



Informatica® Intelligent Cloud Services  
September 2023

# Connections

Informatica Intelligent Cloud Services Connections  
September 2023

© Copyright Informatica LLC 2006, 2024

Publication Date: 2024-10-01

# Table of Contents

<b>Chapter 1: Connectors and connections.....</b>	<b>9</b>
Add-on connectors. . . . .	9
Installing an add-on connector. . . . .	9
 <b>Chapter 2: Connection configuration.....</b>	 <b>11</b>
Configuring a connection. . . . .	12
Viewing connection dependencies. . . . .	13
 <b>Chapter 3: Connection properties.....</b>	 <b>15</b>
Adabas CDC Connection Properties. . . . .	15
Adabas connection properties. . . . .	17
Adobe Analytics Mass Ingestion connection properties. . . . .	19
Adobe Experience Platform connection properties. . . . .	19
Advanced FTP V2 connection properties. . . . .	20
Advanced FTPS V2 connection properties. . . . .	22
Advanced SFTP V2 connection properties. . . . .	24
Amazon Athena connection properties. . . . .	25
AMQP connection properties. . . . .	26
Amazon Aurora connection properties. . . . .	28
Amazon DynamoDB V2 connection properties. . . . .	29
Amazon Kinesis connection properties. . . . .	29
Amazon Kinesis Firehose connection properties. . . . .	30
Amazon Kinesis Streams connection properties. . . . .	31
Amazon Redshift connection properties. . . . .	32
Amazon Redshift V2 connection properties. . . . .	34
Amazon S3 connection properties. . . . .	38
Amazon S3 V2 connection properties. . . . .	39
Anaplan V2 connection properties. . . . .	44
Ariba V2 connection properties. . . . .	46
AS2 connection properties. . . . .	47
Connection properties. . . . .	47
Message properties. . . . .	49
Receipt properties. . . . .	50
Proxy properties. . . . .	51
Birst Cloud Connect connection properties. . . . .	51
Business 360 connection properties. . . . .	52
Business 360 Events connection properties. . . . .	53
Business 360 FEP Connection Properties. . . . .	53
CallidusCloud Commissions connection properties. . . . .	54
CallidusCloud File Processor connection properties. . . . .	55

Chatter connection properties. . . . .	57
Concur V2 connection properties. . . . .	57
Cassandra V2 connection properties. . . . .	59
Couchbase connection properties. . . . .	60
Coupa V2 connection properties. . . . .	61
Cvent connection properties. . . . .	62
Databricks Delta connection properties. . . . .	63
AWS cluster properties. . . . .	66
Azure cluster properties. . . . .	67
Datacom CDC Connection Properties. . . . .	68
Datacom Connection Properties. . . . .	70
Db2 Data Map connection properties. . . . .	72
Db2 for i CDC connection properties. . . . .	74
Db2 for i connection properties. . . . .	76
Db2 for i Database Ingestion connection properties. . . . .	78
Db2 for LUW CDC connection properties. . . . .	79
Db2 for LUW Database Ingestion connection properties. . . . .	82
Db2 for z/OS Bulk Load connection properties. . . . .	83
Db2 for z/OS CDC connection properties. . . . .	84
Db2 for z/OS connection properties. . . . .	86
Db2 for z/OS Image Copy connection properties. . . . .	88
Db2 for z/OS Unload File connection properties. . . . .	90
Db2 for zOS Database Ingestion connection properties. . . . .	92
DB2 Loader connection properties. . . . .	93
Db2 Warehouse on Cloud connection properties. . . . .	94
Domo connection properties. . . . .	95
Dropbox connection properties. . . . .	96
Elasticsearch connection properties. . . . .	97
Eloqua Bulk API connection properties. . . . .	98
Eloqua REST connection properties. . . . .	99
FHIR connection properties. . . . .	100
OAuth 2.0 authorization code authentication. . . . .	102
OAuth 2.0 client credentials authentication. . . . .	103
FileIO connection properties. . . . .	104
File List connection properties. . . . .	105
File Processor connection properties. . . . .	106
Flat file connections. . . . .	107
Flat file connection properties. . . . .	107
Configuring a locale in Linux for flat file connections. . . . .	108
FTP/SFTP connections. . . . .	109
FTP/SFTP connection properties. . . . .	109
Key exchange algorithms and ciphers. . . . .	110

FTP/SFTP connection rules and guidelines. . . . .	111
Google Ads connection properties. . . . .	111
Google Analytics connection properties. . . . .	112
Google Analytics Mass Ingestion connection properties. . . . .	113
Google BigQuery connection properties. . . . .	113
Connection modes. . . . .	114
Rules and guidelines for Google BigQuery connection modes. . . . .	118
Google BigQuery V2 connection properties. . . . .	119
Connection modes. . . . .	122
Rules and guidelines for Google BigQuery V2 connection modes. . . . .	125
Google Bigtable connection properties. . . . .	127
Google Cloud Spanner connection properties. . . . .	127
Google Cloud Storage connection properties. . . . .	128
Google Cloud Storage V2 connection properties. . . . .	129
Google Drive connection properties. . . . .	130
Google PubSub connection properties. . . . .	131
Google PubSub V2 connection properties. . . . .	131
Google PubSub - Mass Ingestion Streaming connection properties. . . . .	132
Google Sheets connection properties. . . . .	133
Google Sheets V2 connection properties. . . . .	134
Greenplum connection properties. . . . .	134
Hadoop Files V2 connection properties. . . . .	135
Hive connection properties. . . . .	137
HubSpot connection properties. . . . .	139
IBM MQ connection properties. . . . .	139
IDMS CDC connection properties. . . . .	140
IDMS connection properties. . . . .	142
IMS CDC Connection Properties. . . . .	144
IMS connection properties. . . . .	146
JDBC connection properties. . . . .	148
JDBC V2 connection properties. . . . .	149
JD Edwards EnterpriseOne connection properties. . . . .	150
JIRA connection properties. . . . .	152
JIRA Cloud connection properties. . . . .	152
JMS connection properties. . . . .	153
JSON Target connection properties. . . . .	154
Kafka connection properties. . . . .	155
LDAP connection properties. . . . .	158
Litmos connection properties. . . . .	159
Marketo V3 connection properties. . . . .	159
Microsoft Access connection properties. . . . .	160
Microsoft Azure Blob Storage V2 connection properties. . . . .	161

