Default	768	1024
JVM Max Heap (MB)	Default	Default	4096

The default JVM Min Heap is 512 MB, and the default JVM Max Heap is 1536 MB.

For example, to configure the Process Count, Resources Cache, Work Manager Thread Pool Min, and Work Manager Thread Pool Max related properties, perform the following steps:

1. In Application Integration Console, click **Server Configuration**.
2. On the **Server Configuration** page, select a Secure Agent.
3. Click the **Server Settings** tab.
4. Update the Process Count, Resource Cache, Work Manager Thread Pool Min, and Work Manager Thread Pool Max related property values as shown in the following image:

The screenshot displays the 'Server Configuration' page in the Informatica Application Integration Console. The left sidebar contains navigation options: Processes, Guides, APIs, Connections, Process Schedules, Logs, Server Configuration (selected), Deployed Assets, Process Server Health, and Process Metrics. The main content area shows configuration settings for the Secure Agent 'asv23soas101'. The following properties are highlighted with red boxes:

- Process Count: 250
- Resource Cache (MB): 100
- Default Work Manager Thread Pool Min: 5
- Default Work Manager Thread Pool Max: 100
- System Work Manager Thread Pool Min: 1
- System Work Manager Thread Pool Max: 50
- Invoke Work Manager Thread Pool Min: 25
- Invoke Work Manager Thread Pool Max: 300

Other visible properties include Process Activity Execution Limit (10000), Process Idle Timeout (10), Terminate suspended processes after (0), Suspended processes termination timer interval (1440), Suspended processes termination limit per run (-1), Suspend long running processes after (0), Running processes suspension timer interval (1440), Running processes suspension limit per run (-1), Screen Cache Size (50), Unmatched Correlated Receive Timeout (30), Web Service Invoke Timeout (600), Web Service Reply Timeout (600), Maximum HTTP Connections (500), Maximum HTTP Connections Per Host (100), Max Connection Timeout (0), Message size limit (5242880), Message TTL (90), Message with attachments size limit (5242880), Work Manager Threads For Alarms Max (15), Work Manager Threads For Process Migration Max (50), and Work Manager Threads Per Process Max (10).

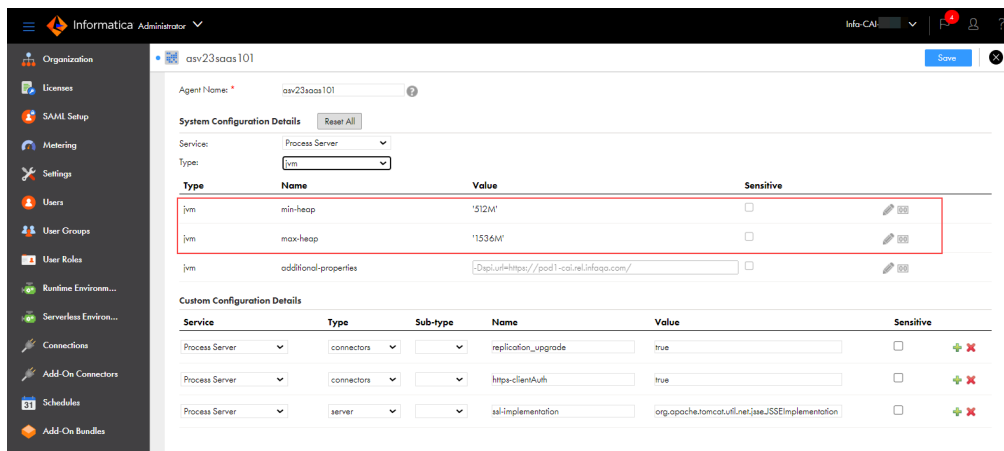
5. Click **Save**.
6. Restart the Process Server for the changes to take effect.

For more information about the Process Server configuration properties in Application Integration Console, see [Process Server properties](#).

To configure the JVM Min Heap and JVM Max Heap, perform the following steps:

1. In Administrator, click **Runtime Environments**.
2. On the **Runtime Environments** page, click the name of the Secure Agent. 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 upper right corner, click **Edit**.
5. Scroll down to the **System Configuration Details** section.
6. Select the service as **Process Server**.
7. Select the configuration property type as **jvm**.
8. In the row that contains the **jvm min-heap** and **jvm max-heap** properties, click the **Edit Agent Configuration** icon and update the property values.

The following image shows the **jvm min-heap** and **jvm max-heap** properties:



9. Click **Save**.
10. Restart the Process Server for the changes to take effect.

For more information about the Process Server properties in Administrator, see [“Process Server properties” on page 56](#).

When you start the Process Server on UNIX operating systems, you might see the following error:

```
Cannot write to temp location [/tmp]
```

This error occurs because UNIX limits the number of files that can be created by a single process. The maximum number of files that can be created by a single process is 1024.

To avoid this error, Informatica recommends that you increase the open files limit to at least 10 times the default value of 1024. Contact your system administrator to increase the value of any other relevant parameters such as max user processes.

For more information about Process Server sizing for a Secure Agent, see the following document:

<https://knowledge.informatica.com/s/article/DOC-17439>

# Communication with the Secure Agent

Informatica Intelligent Cloud Services sends data from the Secure Agent to the Process Server through the Secure Agent Channel or a through a direct HTTP or HTTPS link.

The Secure Agent communicates with Process Server in two ways:

## The Secure Agent Channel

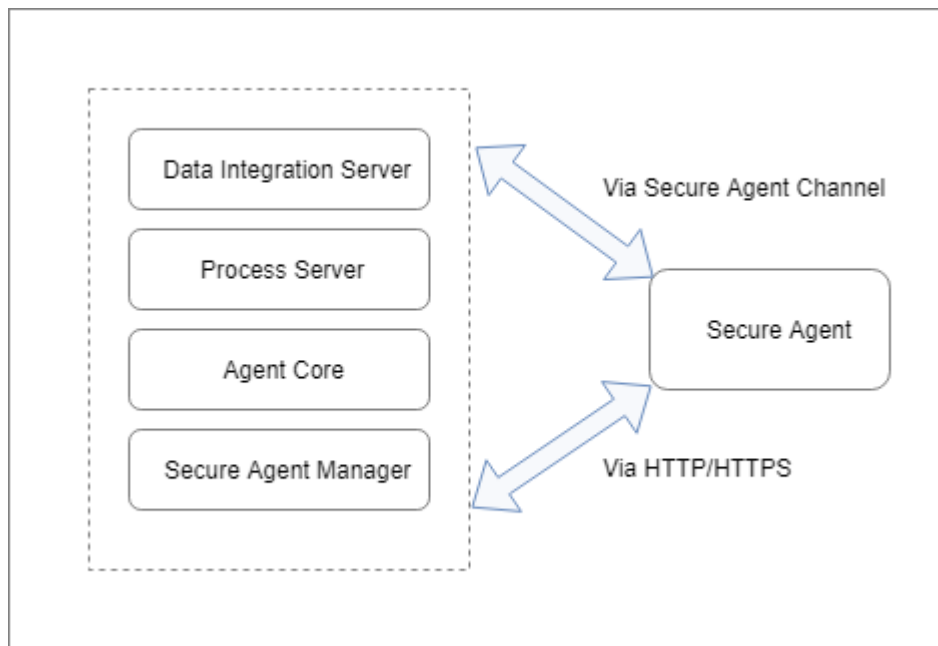
A secure channel that creates tunnels between each connected Secure Agent and Process Server.

