Informatica® Intelligent Cloud Services
April 2024

Data Integration Connections

Informatica Intelligent Cloud Services Data Integration Connections
April 2024

Publication Date: 2024-04-08

Table of Contents

Preface

Use *Data Integration Connections* to learn how to configure connections between Data Integration and cloud and on-premises applications, platforms, databases, and flat files. Refer to *Data Integration Connections* for information about the connection properties for all connectors that can be used with Data Integration.

Informatica Resources

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

Informatica Documentation

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

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

Informatica Intelligent Cloud Services web site

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

Informatica Intelligent Cloud Services Communities

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

Access the Informatica Intelligent Cloud Services Community at:

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

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

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

Informatica Intelligent Cloud Services Marketplace

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

https://marketplace.informatica.com/

Data Integration connector documentation

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

Informatica Knowledge Base

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

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

Informatica Intelligent Cloud Services Trust Center

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

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

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

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

Informatica Global Customer Support

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

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

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

CHAPTER 1

Connectors and connections

Connections provide access to data in cloud and on-premise applications, platforms, databases, and flat files. They specify the location of sources, lookup objects, and targets that are included in a task.

You use connectors to create connections. You can create a connection for any connector that is installed in Informatica Intelligent Cloud Services. Many connectors are pre-installed. However, you can also use a connector that is not pre-installed by installing an add-on connector created by Informatica or an Informatica partner.

Add-on connectors

Add-on connectors provide connectivity for connection types that are not installed by default in Informatica Intelligent Cloud Services.

When you install an add-on connector, the connector becomes available as a connection type for the organization and all sub-organizations. Users can create connections of this type and use them in tasks. Some connectors require configuration before you can use them.

If your organization includes sub-organizations, you install add-on connectors in the parent organization. You cannot install add-on connectors in a sub-organization. If a sub-organization should not use a connector that is available to the parent organization, disable the connector license for the sub-organization.

For information about individual connectors, see the help for the appropriate connector.

If you have a request for a connector that is not yet available, or if you would like information about building a connector, contact Informatica Global Customer Support.

Installing an add-on connector

You can install a free trial version of an Informatica Intelligent Cloud Services add-on connector, or you can buy the connector from Informatica. After you install an add-on connector, it becomes available as a connection type for the organization and all sub-organizations.

Note: If you want to install an add-on connector for use in a sub-organization, install the connector in the parent organization. You cannot install an add-on connector in a sub-organization.

1. In Administrator, select **Add-On Connectors**.
2. Perform either of the following steps:

- To start a free trial for an Informatica Intelligent Cloud Services Connector, click **Free Trial** for the connector, and confirm that you want to start the free trial.

- To buy a license for a connector with an expired free trial, click **Contact Us**.

  An Informatica representative will contact you.

After you install the connector, it is displayed on the **Add-On Connectors** page with the message, "Connector Available," and the connection type becomes available to your organization and sub-organizations. The connection type uses the naming convention `<connector name> (<publisher name>)`, for example, "Teradata (Informatica Cloud)."

CHAPTER 2

Connection configuration

When you configure a connection, the connection becomes available for use within the organization. If you use sub-organizations and you want a connection to be available to multiple sub-organizations, create the connection in each sub-organization.

Configure connections on the **Connections** page. The **Connections** page lists all of the connections that have been configured in the organization. You can create a connection on this page. You can also search for an existing connection by name or description, by name only, or by description only.