Microsoft Azure Blob Storage V3 connection properties. . . . .	161
Microsoft Azure Cosmos DB SQL API connection properties. . . . .	162
Microsoft Azure Data Lake Storage Gen1 V2 connection properties. . . . .	163
Microsoft Azure Data Lake Storage Gen1 V3 connection properties. . . . .	163
Microsoft Azure Data Lake Storage Gen2 connection properties . . . . .	164
Microsoft Azure Event Hub connection properties. . . . .	166
Microsoft Azure SQL Data Warehouse - Database Ingestion connection properties. . . . .	167
Microsoft Azure SQL Data Warehouse V2 connection properties. . . . .	168
Microsoft Azure Synapse SQL connection properties. . . . .	169
Microsoft Azure Synapse Analytics Database Ingestion connection properties. . . . .	171
Microsoft CDM Folders V2 connection properties. . . . .	173
Microsoft Dynamics 365 for Operations connection properties. . . . .	174
Microsoft Dynamics 365 for Sales connection properties. . . . .	175
Microsoft Dynamics 365 Mass Ingestion connection properties. . . . .	176
Microsoft Dynamics AX V3 connection properties. . . . .	179
Microsoft Excel connection properties. . . . .	180
Microsoft SharePoint connection properties. . . . .	180
Microsoft Sharepoint Online connection properties. . . . .	181
Microsoft SQL Server CDC connection properties. . . . .	182
Microsoft SQL Server connection properties. . . . .	184
MLLP connection properties. . . . .	187
MongoDB V2 connection properties. . . . .	188
Additional connection properties. . . . .	189
Configure SSL for the serverless runtime environment. . . . .	190
MQTT connection properties. . . . .	191
MRI Software connection properties . . . . .	192
MySQL CDC connection properties. . . . .	193
MySQL connection properties. . . . .	195
SSL properties. . . . .	196
Netezza connection properties. . . . .	199
NetSuite Mass Ingestion connection properties. . . . .	199
NICE Satmetrix connection properties. . . . .	201
OData connection properties. . . . .	201
OData V2 Protocol Writer connection properties. . . . .	202
OData V2 Protocol Reader connection properties. . . . .	203
Authorization code authentication. . . . .	204
Client credential authentication. . . . .	206
ODBC connection properties. . . . .	207
OpenAir connection properties. . . . .	209
Oracle Business Intelligence Publisher V1 connection properties. . . . .	210
Oracle CDC V2 connection properties. . . . .	211
Oracle Cloud Object Storage connection properties. . . . .	214

Oracle connection properties. . . . .	215
Oracle CRM Cloud V1 connections properties. . . . .	218
Oracle CRM On Demand connection properties. . . . .	218
Oracle Database Ingestion connection properties. . . . .	219
Oracle E-Business Suite connection properties. . . . .	224
Oracle E-Business Suite Interface connection properties. . . . .	225
Oracle Financials Cloud connections properties. . . . .	227
Oracle Financials Cloud V1 connections properties. . . . .	228
Oracle Fusion Cloud Mass Ingestion connection properties. . . . .	230
Oracle HCM Cloud connection properties. . . . .	230
Oracle HCM Cloud V1 connection properties. . . . .	232
PostgreSQL CDC connection properties. . . . .	234
PostgreSQL connection properties. . . . .	236
QuickBooks V2 Connection Properties. . . . .	238
Redis connection properties. . . . .	238
REST V2 connection properties. . . . .	239
OAuth 2.0 client credentials authentication. . . . .	242
OAuth 2.0 authorization code authentication. . . . .	244
JWT bearer token authentication. . . . .	247
API key authentication. . . . .	251
Rules and guidelines for REST V2 connections. . . . .	254
REST V3 Connection Properties. . . . .	255
Authorization Code Authentication. . . . .	256
Client Credential Authentication. . . . .	259
Rules and guidelines for REST V3 connections. . . . .	261
Salesforce Analytics connection properties. . . . .	262
Salesforce connection properties. . . . .	262
Salesforce Marketing Cloud connection properties. . . . .	264
Salesforce Mass Ingestion connection properties. . . . .	265
SAP ADSO Writer connection properties. . . . .	268
SAP BW BEx Query connection properties. . . . .	272
SAP BW Reader connection properties. . . . .	273
SAP HANA CDC Connection Properties. . . . .	275
SAP HANA connection properties. . . . .	278
SAP HANA Database Ingestion connection properties. . . . .	279
SAP IDoc Reader connection properties. . . . .	280
SAP IDoc Writer connection properties. . . . .	280
SAP IQ connection properties. . . . .	281
SAP Mass Ingestion connection properties. . . . .	282
SAP RFC/BAPI interface connection properties. . . . .	287
SAP Table connection properties . . . . .	288
SAP ODP Extractor connection properties. . . . .	290

SAS connection properties. . . . .	295
Satmetrix connection properties. . . . .	295
ServiceNow connection properties. . . . .	296
Sequential File connection properties. . . . .	296
ServiceNow Mass Ingestion connection properties. . . . .	298
Snowflake Data Cloud connection properties. . . . .	299
Standard authentication. . . . .	300
OAuth 2.0 authorization code authentication. . . . .	301
Key pair authentication. . . . .	303
OAuth 2.0 client credentials authentication. . . . .	304
SuccessFactors LMS connection properties. . . . .	306
SuccessFactors ODATA connection properties. . . . .	307
SuccessFactors SOAP connection properties. . . . .	308
Tableau V3 connection properties. . . . .	309
Teradata connection properties. . . . .	310
UKGPro connection properties. . . . .	312
UKGPro V2 connection properties. . . . .	313
UltiPro connection properties. . . . .	315
VSAM CDC connection properties. . . . .	316
VSAM connection properties. . . . .	318
Web Service Consumer connection properties. . . . .	319
Workday Mass Ingestion connection properties. . . . .	320
Workday V2 connection properties. . . . .	322
Xactly connection properties. . . . .	323
XML Source connection properties. . . . .	324
XML Target connection properties. . . . .	324
Yellowbrick Data Warehouse connection properties. . . . .	325
Zendesk Mass Ingestion connection properties. . . . .	326
Zendesk V2 connection properties. . . . .	327
Zuora AQuA connection properties. . . . .	328
Zuora Multi-Entity connection properties. . . . .	329
Zuora REST V2 connection properties. . . . .	330
<b>Chapter 4: Swagger file generation for REST V2 connections.....</b>	<b>332</b>
Generating a Swagger file. . . . .	332
<b>Index. ....</b>	<b>335</b>

## 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)."

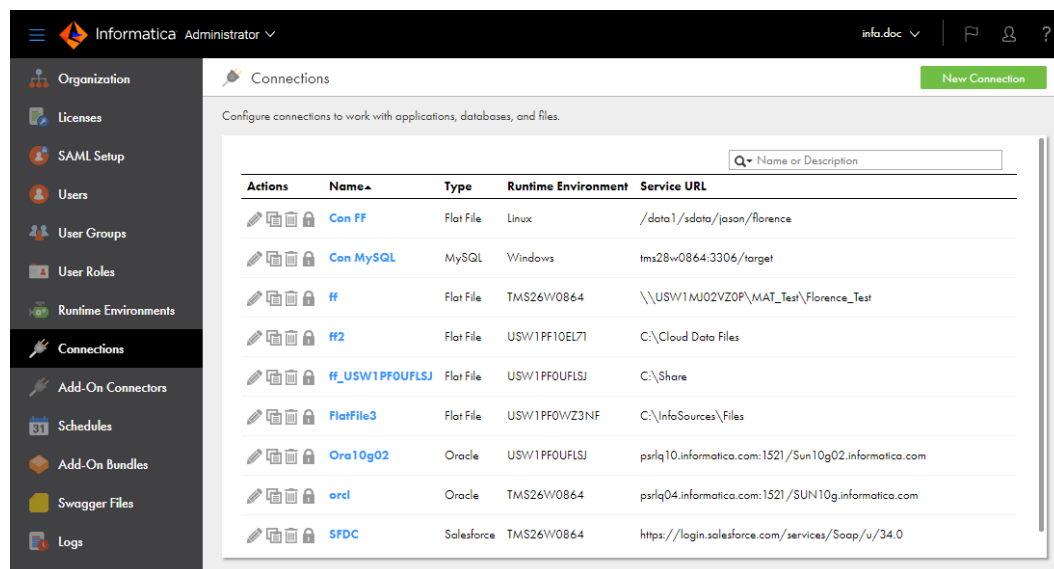
## CHAPTER 2

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

You can configure a connection to a database. When you create a source connection to a database, you create the connection to a database table, alias, or view. When you create a target connection to a database, you create a connection to a database table.