## HTTP or HTTPS

A protocol over which the Secure Agent directly sends data to Process Server. If you use this communication method, Informatica Intelligent Cloud Services validates your credentials against the authentication provider.

For more information about the communication method that each Process Server property uses, see the [Process Server Properties on page 56](#).

The following image shows the two methods of communication between the Secure Agent and Process Server:



# Secure Agent configurations for Process Server

Deploy an asset to a single Secure Agent or a Secure Agent group based on your business needs. If the Process Server uses the Secure Agent group, you can use the Secure Agent load balanced configuration or a Secure Agent Cluster configuration based on your requirements.

When you deploy Application Integration processes, connections, or service connectors to a Secure Agent, you deploy the assets to the Process Server service of the Secure Agent. All Secure Agents with the Process Server service use a PostgreSQL database.

You can deploy an asset to the following Secure Agent configurations:

#### Single Secure Agent

A single Secure Agent might be the only agent in a group, or one of many agents on a group.

For more information, see [“Deploy to a single Secure Agent” on page 68](#).

#### Secure Agent group

A Secure Agent group can contain multiple agents.

You can use Secure Agent groups to deploy Process Server services using the following Secure Agent configurations:

#### Secure Agent load balancing

When you deploy an asset to a Secure Agent group, Informatica Intelligent Cloud Services performs load balancing. Use the Secure Agent load balanced configuration to distribute requests if you process stateless requests or use the Secure Agent only to serve OData requests.

#### Secure Agent Cluster

A Secure Agent Cluster is an agent group that has a master Secure Agent. Use the Secure Agent Cluster configuration when you want all Process Servers to receive information about process execution activity.

For more information, see [Deploy to a Secure Agent group on page 69](#).

The following table summarizes the process execution of the Secure Agent in different scenarios:

	Single Secure Agent	Secure Agent Group	
		Secure Agent Load Balancing	Secure Agent Cluster
<b>Agent Available</b>	Process executes.	Process executes.	Process executes.
<b>Agent Unavailable</b>	Process does not execute.	Process executes on any available Secure Agent.	Process executes on any available Secure Agent.
<b>Agent Stops Mid-Execution</b>	Process does not execute.	Process stops when the Secure Agent stops.	Process continues to execute on another Secure Agent.

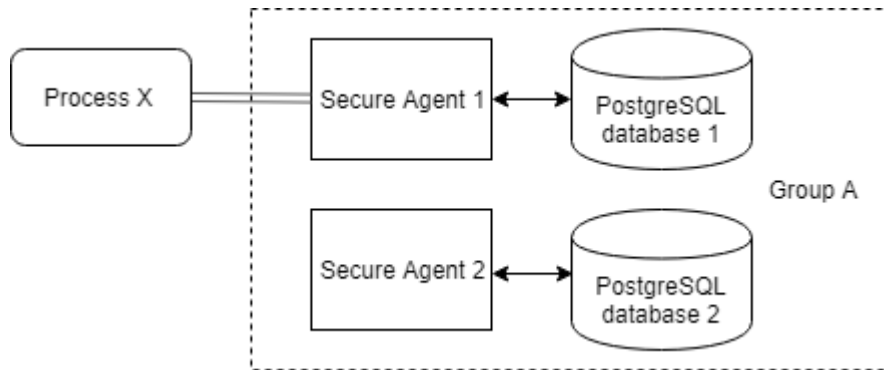
For more information about Process Server load balancing and clustering on a Secure Agent, see Knowledge Base article [DOC-17437](#).

## Deploy to a single Secure Agent

You can deploy an asset directly to one agent in a group.

When you deploy an asset to a single Secure Agent, no other Process Server in the Secure Agent group receives the asset definitions.

The following image shows a sample configuration where process X is deployed directly to Secure Agent 1:



Only Secure Agent 1 can execute Process X. If Secure Agent 1 is unavailable, the process does not execute.

## Deploy to a Secure Agent group

A Secure Agent group contains multiple agents. You can deploy an asset to a Secure Agent group.

Depending on the business requirements, you can use the Secure Agent groups to deploy Process Server services using the following Secure Agent configurations:

### Secure Agent load balanced configuration

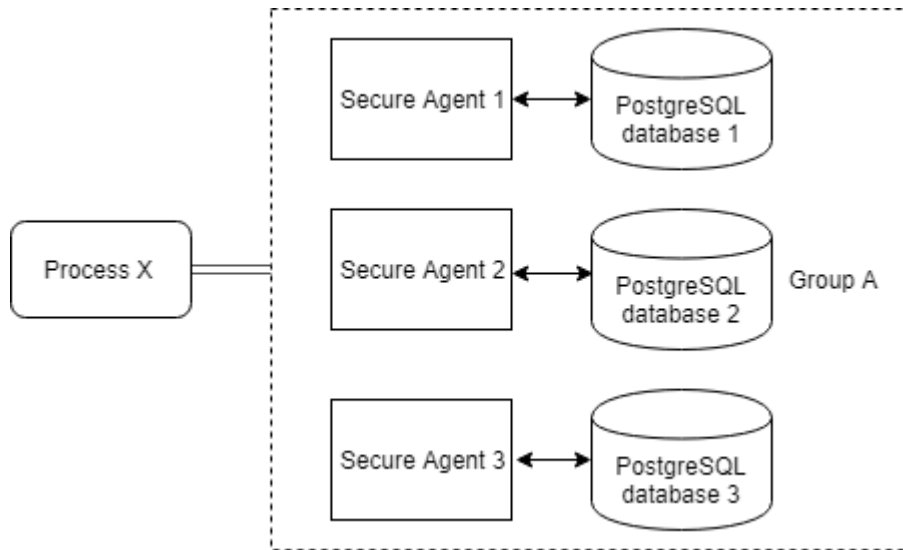
Use the Secure Agent load balanced configuration to distribute requests if you process stateless requests or use the Secure Agent only to serve OData requests.

When you deploy an asset to a Secure Agent group, you use a load balanced configuration. Informatica Intelligent Cloud Services performs the load balancing. You can add multiple Secure Agents to a group to balance the distribution of tasks across Process Servers. At run time, Informatica Intelligent Cloud Services dispatches incoming requests to available Secure Agents in a round-robin manner.

You can also use a custom load balancer by setting the `load-balance-url` Process Server property. For more information, see [Process Server Properties on page 56](#).

All Secure Agents in a group use individual PostgreSQL databases. When you deploy an asset to a Secure Agent group, all Process Servers within the group receive details about new or updated asset definitions. However, the other Process Servers in the group do not receive details about the execution activity of an asset. For example, if a Secure Agent within the group fails during process execution, the process does not continue to execute on another Secure Agent within the group.