The following image shows the **Connections** page:
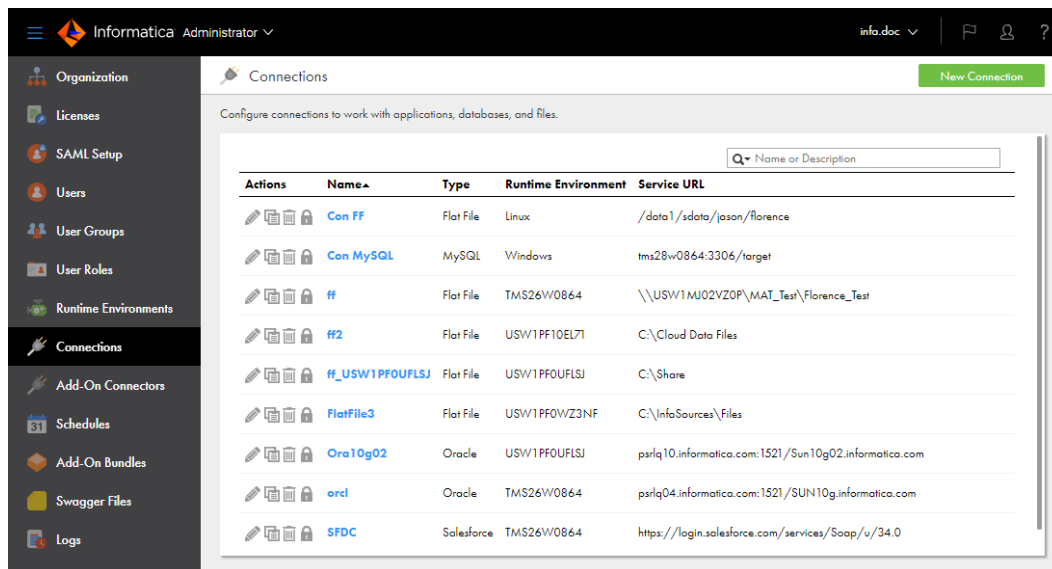
When you configure a connection, you specify the runtime environment for the connection. The runtime environment must contain an agent that is running. You can override the runtime environment in the connection from the mapping or mapping task.

The runtime environment manages the connection between Informatica Intelligent Cloud Services and the connection endpoint. It helps you perform the following tasks:

- Test the connection to the endpoint.
- Display objects available for the connection and retrieve metadata when you use the connection in an asset. You can preview data in the source, target, or lookup object selected in the asset.
- Run assets that use the connection to read from a source, transform data, or write data to a target.

You can configure a connection to a database, cloud data warehouse, or other endpoint type. When you create a source or target connection to a database or cloud data warehouse, you connect to a table, alias, or view. For example, when you create a Snowflake Data Cloud connection, you connect to a Snowflake table or

view. For more information about creating connections to different types of endpoints, see the help for the appropriate connector.

When you configure connections for sources and targets in a mapping or task, where the connections require you to specify the code page, ensure that the code pages are the same. If the source system and target system in a task use different code pages, the Informatica Intelligent Cloud Services might load unexpected data to the target.

You can delete any connection that you create as long as the connection is not used by a saved query or task.

Configuring a connection

You can create a connection for connectors that are installed in Informatica Intelligent Cloud Services. You can create a connection on the **Connections** page in Administrator or when you create a source, target, or lookup object in a mapping or task in Data Integration.

When you configure a connection, you specify properties for the connection. Connection properties enable an agent to connect to data sources.

1. Configure the following connection details:

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

2. Select the runtime environment to be used with the connection.

3. Configure the connection-specific properties.

   For example, if you configure a flat file connection, enter the directory where the files are stored, the date format for date fields in the files, and the code page of the system that hosts the files.

4. To test the connection, click **Test Connection**.

5. Click **Save**.

Configuring a connection using sample data

You can configure a connection to use sample data. You might want to use sample data when you want to test a mapping without affecting your organization's data.

When you configure a connection to use sample data, you can choose a mock connector from a variety of connector types such as Snowflake, Google BigQuery, and Salesforce. The connection properties are already configured.

1. On the **New Connection** page, select **Sample Data**.
2. Select a mock connector to use for the connection and click **OK**.
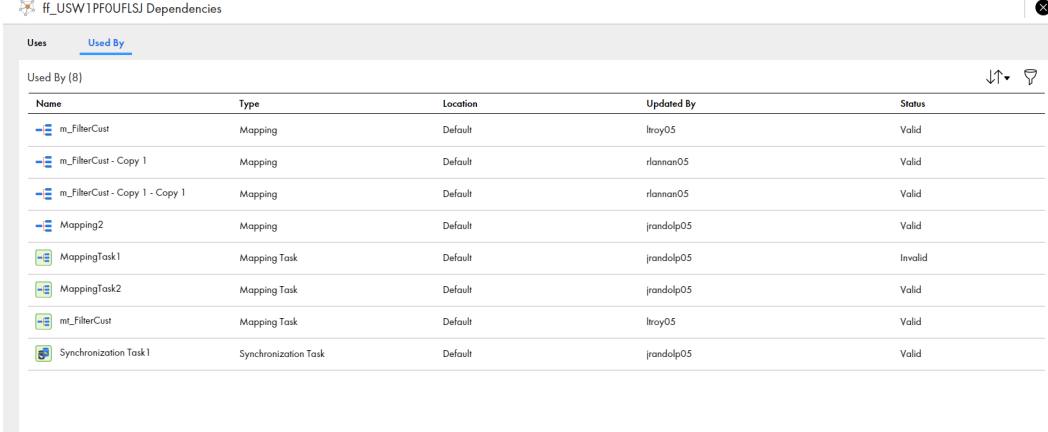
Viewing connection dependencies

You can view object dependencies for connections. When you view object dependencies for connections, Administrator lists the runtime environments that the connection uses as well as the assets in each service that use the connection.