When you configure connections for sources and targets in a mapping or task, 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 configure a connection on the **Connections** page in Administrator or in a wizard when you configure a mapping or task.

1. Perform either of the following steps:
  - In Administrator, select **Connections**.
  - In Data Integration, open a source, target, or lookup object in a mapping or task.
2. Click **New Connection**.
3. 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.

4. Configure the connection-specific properties.

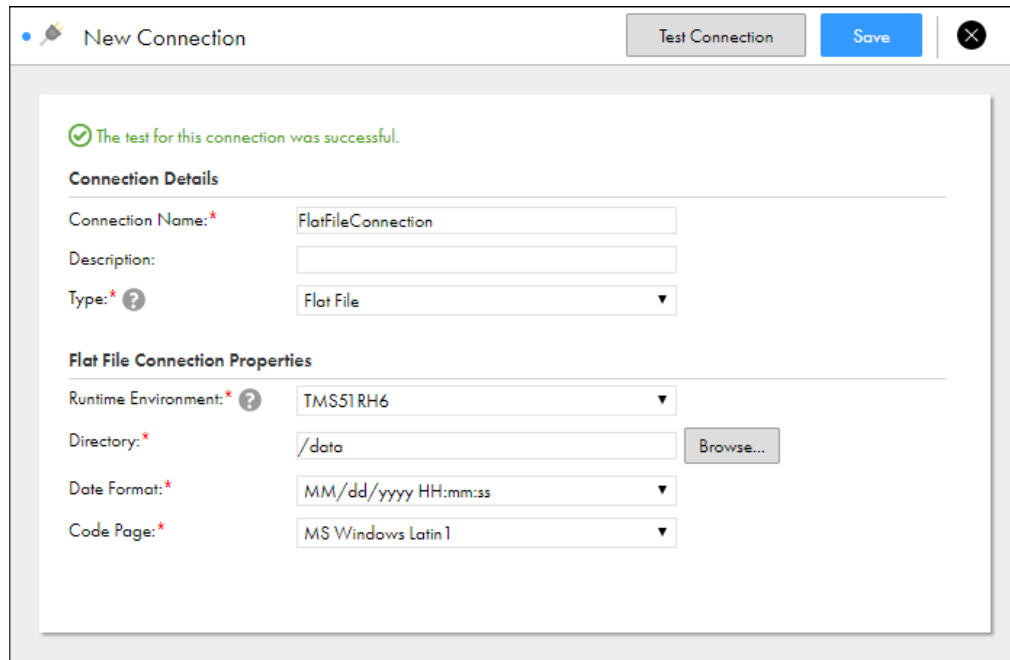
For example, if you configure a flat file connection, enter the runtime environment to be used with the connection, the directory where the files are stored, the date format for date fields in the files, and the code page of the system that hosts the files.

The following image shows the properties for a flat file connection:

The screenshot shows the 'New Connection' wizard interface. At the top, there's a title bar with a pin icon, the text 'New Connection', and buttons for 'Test Connection', 'Save', and a close icon. The main content area is divided into two sections. The first section, 'Connection Details', contains three fields: 'Connection Name' (required, marked with a red asterisk) with the value 'FlatFileConnection', 'Description' (optional), and 'Type' (required, marked with a red asterisk and a question mark icon) with a dropdown menu set to 'Flat File'. The second section, 'Flat File Connection Properties', contains four fields: 'Runtime Environment' (required, marked with a red asterisk and a question mark icon) with a dropdown menu set to 'Select...', 'Directory' (required, marked with a red asterisk) with a text input field and a 'Browse...' button, 'Date Format' (required, marked with a red asterisk) with a dropdown menu set to 'MM/dd/yyyy HH:mm:ss', and 'Code Page' (required, marked with a red asterisk) with a dropdown menu.

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

The results of the test are displayed on the page, as shown in the following image:



The screenshot shows a 'New Connection' dialog box with a success message: 'The test for this connection was successful.' Below this, the 'Connection Details' section includes fields for 'Connection Name' (FlatFileConnection), 'Description', and 'Type' (Flat File). The 'Flat File Connection Properties' section includes fields for 'Runtime Environment' (TMS51RH6), 'Directory' (/data), 'Date Format' (MM/dd/yyyy HH:mm:ss), and 'Code Page' (MS Windows Latin 1). Buttons for 'Test Connection', 'Save', and a close button are visible at the top right.

If a database connection fails, contact the database administrator.

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

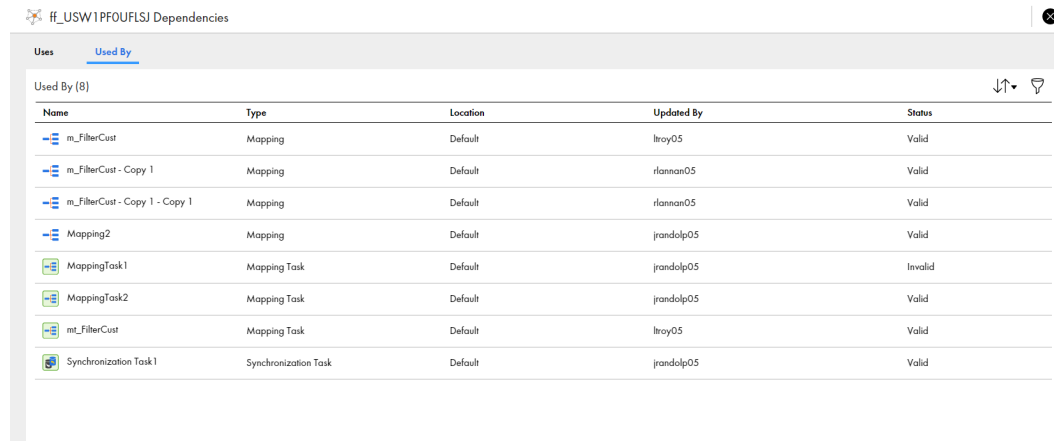
## Viewing connection dependencies

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:



Name	Type	Location	Updated By	Status
m_FilterCust	Mapping	Default	ltroy05	Valid
m_FilterCust - Copy 1	Mapping	Default	rlannan05	Valid
m_FilterCust - Copy 1 - Copy 1	Mapping	Default	rlannan05	Valid
Mapping2	Mapping	Default	jrandolp05	Valid
MappingTask1	Mapping Task	Default	jrandolp05	Invalid
MappingTask2	Mapping Task	Default	jrandolp05	Valid
mt_FilterCust	Mapping Task	Default	ltroy05	Valid
Synchronization Task1	Synchronization Task	Default	jrandolp05	Valid

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

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

## Adabas CDC Connection Properties

When you configure an Adabas CDC connection, you must set the connection properties.