The following image shows a sample configuration where process X is deployed to Secure Agent group A:



If you modify and re-publish process X, all three Secure Agents receive the updated definition. Any Secure Agent can execute the process.

For example, if the process is invoked and Secure Agent 1 and Secure Agent 2 are unavailable, the load balanced configuration ensures that Secure Agent 3 executes process X. However, Secure Agent 1 and Secure Agent 2 do not receive information about whether the process has faulted or completed successfully. If Secure Agent 3 stops while executing the process X, the process does not execute further.

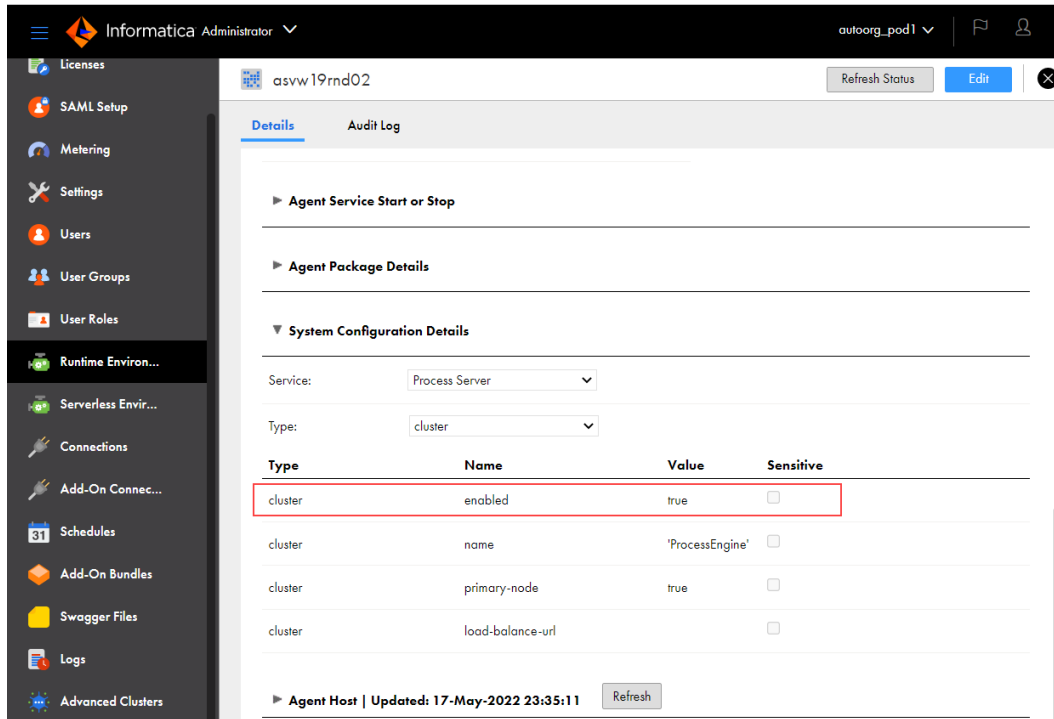
### Secure Agent Cluster configuration

Use the Secure Agent Cluster configuration if you are processing long-running processes and need to perform recovery of payload processing from one node to another. A clustered configuration shares a single database server with all the cluster nodes.

A Secure Agent Cluster is an agent group with a master Secure Agent. You can deploy an asset to a Secure Agent Cluster.

When you deploy an asset to a Secure Agent Cluster, all Process Servers receive information about process execution activity. The master Secure Agent receives information and informs the other Secure Agents. If a Secure Agent fails during process execution, the process continues to execute on another Secure Agent within the cluster.

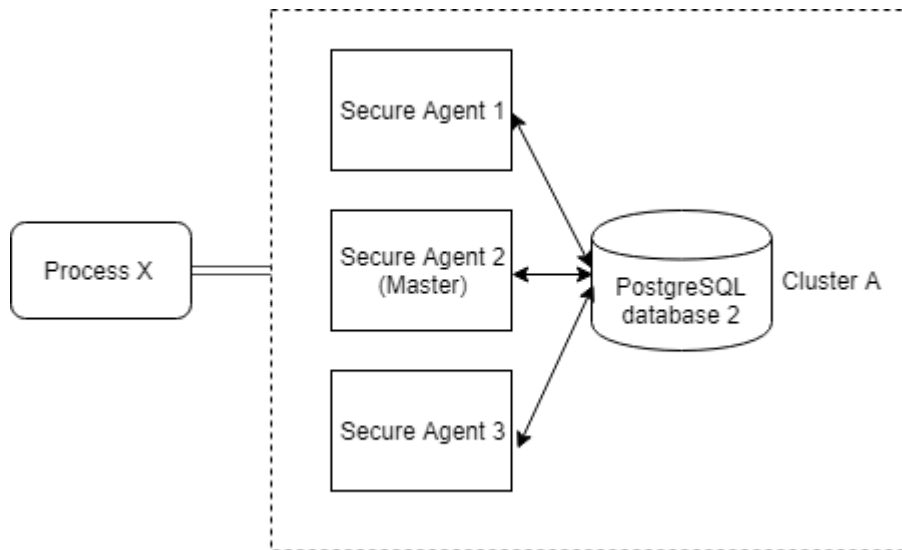
To enable the cluster configuration for a Process Server, click the **Runtime Environments** tab in Administrator. In the **System Configuration Details** section, set the `cluster-enabled` Process Server property value to `true` as shown in the following image:



All Process Servers in a cluster share the PostgreSQL database of the master agent.

To define the master Secure Agent, use the `primary-node` Process Server property. For more information, see [Process Server Properties on page 56](#).

The following image shows a sample configuration where process X is deployed to Secure Agent Cluster A:



If Secure Agent 3 starts executing process X but stops midway, either Secure Agent 1 or Secure Agent 2 continues to execute the process.

For more information about Secure Agent groups, see *Runtime Environments*.

# Prerequisites for PostgreSQL database installation and upgrade

Before you install or upgrade the PostgreSQL database, ensure that the following prerequisites are met:

- You have sufficient free disk space. Informatica recommends that you have a minimum free disk space that is twice the size of the Data folder in the following directory:

`<Secure Agent installation directory>\apps\process-engine\data\PostGreSql\Data`

- The user who runs scripts to install or upgrade the PostgreSQL database must have read, write, and modify permissions for the folders within the following directory:

`<Secure Agent installation directory>\apps\process-engine\data`

- Stop the PostgreSQL database and Process Server. If the Secure Agent is associated with an advanced cluster, you must stop Process Server on all nodes.

**Note:** This step is required when you run the `db_upgrade` script with the upgrade command line option. However, it is optional when you run the `db_upgrade` script with the check command line option. Therefore, you can run the `db_upgrade` script with the check command line option without any downtime.

- On Linux operating systems, the operating system user's locale must use the UTF-8 encoding to match the encoding of the PostgreSQL database. Otherwise, Process Server fails to start.
- On Linux operating systems, verify that the GNU C (GLIBC) library file is of version 2.14 or later. To find the version number, run the following command: `ldd --version`

## Managing the PostgreSQL database on Windows

Use binaries and utility scripts to manage the PostgreSQL database.