To view object dependencies for a connection, on the Connections page, click the **Show Dependencies** icon.

The **Dependencies** page opens with showing the Uses tab by default. To see the assets that use the connection, select the Used By tab.

The following image shows the asset dependencies on the Used By tab for a connection:

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

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

CHAPTER 3

Connection properties

When you configure a connection, you specify the connection properties for the connection. Connection properties enable an agent to connect to data sources.

You can create a connection for connectors that are installed in Informatica Intelligent Cloud Services.

For more information about the properties that you need to configure to create a connection to a particular endpoint, see the help for the appropriate connector.

CHAPTER 4

FTP/SFTP Connections

File Transfer Protocol (FTP) connections enable you to use FTP to access source and target files. Secure File Transfer Protocol (SFTP) connections use secure protocols, such as SSH, to access source and target files.

When you configure an FTP/SFTP connection, you define the following directories:

Local directory

> Directory local to the Secure Agent that contains a copy of the source or target files.

Remote directory

> Location of the files you want to use as sources or targets.

Informatica Intelligent Cloud Services validates the file in the local directory, not the remote directory. When you configure FTP/SFTP connections, ensure that the local directory contains valid copies of all source and target files. When you configure a task with an FTP/SFTP connection, Informatica Intelligent Cloud Services uses the file structure of the local file to define the source or target for the task. The file structure of the local file must match the source or target file in the remote directory. Informatica Intelligent Cloud Services also uses the local file to generate data preview. If the data in the local file does not match the data in the source or target file in the remote directory, data preview might display inaccurate results.

When Informatica Intelligent Cloud Services runs a data integration task with a FTP/SFTP target connection, it creates a target file based on the target defined in the task. As it completes the task, Informatica Intelligent Cloud Services writes the target file to the remote directory, overwriting the existing file.

FTP/SFTP Connection Properties

The following table describes the FTP/SFTP connection properties:

Connection property	Description
Runtime Environment	Runtime environment that contains the Secure Agent to use to access the files.
User Name	User name used to log in to the FTP server.
Password	Password for the user name used to log in to the FTP server.
Host	Host name or IP address of the FTP/SFTP host.

Connection property	Description
Port	Network port number used to connect to FTP/SFTP connection. Default port is 21 for FTP and 22 for SFTP.
Local Directory	Directory on a local machine that stores the local file. The local machine must also run the Secure Agent used to run the corresponding task. Enter a local directory or use the Browse button to select a local directory.
Remote Directory	Directory on the FTP/SFTP host that stores the remote flat file. Depending on the FTP/SFTP server, you might have limited options to enter directories. For more information, see the FTP/SFTP server documentation.
Date Format	Date format for date fields in the flat file. Default date format is: MM/dd/yyyy HH:mm:ss
Code Page	Code page compatible with the system where the source or target flat file resides. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode data. - Shift-JIS. Select for double-byte character data. - ISO 8859-15 Latin 9 (Western European). - ISO 8859-2 Eastern European. - ISO 8859-3 Southeast European. - ISO 8859-5 Cyrillic. - ISO 8859-9 Latin 5 (Turkish). - IBM EBCDIC International Latin-1. - Japanese EUC (with \ <-> Yen mapping - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - MS Windows Traditional Chinese, superset of Big 5 - Taiwan Big-5 (w/o euro update) - Chinese EUC - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew (w/o euro update) - EBCDIC Hebrew (updated with new sheqel, control characters)
This is a Secure FTP Connection	Indicates whether the connection is secure or not secure. Select to create an SFTP connection.