The following table describes Adabas CDC connection properties:

Property	Description
Connection Name	A name for the Adabas CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Adabas CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Adabas CDC, the type must be <b>Adabas CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Adabas change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: ADACDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .

Property	Description
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Adabas instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Adabas source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: ADACDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.

Property	Description
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Adabas table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPCL) Adabas CDC connections in PowerCenter.

## Adabas connection properties

When you configure an Adabas connection, you must set the connection properties.

The following table describes the Adabas connection properties:

Property	Description
Connection Name	A name for the Adabas connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Adabas connection. Maximum length is 4000 characters.
Type	Type of connection. For Adabas, the type must be <b>Adabas</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Adabas runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <div style="text-align: center;"><i>host_name:port_number</i></div> For example: ADALSNR:14673
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .

Property	Description
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name in the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processing transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> Default is No.
Offload Threads	The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs. Valid values are 1 through 64. Default is 0, which disables multithreading. Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.
Array Size	For Adabas data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions. For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size. Valid values are from 1 through 5000. Default is 25. To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b> , increase the array size.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Adabas connections in PowerCenter.
Write Mode	Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On</b>. Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off</b>. Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> Default is <b>Confirm Write On</b> .

# Adobe Analytics Mass Ingestion connection properties

When you set up an Adobe Analytics Mass Ingestion connection, you must configure the connection properties.

Adobe Analytics uses a JSON Web Token (JWT) to authenticate the Adobe Analytics Mass Ingestion connection. To use an Adobe Analytics Mass Ingestion connection, you must create a Service Account Integration on Adobe Developer Console and then specify the service integration details in the connection properties. For more information about creating a Service Account Integration on Adobe Developer Console, see the [Adobe documentation](#).

The following table describes the connection properties for an Adobe Analytics Mass Ingestion connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the Service Account that you created on Adobe Developer Console.
Client Secret	Client secret of the Service Account that you created on Adobe Developer Console.
Technical Account ID	Technical account ID of the Service Account.
Organization ID	Organization ID of the Service Account.
Private Key	Private key that is generated when you create the Service Account Integration. The private key is required to generate the JWT.
IMS Host	Base URL of Adobe Identity Management System (IMS). The default value is: <code>ims-na1.adobelogin.com</code>
IMS Exchange	Exchange URL of IMS. The connection use the JWT to obtain an access token from Adobe by making a POST request to the exchange URL. The default value is: <code>https://ims-na1.adobelogin.com/ims/exchange/jwt</code>

## Adobe Experience Platform connection properties

When you set up an Adobe Experience Platform connection, you must configure the connection properties.

After you generate a service integration, you can get the organization specific properties that are required to generate the access token.

To obtain access token for your integration, you must first create a JSON Web Token (JWT) that encapsulates your client credentials. For each API session, you can exchange your JWT for an access token from Adobe IMS. The token identifies your integration and grants access to the services you have configured.

The following table describes the Adobe Experience Platform connection properties that are required to generate a JWT token every time you connect to Adobe Experience Platform:

Property	Description
Environment	The Adobe Experience Platform environment. Select prod.
Private Key Path	Path of the private key on the Secure Agent machine. Enter the private key path without the drive name. For example, if the private key file resides in the C drive path C:\a_IOD\Files\AdobeExperiencePlatform\key.der then the private key path is: file:///a_IOD/Files/AdobeExperiencePlatform/key.der
Client Id	Client ID in Adobe Experience Platform required for generating a valid access token.
Client Secret	The client secret key in Adobe Experience Platform required for generating a valid access token.
Account Id	The Adobe Experience Platform Account ID.
IMS Org	The Adobe Identity Management System (IMS) Organization ID.
Sandbox Name	Optional. Name of the Adobe Experience Platform sandbox account that you want to connect to.

## Advanced FTP V2 connection properties

When you set up an Advanced FTP V2 connection, you must configure the connection properties.

The following table describes the Advanced FTP V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*() - + = { }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced FTP V2</b> connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent.
Host	The host name or IP address of the FTP server.
Port	The port number to use for connecting to the FTP server. If left blank, the default port number 21 is used.
Username	User name to connect to the FTP server.
Password	Password to connect to the FTP server.

Connection property	Description
Folder Path	The directory to use after connecting to the FTP server.
Use passive mode	<p>Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode.</p> <p>The default value is <b>Yes</b>.</p> <p>In Passive mode, the server does not need to connect back to a port on the connection client, which is a firewall-friendly mode. If you have problems with connecting to the server, you might want to change the mode to Passive by selecting <b>Yes</b> for this option. In Passive mode, depending on the FTP server, the connection may require high port range based on the port availability to transfer data.</p> <p>In Active mode, the server attempts to connect back to a port on the connection client to perform the data transfer.</p>
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the FTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.
Connection Retry Interval	<p>The number of seconds to wait between each connection retry attempt.</p> <p><b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b>.</p>
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings such as UTF-8 can be specified to support international characters.
List Parser	The list parser to use for the server connection. If the field is left blank, the Advanced FTP V2 Connector attempts to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser is used. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting ignores any user specified value.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting ignores any user-specified value.

**Note:** Advanced FTP V2 connector doesn't support NTLM proxy authentication.

# Advanced FTPS V2 connection properties

When you set up an Advanced FTPS V2 connection, you must configure the connection properties.

The following table describes the Advanced FTPS V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced FTPS V2</b> connection type.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
Username	User name to connect to the FTPS server.
Password	Password to connect to the FTPS server.
Folder Path	The directory to use after connecting to the server.
Use passive mode	<p>Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode.</p> <p>The default value is <b>Yes</b>.</p> <p>In Passive mode, the server does not need to connect back to a port on the connection client, which is a firewall-friendly mode. If you have problems with connecting to the server, you might want to change the mode to Passive by selecting <b>Yes</b> for this option. In Passive mode, depending on the FTPS server, the connection may require high port range based on the port availability to transfer data.</p> <p>In Active mode, the server attempts to connect back to a port on the connection client to perform the data transfer.</p>
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs will if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the Advanced FTP V2 connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.