**Important:** To manage the PostgreSQL database, you must log in as a user who does not have system administrator rights. A system administrator will be unable to run PostgreSQL binaries and utility scripts.

Informatica has created some utility scripts based on PostgreSQL binaries. These utility scripts make it easier for you to manage the PostgreSQL database.

The following directories contain files for the PostgreSQL database:

- **PostgreSQL binaries:** `<Secure Agent installation directory>\apps\process-engine\data\db\postgresql-windows-x64-binaries\pgsql\bin`
- **PostgreSQL utility scripts:** `<Secure Agent installation directory>\apps\process-engine\data\db\util`
- **PostgreSQL logs:** `<Secure Agent installation directory>\apps\process engine\logs\PostGreSql\postgresql.log`
- **PostgreSQL data:** `<Secure Agent installation directory>\apps\process engine\data\PostGreSql\Data`

For more information about PostgreSQL scripts, see the PostgreSQL help at <https://www.postgresql.org/docs/current/static/index.html>.

Some of the following sections contain sample commands that use these default values:

- Default database name: `activevos`
- Default database user name: `bpeluser`



- Default database password: bpel

## Backing up the PostgreSQL database on Windows

Use the script `db_backup.bat` to back up the PostgreSQL database.

To back up the PostgreSQL database, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.
2. Run the following command:  
`db_backup.bat <dbusername> <dbpassword> <path to backup file along with name of backup file with a ".dump" extension> <dbport>`

For example, the Secure Agent creates the backup file 'BackupFile1.dump' in the location `C:\postgre\backup` if you run the following command:

```
db_backup.bat bpeluser bpel "C:\postgre\backup\BackupFile1.dump" 6432
```

**Note:** The `dbport` argument is optional. Specify the `dbport` argument if you use a port that is different from the default port, 5432.

## Restoring the PostgreSQL database on Windows

Use the command `db_restore.bat` to restore the PostgreSQL database from a backup file.

To restore the PostgreSQL database file from a backup file, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.
2. Run the following command:  
`db_restore.bat <dbusername> <dbpassword> <path to dump file> <dbport>`

For example, you use the file `BackupFile1.dump` to restore the PostgreSQL database if you run the following command:

```
db_restore.bat bpeluser bpel "C:\postgre\backup\BackupFile1.dump" 6432
```

**Note:** The `dbport` argument is optional. Specify the `dbport` argument if you use a port that is different from the default port, 5432.

## Resetting the PostgreSQL database on Windows

Shut down the PostgreSQL database and then use the command `db_reset.bat` to reset it.

To reset the PostgreSQL database to its original state, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`
2. To shut down the server, run the following command:  
`server_stop.bat`
3. To reset the PostgreSQL database, run the following command:  
`db_reset.bat`

## Starting the PostgreSQL server on Windows

To start the PostgreSQL server on Windows, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.

2. Run the following script:

```
server_start.bat
```

**Note:** If you do not use the default 5432 port, you must pass the port number as an argument as follows:

```
server_start.bat <port_number>
```

For example, `server_start.bat 6789`

## Stopping the PostgreSQL server on Windows

To stop the PostgreSQL server on Windows, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.
2. Run the following script:  

```
server_stop.bat.
```

## Getting the PostgreSQL server status on Windows

To get the status of the PostgreSQL server on Windows, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.
2. Run the following script:  

```
server_status.bat
```

**Note:** If you do not use the default 5432 port, you must pass the port number as an argument as follows:

```
server_status.bat <port_number>
```

For example, `server_status.bat 6789`

## Vacuuming the PostgreSQL database on Windows

Vacuum the PostgreSQL database to delete obsolete tuples and gain space. You use the script `db_maintenance.bat` to vacuum the PostgreSQL database.

By default, the PostgreSQL database autovacuum. If you want to manually vacuum the database, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\util`.
2. To vacuum the entire database, run the following command:  

```
db_maintenance.bat <dbusername> <dbpassword> <dbport> vacuum
```
3. To vacuum a single table, run the following command:  

```
db_maintenance.bat <dbusername> <dbpassword> <dbport> vacuum <tablename>
```

For example, you vacuum the 'aeoprocesslogdata' table if you run the following command:

```
db_maintenance.bat bpeluser bpel 5432 vacuum aeoprocesslogdata
```

**Note:** The `dbport` argument is required even if you use the default port, 5432.

## Reindexing the PostgreSQL database on Windows

Use the reindexing option to clean the index and free up space after you vacuum data on PostgreSQL. You use the script `db_maintenance.bat` to reindex the PostgreSQL database.

To reindex the PostgreSQL database, perform the following steps:

1. Go to `< Secure Agent installation directory>\apps\process-engine\data\db\util`.

2. To reindex the entire database, run the following command:  
`db_maintenance.bat <dbusername> <dbpassword> <dbport> reindex`
3. To reindex a single table, run the following command:  
`db_maintenance.bat <dbusername> <dbpassword> <dbport> reindex <tablename>`

For example, you reindex the 'aeprocesslogdata' table if you run the following command:

```
db_maintenance.bat bpeuser bpe1 5432 reindex aeprocesslogdata
```

**Note:** The dbport argument is required even if you use the default port, 5432.

## Resetting transaction logs on Windows

If the PostgreSQL server does not start because of corruption of the control information, use the command `pg_resetxlog.exe` to reset the control information.

To reset the PostgreSQL database control information, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\process-engine\data\db\postgresql-windows-x64-binaries\pgsql\bin`.
2. Run the following command:  
`pg_resetxlog.exe -D <path to postgresQL data directory>`

For example, you reset transactions logs in the 'Data' directory if you run the following command:

```
pg_resetxlog.exe -D "C:\postgre\apps\process-engine\data\PostGreSql\Data"
```

## Managing the PostgreSQL database on Linux

Use binaries utility scripts to manage the PostgreSQL database.

**Important:** To manage the PostgreSQL database, you must log in as a user who does not have root access. A root user will be unable to run PostgreSQL binaries and utility scripts.

Informatica has created some utility script based on PostgreSQL binaries. These utility scripts make it easier for you to manage the PostgreSQL database.

The following directories contain files for the PostgreSQL database:

- **PostgreSQL binaries:** `<Secure Agent installation directory>/apps/process-engine/data/db/postgresql-linux-x64-binaries/pgsql/bin`
- **PostgreSQL utility scripts:** `<Secure Agent installation directory>/apps/process-engine/data/db/util`
- **PostgreSQL logs:** `<Secure Agent installation directory>/apps/process-engine/logs/PostGreSql/postgresql.log`
- **PostgreSQL data:** `<Secure Agent installation directory>/apps/process-engine/data/PostGreSql/Data`

For more information about PostgreSQL scripts, see the PostgreSQL help at <https://www.postgresql.org/docs/current/static/index.html>.