Key exchange algorithms and ciphers

You can use the following key exchange algorithms and ciphers for SFTP connections:

Key exchange algorithms

- diffie-hellman-group14-sha1

- diffie-hellman-group-exchange-sha1

- diffie-hellman-group1-sha1

Ciphers

- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc (rijndael-cbc@lysator.liu.se)
- aes192-cbc
- aes128-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- arcfour
- arcfour128
- none

FTP/SFTP Connection Rules and Guidelines

Consider the following rules and guidelines for FTP/SFTP connections:

- Informatica Intelligent Cloud Services does not lock the target file while writing to the file. To prevent data corruption, verify that only one task writes to a target file at any given time.
- If metadata in the local target file and remote target file are different, Informatica Intelligent Cloud Services overwrites the metadata of the remote target file with the local target file at run time.
- To find the row count of rows loaded into the local target file, open the job details from the **All Jobs** or **My Jobs** page.
- In Windows, you cannot select FTP/SFTP directory on a mapped drive through the **Browse for Directory** dialog box. You can access a network directory by browsing My Network Places. You can also enter the directory with the following format:

      \\<server_name>\<directory_path>

  If the **Browse for Directory** dialog box does not display My Network Places, you might need to configure a network login for the Secure Agent service.
- Error messages for FTP/SFTP connections might only reference FTP or SFTP. Read any error message that references FTP or SFTP as an error message for an FTP/SFTP connection.

CHAPTER 5

REST V3 Connection Properties

When you set up a REST V3 connection, you must configure the connection properties.

When you create a connection, you can specify the following authentication methods:

- None. Does not require an authentication method to connect to the REST endpoint.
- Basic. Requires user ID and password to connect to the REST endpoint.
- OAuth 2.0 authorization code. Requires an authorization server to connect to the REST endpoint. Authorization Code allows authorized access to the endpoint without sharing or storing your credentials.
- OAuth 2.0 client credentials. Requires client ID and client secret to connect to the REST endpoint.

The following table describes the REST V3 connection properties for a basic authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select **Basic**. Default is None.
Auth User ID	The user name to log in to the web service application when you select the Basic authentication type.
Auth Password	The password associated with the user name when you select the Basic authentication type.
TrustStore File Path	The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.

Connection property	Description
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: - None. Bypasses the proxy server configured at the agent or the connection level. - Custom. Considers proxy configured at the connection level. - Platform. Considers proxy configured at the agent level. Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	The IP address or host name of the proxy server. Required only for the Custom proxy type.
Proxy Port	The port number of the proxy server. Required only for the Custom proxy type.
Proxy User	The user name for the proxy server. Required only for the Custom proxy type.
Proxy Password	The password for the proxy server. Required only for the Custom proxy type.
Connection Timeout	The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is 60 seconds. **Note:** If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the REST endpoint. You can select one of the following options: - HTTP 2 - HTTP 1.1 Default is HTTP 2.

Authorization Code Authentication

To use authorization code authentication, you must first register the following Informatica redirect URL in your application:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires and the error codes `400`, `401`, and `403` are returned in the response, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieve a new access token.

The following table describes the REST V3 connection properties for an OAuth 2.0 authorization code authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select **OAuth 2.0 authorization code**. Default is None.
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the REST endpoint has defined custom scopes. Enter space-separated scope attributes. For example: `root_readonly root_readwrite manage_app_users`
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: `[{"Name":"resource","Value":"https://<serverName>"}]`
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in the JSON format. For example: `[{"Name":"max_age","Value":60},{"Name":"state","Value":"test"}]`
Client Authentication	The client authentication details for authorization. Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is **Send client credentials in body**.
Generate Access Token	Generates access token and refresh token based on the authentication details provided.
Access Token	The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click **Generate Access Token** to populate the access token value. To pass the generate access token call through a proxy server, you must configure a proxy server at the Secure Agent level. The REST V3 connection-level proxy configuration does not apply to the generate access token call.

Connection property	Description
Refresh Token	Allows the Secure Agent to fetch new access token if the access token is not valid or expires. Enter the refresh token value or click **Generate Access Token** to populate the refresh token value. If the refresh token expires, you must either provide a valid refresh token or click **Generate Access Token** to regenerate a new refresh token.
TrustStore File Path	The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: - None. Bypasses the proxy server configured at the agent or the connection level. - Custom. Proxy configured at the connection level is considered. - Platform. Proxy configured at the agent level is considered. Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	The IP address or hostname of the proxy server. Required only for the Custom proxy type.
Proxy Port	The port number of the proxy server. Required only for the Custom proxy type.
Proxy User	The user name for the proxy server. Required only for the Custom proxy type.
Proxy Password	The password for the proxy server. Required only for the Custom proxy type.
Connection Timeout	The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is 60 seconds. **Note:** If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.