Connection property	Description
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support international characters.
Trusted Server	Specify whether the FTPS server is a trusted server. The Advanced FTP V2 Connector only supports a trusted server.
List Parser	The list parser to use for the server connection. If the field is empty, the Advanced FTP V2 Connector tries to use the MLSD parser. If the server does not support the MLSD parser, the connector uses the UNIX parser. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting ignores any user specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting ignores any user-specified values.
Connection Type	Indicates if the connection type is IMPLICIT_SSL or EXPLICIT_SSL. - IMPLICIT_SSL. The connection automatically starts as an SSL connection. - EXPLICIT_SSL. After initial authentication with the FTPS server, the connection is encrypted with SSL or TLS depending on the security protocol you select. Default is IMPLICIT_SSL.
SecurityProtocol	Indicates whether SSL or TLS is used for EXPLICIT_SSL connections. Default is SSL.
Key Store File	The path and file name of the keystore file. The keystore file contains the certificates to authenticate the FTPS server.
Key Store Password	The password for the keystore file required to access the Trusted Server Certificate Store.
Key Alias	The alias of the individual key.
Key Store Type	Indicates if the type of the keystore is Java KeyStore (JKS) or Public Key Cryptology Standard (PKCS12). Default is JKS.

**Note:** Advanced FTPS V2 connector doesn't support NTLM proxy authentication.

# Advanced SFTP V2 connection properties

When you set up an Advanced SFTP V2 connection, you must configure the connection properties.

The following table describes the Advanced SFTP V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ ` ! \$ % ^ & * ( ) - + = { } ]   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced SFTP V2</b> connection type.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server.
Port	The port number to use to connect to the server. Default is 21.
Username	User name to connect to the SFTP server.
Password	Password to connect to the SFTP server.
Folder Path	The directory to use after connecting to the server.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the SFTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. For example, if you want to retry to connect up to 10 times with a five second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.
Private Key File	The name of the SSH private key file along with the path where the file is stored. Ensure that the file path is on the machine that hosts the Secure Agent. For example, C:/SSH/my_keys/key.ppk
Private Key Passphrase	Specify the passphrase to encrypt the SSH private key.
Use Curve Kex Algorithm	Enable additional key exchange algorithms such as curve, and keyed-hash algorithm such as, -hmac-sha2-512, and -hmac-sha2-256.

Connection property	Description
Use File Integration Proxy Server	The connector connects to the SFTP server through the file integration proxy server. Verify that the following prerequisites are met: <ul style="list-style-type: none"> <li>- You must have the File Integration Service license to use this option.</li> <li>- You must define a proxy server in File Servers.</li> <li>- If you don't have the File Integration Service proxy, you need to use the agent proxy through the proxy.ini file.</li> </ul>
Proxy Server Host Name	Host name or IP address of the outgoing File Integration Service proxy server.
Proxy Server Port	Port number of the outgoing File Integration Service proxy server.

**Note:** Advanced SFTP V2 connector doesn't support NTLM proxy authentication.

## Amazon Athena connection properties

When you set up an Amazon Athena connection, you must configure the connection properties.

The following table describes the Amazon Athena connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Amazon Athena connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication Type	The authentication mechanism to connect to Amazon Athena. Select <b>Permanent IAM Credentials</b> .
Access Key	Optional. The access key to connect to Amazon Athena.
Secret Key	Optional. The secret key to connect to Amazon Athena.

Property	Description
JDBC URL	<p>The URL of the Amazon Athena connection.</p> <p>Enter the JDBC URL in the following format:</p> <pre>jdbc:awsathena://AwsRegion=&lt;region_name&gt;;S3OutputLocation=&lt;S3_Output_Location&gt;;</pre> <p>You can use pagination to fetch the Amazon Athena query results. Set the property <code>UseResultsetStreaming=0</code> to use pagination.</p> <p>Enter the property in the following format:</p> <pre>jdbc:awsathena:// AwsRegion=&lt;region_name&gt;;S3OutputLocation=&lt;S3_Output_Location&gt;;UseResultsetStreaming=0;</pre> <p>You can also use streaming to improve the performance and fetch the Amazon Athena query results faster. When you use streaming, ensure that port 444 is open.</p> <p>By default, streaming is enabled.</p>
Customer Master Key ID	<p>Optional. Specify the customer master key ID generated by AWS Key Management Service (AWS KMS) or the Amazon Resource Name (ARN) of your custom key for cross-account access.</p> <p>You must generate the customer master key ID for the same region where your Amazon S3 bucket resides. You can either specify the customer-generated customer master key ID or the default customer master key ID.</p>

## AMQP connection properties

When you set up an AMQP connection, you must configure the connection properties.

The following table describes the AMQP connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <pre>~ ` ! \$ % ^ &amp; * ( ) - + = { [ ] }   \ : ; " ' &lt; , &gt; . ? /</pre>
Description	<p>Optional. Description that you can use to identify the connection.</p> <p>The description cannot exceed 4,000 characters.</p>
Type	<p>The AMQP connection type.</p> <p>If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.</p>
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Host Name	Network address of the AMQP broker.
Port	<p>Port number of the AMQP broker to which the underlying TCP connection is made.</p> <p>Default is 5672.</p>
Virtual Host	<p>Virtual host name that identifies the AMQP system.</p> <p>Use the virtual host name for enhanced security.</p>

Property	Description
Username	Username for the AMQP broker.
Password	Password for the AMQP broker.
Use SSL	Enable this option to use SSL for secure transmission. If you enable the SSL authentication, ensure that you provide both keystore and truststore details for using the AMQP connection in a streaming ingestion task.
Keystore File Name	Contains the keys and certificates required for secure communication.
Keystore Password	Password for the keystore filename.
Keystore Type	Type of keystore that you want to use. Keystore type defines the storage and data format of the keystore information and the algorithms used to protect private keys in the keystore. Use one of the following types: <ul style="list-style-type: none"> <li>- JKS. Stores private keys and certificates.</li> <li>- PKCS12. Stores private keys, secret keys, and certificates.</li> </ul>
Truststore File Name	Name of the truststore file.
Truststore Password	Password for the truststore file.
Truststore Type	Type of truststore that you want to use. Use one of the following types: <ul style="list-style-type: none"> <li>- JKS</li> <li>- PKCS 12</li> </ul>
TLS Protocol	Transport protocols that you want to use. Use one of the following types: <ul style="list-style-type: none"> <li>- SSL</li> <li>- SSLv2Hello</li> <li>- SSLv3</li> <li>- TLS</li> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul>
Client Authentication	Client authentication policy when connecting to the secured AMQP broker. Use one of the following property values when you define and enable an SSL context. <ul style="list-style-type: none"> <li>- WANT</li> <li>- REQUIRED</li> <li>- NONE</li> </ul>

# Amazon Aurora connection properties

When you set up an Amazon Aurora connection, configure the connection properties.