Some sections contain sample commands that use the following default values:

- Default database name: activevos

- Default database user name: bpeluser
- Default database password: bpel

## Backing up the PostgreSQL database on Linux

Use the script `db_backup.sh` to back up the PostgreSQL database.

To back up the PostgreSQL database, perform the following steps:

1. Go to `<Secure Agent installation directory>/apps/process-engine/data/db/util`.
2. Run the following command:  

```
db_backup.sh <dbusername> <dbpassword> <path to backup file along with name of backup file>.dump <dbport>
```

For example, the Secure Agent creates the backup file `backupfile1.dump` in the location `/home/data/myfolder/` if you run the following command:

```
db_backup.sh bpeluser bpel "/home/data/myfolder/backupfile1.dump" 6432
```

**Note:** The `dbport` argument is optional. Specify the `dbport` argument if you use a port that is different from the default port, 5432.

## Restoring the PostgreSQL database on Linux

Use the script `db_restore.sh` to restore the PostgreSQL database from a backup file.

To restore the PostgreSQL database file from a backup file, perform the following steps:

1. Go to `<Secure Agent installation directory>/apps/process-engine/data/db/util`.
2. Run the following command:  

```
db_restore.sh <dbusername> <dbpassword> <path to dump file> <dbport>
```

For example, you use the file `backupfile1.dump` to restore the PostgreSQL database if you run the following command:

```
db_restore.sh bpeluser bpel "/home/data/myfolder/backupfile1.dump" 6432
```

**Note:** The `dbport` argument is optional. Specify the `dbport` argument if you use a port that is different from the default port, 5432.

## Resetting the PostgreSQL database on Linux

You first shut down the PostgreSQL database and then use the script `db_reset.sh` to reset it.

To reset the PostgreSQL database to its original state, perform the following steps:

1. Go to `<Secure Agent installation directory>/apps/process-engine/data/db/util`
2. To shut down the server, run the following script:  

```
server_stop.sh
```
3. To reset the PostgreSQL database, run the following script:  

```
db_reset.sh
```

## Starting the PostgreSQL server on Linux

To start the PostgreSQL server on Linux, perform the following steps:

1. Go to <Secure Agent installation directory>/apps/process-engine/data/db/util.

2. Run the following script:

```
server_start.sh
```

**Note:** If you do not use the default 5432 port, you must pass the port number as an argument as follows:

```
server_start.sh <port_number>
```

For example, `server_start.sh 6789`

## Stopping the PostgreSQL server on Linux

To stop the PostgreSQL server, perform the following steps:

1. Go to <Secure Agent installation directory>/apps/process-engine/data/db/util.

2. Run the following script:

```
server_stop.sh.
```

## Getting the PostgreSQL server status on Linux

To get the status of the PostgreSQL server on Linux, perform the following steps:

1. Go to <Secure Agent installation directory>/apps/process-engine/data/db/util.

2. Run the following script:

```
server_status.sh
```

**Note:** If you do not use the default 5432 port, you must pass the port number as an argument as follows:

```
server_status.sh <port_number>
```

For example, `server_status.sh 6789`

## Vacuuming the PostgreSQL database on Linux

Vacuum the PostgreSQL database to delete obsolete tuples and gain space. You use the script `db_maintenance.sh` to vacuum the PostgreSQL database.

By default, the PostgreSQL database auto vacuums. If you want to manually vacuum the database, perform the following steps:

1. Go to <Secure Agent installation directory>/apps/process-engine/data/db/util.

2. To vacuum the entire database, run the following command:

```
db_maintenance <dbusername> <dbpassword> <dbport> vacuum
```

3. To vacuum a single table, run the following command:

```
db_maintenance.sh <dbusername> <dbpassword> <dbport> vacuum <tablename>
```

For example, you vacuum the 'aeprocesslogdata' table if you run the following command:

```
db_maintenance.sh bpeluser bpel 5432 vacuum aeprocesslogdata
```

**Note:** The `dbport` argument is required even if you use the default port, 5432.

## Reindexing the PostgreSQL database on Linux

Use the reindexing option to clean the index and free up space after you vacuum data on PostgreSQL. You use the script `db_maintenance.sh` to reindex the PostgreSQL database.

To reindex the PostgreSQL database, perform the following steps:

1. Go to `<Secure Agent installation directory>/apps/process-engine/data/db/util`.
2. To reindex the entire database, run the following command:  
`db_maintenance <dbusername> <dbpassword> <dbport> reindex`
3. To reindex a single table, run the following command:  
`db_maintenance.sh <dbusername> <dbpassword> <dbport> reindex <tablename>`

For example, you reindex the 'aeprocesslogdata' table if you run the following command:

```
db_maintenance.sh bpeluser bpel 5432 reindex aeprocesslogdata
```

**Note:** The `dbport` argument is required even if you use the default port, 5432.

## Resetting transaction logs on Linux

If the PostgreSQL server does not start because of corruption to the control information, use the command `pg_resetxlog` to reset the control information.

To reset the control information of the PostgreSQL database, perform the following steps:

1. Go to `<Secure Agent installation directory>/apps/process-engine/data/db/postgresql-linux-x64-binaries/pgsql/bin`.
2. Run the following command:  
`pg_resetxlog -D <path to postgresQL data directory>`

For example, you reset the transactions logs in the `Data` directory, if you run the following command:

```
pg_resetxlog -D "home/apps/process engine/data/PostGreSql/Data"
```

## Upgrading the PostgreSQL database

You can upgrade the PostgreSQL database from version 9.5.2, 12.4, or 12.6 to version 13.5. Version 13.5 offers improved security, performance, and scalability.

You can choose to upgrade at your own convenience by manually running scripts provided by Informatica. The scripts take a backup of the existing database version so that you can restore to the old database version in case of any upgrade issue.

For more information about upgrading the PostgreSQL database, see the following community article:

<https://knowledge.informatica.com/s/article/DOC-18945>

# Upgrading the PostgreSQL database using the replication technique

If your Process Server PostgreSQL database version is earlier than version 13.5, you can upgrade the database when the Process Server restarts.

The Process Server PostgreSQL database upgrade is disabled by default. To enable replication upgrade of the PostgreSQL database for a Secure Agent, you must add a custom property for the Secure Agent.

To add a custom property for a Secure Agent, perform the following steps:

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click the name of the Secure Agent. 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 upper right corner, click **Edit**.
5. Scroll down to the **Custom Configuration Details** area.
6. The following image shows the **Custom Configuration Details** area:

Service	Type	Sub-type	Name	Value	Sensitive
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

7. If there are custom properties already configured, click the **Add** icon to add a new property row.
8. Select the service as **Process Server**.
9. Select a configuration property type as **db**.
10. Enter the property name as **replication\_upgrade** and value as **true**.
11. Click **Save**.  
The status of the Process Server service shows up as **Restart Required**.

When you restart the Process Server for the first time, the database starts replicating the data from your existing database version. Every time you restart the Process Server, the database verifies the replication status. After the replication is complete, the next time you restart the Process Server, the older version of the PostgreSQL database is shut down and the latest version of the database starts automatically.