Connection property	Description
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the REST endpoint. You can select one of the following options: - HTTP 2 - HTTP 1.1 Default is HTTP 2.

Client Credential Authentication

The following table describes the REST V3 connection properties for OAuth 2.0 client credentials authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select **OAuth 2.0 client credentials**. Default is None.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the rest endpoint has defined custom scopes. Enter space-separated scope attributes. For example: `root_readonly root_readwrite manage_app_users`
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: `[{"Name":"resource","Value":"https://<serverName>"}]`
Client Authentication	The client authentication details for authorization. Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is **Send client credentials in body**.
Generate Access Token	Generates access token based on the authentication details provided.

Connection property	Description
Access Token	The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click **Generate Access Token** to populate the access token value. To pass the generate access token call through a proxy server, you must configure a proxy server at the Secure Agent level. The REST V3 connection-level proxy configuration does not apply to the generate access token call.
TrustStore File Path	The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: - None. Bypasses the proxy server configured at the agent or the connection level. - Custom. Considers proxy configured at the connection level. - Platform. Considers proxy configured at the agent level. Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	The IP address or host name of the proxy server. Required only for the Custom proxy type.
Proxy Port	The port number of the proxy server. Required only for the Custom proxy type.
Proxy User	The user name for the proxy server. Required only for the Custom proxy type.
Proxy Password	The password for the proxy server. Required only for the Custom proxy type.
Connection Timeout	The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is 60 seconds. **Note:** If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.

Connection property	Description
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the rest endpoint. You can select one of the following options: - HTTP 2 - HTTP 1.1 Default is HTTP 2.

Rules and guidelines for REST V3 connections

Consider the following rules and guidelines for Rest V3 connections:

- Test the connection to verify if the mandatory parameters are valid.

- You can configure proxy at the agent level or connection level. See the following table to understand the proxy settings that take precedence when you define the System proxy and proxy at the connection level:

System Proxy	REST V3 Connection Attribute			Result
	No Proxy	Platform Proxy	Custom Proxy	
No	Yes	No	No	Does not consider proxy.
No	No	Yes	No	Does not consider proxy.
No	No	No	Yes	Considers Custom proxy.
Yes	Yes	No	No	Does not consider proxy.
Yes	No	Yes	No	Considers Platform proxy.
Yes	No	No	Yes	Considers Custom proxy.

CHAPTER 6

SAP BAPI Connection Properties

The following table defines the SAP BAPI connection properties that you must configure on the **Connection Settings** section:

Connection Property	Description
Username	Required. SAP user name with authorization on S_DATASET, S_TABU_DIS, S_PROGRAM, and B_BTCH_JOB objects.
Password	Required. SAP password.
Host Name	Required. Logical name of the SAP system that you want to connect to.
Client	Required. SAP client number.
Language	Optional. Language code that corresponds to the SAP language.
System Number	Required. SAP system number.

SAP Additional Parameters	Optional. Additional SAP parameters that the Secure Agent must use to connect to the SAP system as an RFC client.
	
	For example, you can define the load balancing parameters as shown in the following sample:
	
	`GROUP=interfaces`
	`MSHOST=tzxscs20.bmwgroup.net`
	
	SAP infers the connection type based on the parameters that you specify. For example, if you define the GROUP and MSHOST parameters, SAP infers the connection type as a load balancing connection. The GROUP parameter defines the group name of the SAP application server and the MSHOST parameter defines the host name of the SAP message server.
	
	You can define the `DOCOMMIT=true` parameter to commit data to the SAP system with each BAPI/RFC call.
	
	For more information about SAP parameters, see the SAP documentation.
	
	You can also enable the Secure Network Communication (SNC) protocol and secure communications between Application Integration and SAP by adding properties in the **SAP Additional Parameters** field. For more information about configuring the SNC parameters, see How to configure the SAP Secure Network Communication Protocol in Application Integration.
	
	Note: If you configure a parameter in both the **SAP Additional Parameters** field and in other connection property fields, the values in the **SAP Additional Parameters** field override the values in the connection property fields.

Connection Property	Description
Jco Trace	Optional. Enables or disables JCo trace. Default is **No**. If you enable JCo trace, you can access the JCo trace file from the following directory: `<Secure Agent installation directory>\apps\process-engine\<latest_version>`
Object Filter	Optional. Fully qualified name of the BAPI function that you want to connect to. You can specify a single BAPI name.

INDEX

W

web site [4]