The following table describes the Amazon Aurora connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Amazon Aurora connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Host	Amazon Aurora server host name. For example, xyzcloud-cluster.cluster-cj8irzt1lmku.us-west-2.rds.amazonaws.com.
Port	Amazon Aurora directory server port number.
Database Name	Name of the Amazon Aurora database.
Code Page	The code page of the database server defined in the connection. Select one of the following code pages: <ul style="list-style-type: none"><li>- MS Windows Latin 1</li><li>- UTF-8</li><li>- Shift-JIS</li><li>- ISO 8859-15 Latin 9 (Western European)</li><li>- ISO 8859-2 Eastern European</li><li>- ISO 8859-3 Southeast European</li><li>- ISO 8859-5 Cyrillic</li><li>- ISO 8859-9 Latin 5 (Turkish)</li><li>- IBM EBCDIC International Latin-1</li></ul>
Metadata Advanced Connection Properties	Additional properties for the JDBC driver to fetch metadata from the source. For example, <code>connectTimeout=180000</code> For more metadata advanced connection properties, see <a href="#">MariaDB Connector for JDBC</a> .
Run-time Advanced Connection Properties	Additional properties for the ODBC driver required at run time. For example, <code>charset=sjis;readtimeout=180</code> For more run-time advanced connection properties, see <a href="#">MariaDB Connector for ODBC</a> .
Username	User name of the Amazon Aurora account.
Password	Password of the Amazon Aurora account.

# Amazon DynamoDB V2 connection properties

When you set up an Amazon DynamoDB V2 connection, you must configure the connection properties.

The following table describes the Amazon DynamoDB V2 connection properties:

Connection property	Description
Connection Name	The 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The DynamoDB V2 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Access Key	The access key to access Amazon DynamoDB. You can optionally enter the access key when you use assume role for an IAM user.
Secret Key	The secret key to access Amazon DynamoDB. This value is associated with the access key and uniquely identifies the account. You can optionally enter the secret key when you use assume role for an IAM user.
Region Name	The AWS region of Amazon DynamoDB that you want to access.
Assume Role	Enables the IAM entity to assume a role.
Assume Role ARN	The ARN of the IAM role assumed by the IAM user to generate the temporary security credentials.
External Id	The external ID to generate the temporary security credentials.

# Amazon Kinesis connection properties

The Amazon Kinesis connection is a messaging connection. Use the Amazon Kinesis connection to access Amazon Kinesis Data Streams or Amazon Kinesis Data Firehose as targets.

## Amazon Kinesis Firehose connection properties

When you set up an Amazon Kinesis Firehose connection, you must configure the connection properties.

The following table describes the Amazon Kinesis Firehose connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <p>~ ` ! \$ % ^ &amp; * ( ) - + = { [ ]   \ : ; " ' &lt; , &gt; . ? /</p>
Description	<p>Optional. Description that you can use to identity the connection.</p> <p>The description cannot exceed 4,000 characters.</p>
Type	<p>The Amazon Kinesis connection type.</p> <p>If you do not see the Amazon Kinesis connection type, go to the <b>Add-On Connectors</b> page to enable the connector.</p>
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p>
Service	<p>The type of Kinesis Service that you want to use. Select <b>Kinesis Firehose</b>.</p>
AWS Access Key ID	<p>The access key ID of the Amazon AWS user account.</p>
AWS Secret Access Key	<p>The secret access key for the Amazon AWS user account.</p>
Region	<p>Region where the endpoint for your service is available. You can select one of the following values:</p> <ul style="list-style-type: none"><li>- us-east-2. Indicates the US East (Ohio) region.</li><li>- us-east-1. Indicates the US East (N. Virginia) region.</li><li>- us-west-1. Indicates the US West (N. California) region.</li><li>- us-west-2. Indicates the US West (Oregon) region.</li><li>- ap-northeast-1. Indicates the Asia Pacific (Tokyo) region.</li><li>- ap-northeast-2. Indicates the Asia Pacific (Seoul) region.</li><li>- ap-northeast-3. Indicates the Asia Pacific (Osaka-Local) region.</li><li>- ap-south-1. Indicates the Asia Pacific (Mumbai) region.</li><li>- ap-southeast-1. Indicates the Asia Pacific (Singapore) region.</li><li>- ap-southeast-2. Indicates the Asia Pacific (Sydney) region.</li><li>- ca-central-1. Indicates the Canada (Central) region.</li><li>- cn-north-1. Indicates the China (Beijing) region.</li><li>- cn-northwest-1. Indicates the China (Ningxia) region.</li><li>- eu-central-1. Indicates the EU (Frankfurt) region.</li><li>- eu-west-1. Indicates the EU (Ireland) region.</li><li>- eu-west-2. Indicates the EU (London) region.</li><li>- eu-west-3. Indicates the EU (Paris) region.</li><li>- sa-east-1. Indicates the South America (São Paulo) region.</li><li>- us-gov-west-1. Indicates AWS GovCloud (US-West) region.</li><li>- us-gov-east-1. Indicates AWS GovCloud (US-East) region.</li></ul> <p>A streaming ingestion task does not support ap-northeast-3 region.</p>

Property	Description
Connection TimeOut (ms)	Optional. Number of milliseconds that the Mass Ingestion service waits to establish a connection to the Kinesis Firehose after which it times out. Default is 10,000 milliseconds.
AWS Credential Profile Name	An AWS credential profile defined in the credentials file. A mapping accesses the AWS credentials through the profile name at run time. If you do not provide an AWS credential profile name, the mapping uses the access key ID and secret access key that you specify when you create the connection.
ARN of IAM Role	The Amazon Resource Name specifying the role of an IAM user. Applies to Cross-Account IAM Roles authentication.
External ID	The external ID for an IAM role is an additional restriction that you can use in an IAM role trust policy to designate who can assume the IAM role. Applies to Cross-Account IAM Roles authentication.

## Amazon Kinesis Streams connection properties

When you set up an Amazon Kinesis Streams connection, you must configure the connection properties.

The following table describes the Amazon Kinesis Streams connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identity the connection. The description cannot exceed 4,000 characters.
Type	The Amazon Kinesis connection type. If you do not see the Amazon Kinesis connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service	The type of Kinesis Service that you want to use. Select <b>Kinesis Streams</b> .
AWS Access Key ID	The access key ID of the Amazon AWS user account.
AWS Secret Access Key	The secret access key for your Amazon AWS user account.