This eliminates the effort of manually upgrading the Process Server PostgreSQL database to the latest version by running the scripts provided by Informatica.

## PostgreSQL configuration files

When you install the PostgreSQL database, the `postgresql.conf` file is automatically created in the following directory:

```
<Secure Agent installation directory>\apps\process-engine\data\PostGreSql\Data
```

The configuration parameters in the `postgresql.conf` file define the default values of the server properties related to auditing, authentication, encryption, and other behaviors.

The `postgresql.conf` file is overwritten every time you install or upgrade to a new version of the PostgreSQL database. Do not update the `postgresql.conf` file for any customized behavior, because the changes are lost when the file is overwritten.

Use the `user.conf` file to override the default values that are defined in the `postgresql.conf` file.

If the `user.conf` file does not already exist, create the file in the same directory as the `postgresql.conf` file, and override the values. Changes take effect after you restart the PostgreSQL database.

## Configuring PostgreSQL log rotation

The PostgreSQL log contains logging information for the PostgreSQL database that is packaged with the Secure Agent.

The PostgreSQL log is available in the following directory:

```
<Secure Agent installation directory>\apps\process-engine\logs\PostGreSql\postgresql.log
```

The PostgreSQL log can become very large and difficult to manage over time. You can configure log rotation to reduce the file size and manage the file easily. You can configure log rotation based on time or file size.

1. Create a file named `user.conf` in the following location if it does not already exist:

```
<Secure Agent installation directory>\apps\process-engine\data\PostGreSql\Data
```

The `user.conf` file overrides the values defined in the `postgresql.conf` file.

2. Perform one of the following steps:

- To rotate the logs based on time, add the following properties to the `user.conf` file:

```
log_filename = 'postgresql-%Y-%m-%d_%H%M%S.log'  
log_rotation_age=<value in minutes>
```

For example, if you set the value of the `log_rotation_age` property to 1440, the log file will be rotated every day.

- To rotate the logs based on file size, add the following properties to the `user.conf` file:

```
log_filename = 'postgresql-%Y-%m-%d_%H%M%S.log'  
log_rotation_size=<value in kilobytes>  
log_truncate_on_rotation=on
```

For example, if you set the value of the `log_rotation_size` property to 10240, the log file will be rotated when the file size exceeds 10 MB.

3. Save the `user.conf` file.
4. Restart the PostgreSQL database for the change to take effect.

## Configuring public certificates and private keys for Process Server

When you use Application Integration processes and connections to connect to an SSL-enabled endpoint, you must have public certificates and/or private keys. You must import the public certificates and private keys for the processes and connections to the Secure Agent.

After configuring public certificates and private keys for Process Server, enable mutual authentication for Process Server,



## Import public certificates and private keys for processes and connections

To connect to an SSL-enabled endpoint, such as a web service, queue, or a JDBC connection, you need a public certificate and/or a private key.

You must import the certificates to the Secure Agent machine where the process or connection is published in order for the process or connection to establish SSL-enabled connections to these endpoints.

To import the public certificates and/or private keys, perform the following steps:

- For public certificates, place the cert file in the following location and restart the Secure Agent:  
`<Secure Agent installation directory>/apps/process-engine/conf/certs`
- For private keys, import the keys to the `ae.keystore` file in the following location and restart the Secure Agent:

`<Secure Agent installation directory>/apps/process-engine/conf`

You must import and place the public cert file in `x509` format in the `certs` folder mentioned above. You must import the certificates and keys in the same locations to ensure ease of use and compatibility with upgrades.

Additionally, to import a secret private key within the Informatica Keystore, the secret key must have the same keystore format, that is, PKCS12 ".p12". For example, if the secret key is provided in the ".pfx" format, you must convert it to ".p12". You can verify this with the certificate provider.

To connect to the Secure Agent through the domain name and not the localhost, you can generate the certificate based on the domain name that you want to connect to and copy the certificate into the `certs` folder.

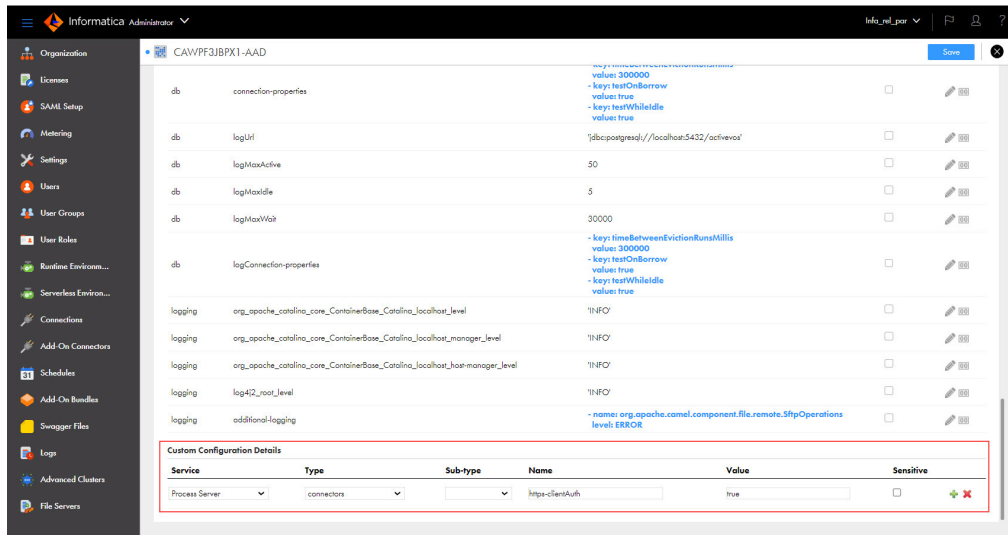
## Enable mutual authentication for Process Server

After upgrading the Process Server with the latest package, enable mutual authentication for Process Server using one of the following methods:

- Enable mutual authentication from Administrator.
- Manually update the `server.xml.mustache` file.

To enable mutual authentication from Administrator, perform the following steps:

1. In Administrator, select **Runtime Environments**.
2. On the **Runtime Environments** page, click the name of the Secure Agent.  
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 upper right corner, click **Edit**.
5. Scroll down to the **Custom Configuration Details** area.
6. If there are custom properties already configured, click the **Add** icon to add a new property row.
7. Select the service as **Process Server**.
8. Select the configuration property type as **connectors**.
9. Enter the property name as **https-clientAuth** and the value as **true** as shown in the following image:



10. Click **Save**.  
The status of the Process Server service shows up as **Restart Required**.
  11. Restart the Process Server for the change to take effect.
- To manually update the `server.xml.mustache` file, perform the following steps:

1. Log in to the Secure Agent machine.
2. Go to the following directory:
 

```
<Secure Agent installation directory>/downloads/package-process-engine.<latest_version>/package/app/conf/
```
3. Edit the `server.xml.mustache` file and change the value of the `clientAuth` property from `want` to `true`.
4. Save the `server.xml.mustache` file.
5. Restart the Secure Agent for the change to take effect.