Property	Description
Region	<p>Region where the endpoint for your service is available. You can select one of the following values:</p> <ul style="list-style-type: none"> <li>- us-east-2. Indicates the US East (Ohio) region.</li> <li>- us-east-1. Indicates the US East (N. Virginia) region.</li> <li>- us-west-1. Indicates the US West (N. California) region.</li> <li>- us-west-2. Indicates the US West (Oregon) region.</li> <li>- ap-northeast-1. Indicates the Asia Pacific (Tokyo) region.</li> <li>- ap-northeast-2. Indicates the Asia Pacific (Seoul) region.</li> <li>- ap-northeast-3. Indicates the Asia Pacific (Osaka-Local) region.</li> <li>- ap-south-1. Indicates the Asia Pacific (Mumbai) region.</li> <li>- ap-southeast-1. Indicates the Asia Pacific (Singapore) region.</li> <li>- ap-southeast-2. Indicates the Asia Pacific (Sydney) region.</li> <li>- ca-central-1. Indicates the Canada (Central) region.</li> <li>- cn-north-1. Indicates the China (Beijing) region.</li> <li>- cn-northwest-1. Indicates the China (Ningxia) region.</li> <li>- eu-central-1. Indicates the EU (Frankfurt) region.</li> <li>- eu-west-1. Indicates the EU (Ireland) region.</li> <li>- eu-west-2. Indicates the EU (London) region.</li> <li>- eu-west-3. Indicates the EU (Paris) region.</li> <li>- sa-east-1. Indicates the South America (São Paulo) region.</li> <li>- us-gov-west-1. Indicates AWS GovCloud (US-West) region.</li> <li>- us-gov-east-1. Indicates AWS GovCloud (US-East) region.</li> </ul> <p>A streaming ingestion task does not support ap-northeast-3 region.</p>
Connection Timeout (ms)	<p>Optional. Number of milliseconds that the Mass Ingestion service waits to establish a connection to the Kinesis Streams after which it times out.</p> <p>Default is 10,000 milliseconds.</p>
AWS Credential Profile Name	<p>An AWS credential profile defined in the credentials file.</p> <p>A mapping accesses the AWS credentials through the profile name at run time. If you do not provide an AWS credential profile name, the mapping uses the access key ID and secret access key that you specify when you create the connection.</p>
ARN of IAM Role	<p>The Amazon Resource Name specifying the role of an IAM user. Applies to Cross-Account IAM Roles authentication.</p>
External ID	<p>The external ID for an IAM role is an additional restriction that you can use in an IAM role trust policy to designate who can assume the IAM role. Applies to Cross-Account IAM Roles authentication.</p>

## Amazon Redshift connection properties

When you set up an Amazon Redshift connection, you must configure the connection properties.

The following table describes the Amazon Redshift connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	User name of the Amazon Redshift account.

Connection property	Description
Password	Password for the Amazon Redshift account.
Schema	Amazon Redshift schema name. Default is public.
AWS Access Key ID	Optional. Amazon S3 bucket access key ID. To run tasks on Secure Agent installed on an EC2 system, you might leave the Access Key ID blank. To run tasks on Secure Agent that is not installed on an EC2 system, you must provide the Access Key ID.
AWS Secret Access Key	Optional. Amazon S3 bucket secret access key ID. To run tasks on Secure Agent installed on an EC2 system, you might leave the Secret Access Key blank. To run tasks on Secure Agent that is not installed on an EC2 system, you must provide the Secret Access Key.
Master Symmetric Key	Optional. Amazon S3 encryption key. Provide a 256-bit AES encryption key in the Base64 format.
Customer Master Key ID	Optional. Specify the customer master key ID or alias name generated by AWS Key Management Service (AWS KMS). You must generate the customer master key ID for the same region where Amazon S3 bucket reside. You can either specify the customer generated customer master key ID or the default customer master key ID.
JDBC URL	Amazon Redshift connection URL.
Number of bytes needed to support multibytes for varchar	Applicable to Create Target. Reads the Varchar precision of the source table and creates the target table with 1x/2x/3x/4x times of the source precision to successfully write multibyte characters in the target table. <b>Note:</b> You cannot create a target table if the Varchar precision exceeds 65535 that is maximum allowed.

**Note:** When you test a connection, Secure Agent validates Redshift connection. Validation of AWS Access key and AWS Secret key requires the Amazon S3 bucket name present in the advanced source and target properties. Therefore, Secure Agent validates AWS Access key and AWS Secret key when a synchronization or mapping task is run.

# Amazon Redshift V2 connection properties

When you set up an Amazon Redshift V2 connection, configure the connection properties.

The following table describes the Amazon Redshift V2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Amazon Redshift V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run an application ingestion task, database ingestion task, file ingestion task, or streaming ingestion task on a Hosted Agent or serverless runtime environment. <b>Note:</b> Hosted Agent is not applicable for mappings that run on an advanced cluster.
Authentication Type	The authentication method that the connector must use to log in to Amazon Redshift. Select one of the following authentication types: <ul style="list-style-type: none"><li>- Default. Uses the username and password to connect to Amazon Redshift.</li><li>- Redshift IAM Authentication via AssumeRole. Uses AssumeRole for IAM authentication to connect to Amazon Redshift.</li></ul>
Username	User name of the Amazon Redshift account.
Password	Password for the Amazon Redshift account. Applies only to default authentication.
Use EC2 Role to Assume Role	Optional. Select the check box to enable the EC2 role to assume another IAM role specified in the IAM Role ARN option. <b>Note:</b> The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different account. Does not apply to application ingestion and database ingestion tasks. By default, this check box is not selected.
S3 Access Key ID	Access key to access the Amazon S3 staging bucket. Enter the access key value based on the following authentication methods: <ul style="list-style-type: none"><li>- Basic authentication. Enter the actual access key value.</li><li>- IAM authentication. Do not enter the access key value.</li><li>- Temporary security credentials using assume role. Enter access key of an IAM user with no permissions to access the Amazon S3 staging bucket.</li><li>- Assume role for EC2. Do not enter the access key value.</li></ul> <b>Note:</b> If you use the connection for application ingestion or database ingestion tasks that use key-based authentication, provide the access key value.

Property	Description
S3 Secret Access Key	<p>Secret access key to access the Amazon S3 staging bucket.</p> <p>The secret key is associated with the access key and uniquely identifies the account.</p> <p>Enter the access key value based on the following authentication methods:</p> <ul style="list-style-type: none"> <li>- Basic authentication. Enter the actual access secret value.</li> <li>- IAM authentication. Do not enter the access secret value.</li> <li>- Temporary security credentials using assume role. Enter access secret of an IAM user with no permissions to access Amazon S3 staging bucket.</li> <li>- Assume role for EC2. Do not enter the access secret value.</li> </ul> <p><b>Note:</b> If you use the connection for application ingestion or database ingestion tasks that use key-based authentication, provide the access key value.</p>
S3 IAM Role ARN	<p>The Amazon Resource Number (ARN) of the IAM role assumed by the user to use the dynamically generated temporary security credentials.</p> <p>Set the value of this property if you want to use the temporary security credentials to access the Amazon S3 staging bucket.</p> <p>For more information about how to get the ARN of the IAM role, see the AWS documentation.</p> <p><b>Note:</b> If you use the connection for application ingestion or database ingestion tasks that uses role-based authentication, but not the default role for the AWS cluster, specify an IAM role ARN. If you use the default role, leave this field blank.</p>
External Id	<p>The external ID for a more secure access to the Amazon S3 bucket when the Amazon S3 staging bucket is in a different AWS account.</p> <p>Does not apply to application ingestion and database ingestion tasks.</p>
Master Symmetric Key <sup>1</sup>	<p>A 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a key using a third-party tool.</p> <p>Does not apply to application ingestion and database ingestion tasks.</p>
JDBC URL	<p>The URL of the Amazon Redshift V2 connection.</p> <p>Enter the JDBC URL in the following format:</p> <pre>jdbc:redshift://&lt;amazon_redshift_host&gt;:&lt;port_number&gt;/&lt;database_name&gt;</pre>