**Note:** The default keystore is `ae.keystore` and it is installed with a localhost certificate.

For more information about the Process Server keystore and truststore configurations, see the attachment in Knowledge Base article [611562](#).

## Configuring thread pool profile to improve throughput

When you use event-based connectors such as AMQP and Kafka, you can increase the number of threads by increasing the thread pool size in the default thread pool profile. To increase the thread pool size, update the `aeEngineConfig.xml.mustache` file on the Secure Agent machine.

By default, the thread pool size is limited to 10 threads and a maximum of 10 messages can be processed concurrently by the connections. Informatica recommends that you increase the thread pool size only if you want to increase throughput, because additional threads occupy some resources, and too large pools are not recommended. The thread pool size applies to all event-based connections.

You can also configure the thread pool profile settings on the **Server Configuration** page in Application Integration Console. When you configure the thread pool profile settings on both the **Server Configuration** page and the `aeEngineConfig.xml.mustache` file on the Secure Agent machine, the properties configured on the **Server Configuration** page take precedence. For more information about the thread pool profile settings on the **Server Configuration** page, see [Server Properties](#).

To configure the thread pool profile, perform the following steps:

1. Log in to the Secure Agent machine.
2. Go to the following directory:

```
<Secure Agent installation directory>/downloads/package-process-engine.<latest_version>/
package/app/webapps/process-engine/WEB-INF/classes
```

3. Open the `aeEngineConfig.xml.mustache` file in a text editor and search for the following entry:

```
<entry name="IAeESBManager">...</entry>
```

4. Within the `IAeESBManager` entry, search for the subentry named `camelContext`.

Based on the status of the `cluster.enabled` option, you will find the following entries:

- If the `cluster.enabled` option is disabled, edit the following `camelContext` entry:

```
<entry name="Class" value="com.activee.rt.camel.AeCamelIntegrationManager"/>
<entry name="camelContext">
  <entry name="Class" value="com.activee.rt.camel.core.AeDefaultCamelContext"/>
</entry>
```

- If the `cluster.enabled` option is enabled, edit the following `camelContext` entry:

```
<entry name="Class"
value="com.activee.rt.cluster.AeClusterDistributedCamelManager"/>
<entry name="camelContext">
  <entry name="Class"
value="com.activevos.socrates.connectors.camel.AeSocratesCamelContext"/>
</entry>
```

5. Append a new `threadpoolProfile` subentry within the `camelContext` entry.

If the `cluster.enabled` option is disabled, add the following lines:

```
<entry name="camelContext">
<entry name="Class" value="com.activee.rt.camel.core.AeDefaultCamelContext"/>
<!-- New subentry -->
<entry name="threadpoolProfile">
  <entry name="PoolSize" value="<PoolSizeValue>"/>
  <entry name="MaxPoolSize" value="<MaxPoolSizeValue>"/>
  <entry name="MaxQueueSize" value="<MaxQueueSizeValue>"/>
  <entry name="KeepAliveTime" value="<KeepAliveTimeValue>"/>
  <entry name="TimeUnit" value="SECONDS"/>
  <entry name="AllowCoreThreadTimeout" value="true"/>
  <entry name="RejectedPolicy" value="CallerRuns"/>
</entry>
</entry>
```

If the `cluster.enabled` option is enabled, add the following lines:

```
<entry name="camelContext">
  <entry name="Class"
value="com.activevos.socrates.connectors.camel.AeSocratesCamelContext"/>
  <!-- New subentry -->
  <entry name="threadpoolProfile">
    <entry name="PoolSize" value="<PoolSizeValue>"/>
    <entry name="MaxPoolSize" value="<MaxPoolSizeValue>"/>
    <entry name="MaxQueueSize" value="<MaxQueueSizeValue>"/>
    <entry name="KeepAliveTime" value="<KeepAliveTimeValue>"/>
    <entry name="TimeUnit" value="SECONDS"/>
    <entry name="AllowCoreThreadTimeout" value="true"/>
    <entry name="RejectedPolicy" value="CallerRuns"/>
  </entry>
</entry>
```

6. Increase the thread pool size as required.  
**Note:** The pool is used by all the running event-based connections on the Secure Agent.
7. Save the `aeEngineConfig.xml.mustache` file.
8. Restart the Secure Agent for the change to take effect.

## Overriding properties in the `platform.yaml` file

You can override the default values for properties that the Process Server uses to get the configuration details related to Application Integration and communicate with the Secure Agent services.

To do this, you create a copy of the `platform.yaml` file and update the property values, name the file as `user-platform.yaml`, and save it in the following directory:

```
<Secure Agent installation directory>\apps\process-engine\conf
```

The `platform.yaml` file is available in the following directory:

```
<Secure Agent installation directory>\apps\process-engine\<latest_process_engine_version>\conf
```

When the Process Server is up and running, if a property is specified in the `user-platform.yaml` file, the Process Server uses that specific value. Otherwise, Process Server uses the values defined in the `platform.yaml` file.

When the Secure Agent is upgraded to a new version, the properties in the `user-platform.yaml` file are unchanged.

## Creating a custom `user-platform.yaml` file

You can create a custom `user-platform.yaml` file with the required properties and their custom values to override the properties in the `platform.yaml` file on the Secure Agent.

You must have the same level of access permissions as the `platform.yaml` file to create and edit the `user-platform.yaml` file.

To create a custom `user-platform.yaml` file, perform the following steps:

1. Log in to the Secure Agent machine.
2. Create a file named `user-platform.yaml` in the following directory:  

```
<Secure Agent installation directory>\apps\process-engine\conf
```
3. Copy the properties that you want to customize from the `platform.yaml` file that is available in the following directory to the `user-platform.yaml` file and override the values, as required:  

```
<Secure Agent installation directory>\apps\process-engine\<latest_process_engine_version>\conf
```

For example, consider that you need to override the values of the `cacheExpiryMillis` and `lockTimeoutMillis` properties.

These properties are available in the IDs section in the default `platform.yaml` file as shown in the following sample:

```
serviceHosts:
  ids:
    context: /identity-service/api/v1/
```

```

agentContext : /identity-service/agent/api/v1/
cache:
  enabled: true
  maxCacheItems: 2500
  cacheExpiryMillis: 60000
  lockTimeoutMillis: 30000
  refreshAheadEnabled: true
  queueCapacity: 500
  corePoolSize: 1
  maxPoolSize: 5
  keepAliveSec: 120
  timeToRefreshSec: 15
  evictOnLoadMiss: false
clientPool:
  socketTimeout : 60000
  connectionTimeout : 60000
  poolMaxTotal : 40
  poolMaxPerRoute : 30
hystrix:
  executionTimeoutInMilliseconds : 60000
  fallbackEnabled: false

```

Copy these properties from the `platform.yaml` file and update the values in the `user-platform.yaml` file as shown in the following sample:

```

serviceHosts:
  ids:
    context: /identity-service/api/v1/
    agentContext : /identity-service/agent/api/v1/
    cache:
      cacheExpiryMillis: 200000
      lockTimeoutMillis: 150000

```

**Note:** You must ensure that you follow the same hierarchy and syntax as the default `platform.yaml` file.

4. Save the `user-platform.yaml` file.
5. Restart the Process Server for the changes to take effect.

When the Process Server is up and running, the properties specified in the `user-platform.yaml` file override the properties in the `platform.yaml` file.

## Troubleshooting

When overriding the properties, if the `user-platform.yaml` file contains incorrect properties or values when compared to the `platform.yaml` file, you might encounter unexpected behavior.

For example, consider the following scenarios where you do not get the expected result because of manual intervention:

- The `agentContext` property is used to fetch the `IDS-SESSION-ID`. If the value for the `agentContext` property in the `platform.yaml` file is `/identity-service/agent/api/v1/` and you entered the value as `/identity-service/agent/api/v2/` in the `user-platform.yaml` file, Process Server fails to fetch the `IDS-SESSION-ID` because of the invalid endpoint. Therefore, the Secure Agent uses the basic authentication mechanism.
- The `cacheExpiryMillis` property value is expected to be numeric. However, if you enter an alphanumeric value, the value will be treated as a string without any error.

# CHAPTER 14

## SecretManagerApp

The SecretManagerApp service is the Secure Agent service that manages communication between Informatica Intelligent Cloud Services and your secrets manager when your organization uses an external secrets manager like AWS Secrets Manager or Azure Key Vault.

To change or optimize the behavior of the SecretManagerApp service, configure its properties in the System Configuration Details section when you edit a Secure Agent.

The following image shows some of the SecretManagerApp service properties:

Type	Name	Value	Sensitive
LOG4J	rootLogger	'INFO'	<input type="checkbox"/>
SECRET_MANAGER_APP_CONF	host	'localhost'	<input type="checkbox"/>
SECRET_MANAGER_APP_CONF	address	'127.0.0.1'	<input type="checkbox"/>
SECRET_MANAGER_APP_CONF	JVM_MIN_MEMORY	'32m'	<input type="checkbox"/>
SECRET_MANAGER_APP_CONF	JVM_MAX_MEMORY	'256m'	<input type="checkbox"/>

You can configure the following SecretManagerApp service properties:

Type	Name	Description
SECRET_MANAGER_APP_CONF	JVM_MIN_MEMORY	Amount of memory allocated for the SecretManagerApp service when the service starts. Default is 32 MB.
SECRET_MANAGER_APP_CONF	JVM_MAX_MEMORY	Maximum memory allocated for the SecretManagerApp service. Default is 256 MB.

**Note:** Do not change the values of other SecretManagerApp service properties unless Informatica Global Customer Support instructs you to do so.

## CHAPTER 15

# Configuring Secure Agent service properties

To configure Secure Agent service properties, open the **Runtime Environments** page and edit the Secure Agent. You can change, mask, and reset Secure Agent service property values. You can add and remove custom properties for a service. You can also change the Secure Agent name.

Custom properties are specific to connectors. For more details about custom properties, see the help for the appropriate connector.

**Warning:** Do not configure agent-level Secure Agent service property settings for an agent in a Secure Agent group that uses group-level property settings. If you want to configure agent-level property settings, delete the group-level property settings before you configure the agent properties. For more information about group-level property settings, see "Runtime Environments" in the *REST API Reference*.

1. On the **Runtime Environments** page, click the name of the Secure Agent.  
You might have to expand the Secure Agent group to see the list of Secure Agents within the group.
2. Click the **Details** tab.
3. In the upper right corner, click **Edit**.
4. To change the Secure Agent name, enter a new name in the **Agent Name** field.
5. To edit a service property, perform the following steps:
  - a. In the **System Configuration Details** area, select a service.
  - b. Select the configuration property type.
  - c. In the row that contains the property that you want to edit, click the **Edit Agent Configuration** icon.
  - d. To change the property value, enter the new property value.  
If the property is a sensitive property, the existing value will be cleared when you edit the property.
  - e. If the property contains sensitive data and you want to mask the value on the Secure Agent details page, enable the **Sensitive** option.  
When you enable the sensitive option, the value you enter is masked. If the field is a multi-line text field, the value is masked after you save the changes.
  - f. To reset the property to the system default value, click the **Reset Agent Configuration to system default** icon.

6. To add a custom property for a service, perform the following steps:

a. Scroll down to the **Custom Configuration Details** area.

The following image shows the **Custom Configuration Details** area:

Custom Configuration Details

Service	Type	Sub-type	Name	Value	Sensitive
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>  

b. If there are custom properties already configured, click the **Add** icon to add a new property row.

c. Select the service that you want to configure.

d. Select a configuration property type.

e. If the configuration property type has a sub-type, select the appropriate sub-type.

For example, to determine the logging level, choose INFO or DEBUG as the sub-type.

f. Enter the property name and value.

g. If the property contains sensitive data and you want to mask the value on the Secure Agent details page, enable the **Sensitive** option.

7. To remove a custom property, click the **Remove** icon next to the custom property.

8. To reset all configuration properties to the default settings, click **Reset All**.

9. Click **Save**.



# INDEX

## C

Cloud Application Integration community  
URL [6](#)  
Cloud Developer community  
URL [6](#)  
custom configuration properties  
Secure Agent [87](#)

## D

Data Integration community  
URL [6](#)  
Data Integration Server  
overview [25](#)

## E

Elastic Server  
overview [33](#)

## F

File Integration Service [37](#)

## G

GitRepoConnectApp  
local repository directory [38](#)  
overview [38](#)

## I

Informatica Global Customer Support  
contact information [7](#)  
Informatica Intelligent Cloud Services  
web site [6](#)

## M

maintenance outages [7](#)

## N

NetworkRetryInterval  
Data Integration Server property [25](#)  
NetworkTimeoutPeriod  
Data Integration Server property [25](#)

## S

SecretManagerApp  
overview [86](#)  
Secure Agent services  
CMI Streaming Agent [14](#)  
Database Ingestion agent environment variable [24](#)  
Database Ingestion service properties [20](#)  
Secure Agents  
changing the agent name [87](#)  
Common Integration Components properties [17](#)  
configuring service properties [87](#)  
custom configuration properties [87](#)  
Data Integration Server configuration properties [26](#)  
Data Integration Server service overview [25](#)  
Elastic Server configuration properties [33](#)  
Elastic Server service overview [33](#)  
File Ingestion configuration properties [41](#)  
GitRepoConnectApp configuration properties [39](#)  
GitRepoConnectApp service overview [38](#)  
masking configuration properties [87](#)  
Metadata Foundation Application [45](#)  
Metadata Foundation Application properties [45](#)  
Metadata Platform Service [50](#)  
Metadata Platform Service properties [50](#)  
network interruption settings [25](#)  
SecretManagerApp service overview [86](#)  
services overview [8](#)  
source control  
configuring the local repository directory [38](#)  
status  
Informatica Intelligent Cloud Services [7](#)  
Streaming ingestion  
secure agent [14](#)  
system status [7](#)

## T

trust site  
description [7](#)

## U

upgrade notifications [7](#)

## W

web site [6](#)