Property	Description
Cluster Region	<p>The AWS cluster region in which the bucket you want to access resides.</p> <p>Select a cluster region if you choose to provide a custom JDBC URL that does not contain a cluster region name in the <b>JDBC URL</b> connection property.</p> <p>If you select a cluster region in both <b>Cluster Region</b> and <b>JDBC URL</b> connection properties, the agent ignores the cluster region that you specify in the <b>JDBC URL</b> connection property.</p> <p>To use the cluster region name that you specify in the <b>JDBC URL</b> connection property, select <b>None</b> as the cluster region in this property.</p> <p>You can only read data from or write data to the cluster regions supported by AWS SDK.</p> <p>Select one of the following cluster regions:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud (US)</li> <li>- AWS GovCloud (US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is <b>None</b>.</p>
Customer Master Key ID	<p>The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access.</p> <p>You must generate the customer master key ID for the same region where your Amazon S3 staging bucket resides. You can either enter the customer-generated customer master key ID or the default customer master key ID.</p> <p>You can use a cross account KMS key for the same regions when you run mappings in advanced mode.</p> <p>Doesn't apply to application ingestion and database ingestion tasks.</p>
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## Amazon Redshift AssumeRole authentication

Configure the following properties when you select the Redshift AssumeRole authentication type:

Property	Description
Cluster Identifier	The unique identifier of the cluster that hosts Amazon Redshift for which you are requesting the security credentials. Specify the cluster name.
Database Name	Name of the Amazon Redshift database.
Database Group	Name of the database group to which an IAM user will be added. You can add multiple database groups separated by a comma. <b>Note:</b> If you do not specify a group, the user is added to the public group.
Expiration Time	The time duration that the password for the Amazon Redshift database user expires. Specify a value between 900 seconds and 3600 seconds. Default is 900.
Auto Create DBUser	Select to create a new Amazon Redshift database user at run time. Default is disabled.
Redshift IAM Role ARN	The Amazon Resource Number (ARN) of the IAM role assumed by the user or EC2 to use the dynamically generated temporary security credentials. Set the value of this property if you want to use the temporary security credentials to access Amazon Redshift. For more information about how to get the ARN of the IAM role, see the AWS documentation.
Redshift Access Key ID	The access key of the IAM user that has permissions to assume the Redshift IAM AssumeRole ARN.
Redshift Secret Access Key	The secret access key of the IAM user that has permissions to assume the Redshift IAM Assume Role ARN.

**Note:** In an Amazon Redshift V2 connection where you write to a target, and the target connection has **Auto Create DBUser** enabled, the new user cannot truncate a table created by an existing user.

# Amazon S3 connection properties

When you set up an Amazon S3 connection, you must configure the connection properties.

The following table describes the Amazon S3 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Access Key	The access key ID used to access the Amazon account resources. Required if you do not use AWS Identity and Access Management (IAM) authentication. <b>Note:</b> Ensure that you have valid AWS credentials before you create a connection.
Secret Key	The secret access key used to access the Amazon account resources. This value is associated with the access key and uniquely identifies the account. You must specify this value if you specify the access key ID. Required if you do not use AWS Identity and Access Management (IAM) authentication.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, <bucket name>/<my folder name>
Master Symmetric Key	Optional. Provide a 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a key using a third-party tool. If you specify a value, ensure that you specify the encryption type as client side encryption in the advanced target properties in the <b>Schedule</b> page.

Connection property	Description
Code Page	<p>The code page compatible with the Amazon S3 source. Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode and non-Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>
Region Name	<p>Specify the name of the region where the Amazon S3 bucket is available and for which you generated the customer master key ID. Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Asia Pacific (Tokyo)</li> <li>- Asia Pacific (Seoul)</li> <li>- Asia Pacific (Singapore)</li> <li>- Asia Pacific (Sydney)</li> <li>- AWS GovCloud</li> <li>- China (Beijing)</li> <li>- EU (Ireland)</li> <li>- EU (Frankfurt)</li> <li>- South America (Sao Paulo)</li> <li>- US East (N. Virginia)</li> <li>- US West (N. California)</li> <li>- US West (Oregon)</li> <li>- US East (Ohio)</li> <li>- Canada (Central)</li> <li>- Asia Pacific (Mumbai)</li> </ul> <p>You can only read from or write data to the regions supported by AWS SDK used by the Amazon S3 connector.</p>

## Amazon S3 V2 connection properties

When you set up an Amazon S3 V2 connection, configure the connection properties.

The following table describes the Amazon S3 V2 connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Amazon S3 V2 connection type.

Property	Description
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run an application ingestion task or a database ingestion task on a Hosted Agent or serverless runtime environment.</p>
Access Key	<p>Access key to access the Amazon S3 bucket.</p> <p>Enter the access key value based on the following authentication methods:</p> <ul style="list-style-type: none"> <li>- Basic authentication. Enter the actual access key value.</li> <li>- IAM authentication. Don't enter the access key value.</li> <li>- Temporary security credentials using assume role. Enter the secret access key of an IAM user with no permissions to access Amazon S3 bucket.</li> <li>- Assume role for EC2. Don't enter the access key value.</li> <li>- Credential profile file authentication<sup>1</sup>. Don't enter the access key value.</li> <li>- Federated user single sign-on<sup>1</sup>. Don't enter the secret access key value.</li> </ul>
Secret Key	<p>Secret access key to access the Amazon S3 bucket. The secret key is associated with the access key and uniquely identifies the account.</p> <p>Enter the secret access key value based on the following authentication methods:</p> <ul style="list-style-type: none"> <li>- Basic authentication. Enter the actual access secret value.</li> <li>- IAM authentication. Don't enter the access secret value.</li> <li>- Temporary security credentials using assume role. Enter access secret of an IAM user with no permissions to access Amazon S3 bucket.</li> <li>- Assume role for EC2. Don't enter the access key value.</li> <li>- Credential profile file authentication<sup>1</sup>. Don't enter the access secret value.</li> <li>- Federated user single sign-on<sup>1</sup>. Don't enter the access secret value.</li> </ul>
IAM Role ARN	<p>The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role assumed by the user to use the dynamically generated temporary security credentials.</p> <p>Enter the value of this property if you want to use the temporary security credentials to access the AWS resources.</p> <p>This property is not applicable to an application ingestion task.</p> <p><b>Note:</b> Even if you remove the IAM role that enables the agent to access the Amazon S3 bucket and create a connection, the test connection is successful.</p> <p>For more information about how to get the ARN of the IAM role, see the AWS documentation.</p>
External Id	<p>Provides a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account.</p>
Use EC2 Role to Assume Role	<p>Enables the EC2 role to assume another IAM role specified in the IAM Role ARN option.</p> <p><b>Note:</b> The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different account.</p> <p>By default, the Use EC2 Role to Assume Role check box is not selected.</p> <p><b>Note:</b> Enter a value for the IAM Role ARN property when you enable this property for a streaming ingestion task.</p>
Folder Path	<p>Bucket name or complete folder path to the Amazon S3 objects.</p> <p>Don't use a slash at the end of the folder path. For example, &lt;bucket name&gt;/&lt;my folder name&gt;.</p>

Property	Description
Master Symmetric Key	<p>A 256-bit AES encryption key in the Base64 format when you use client-side encryption. You can generate a key using a third-party tool.</p> <p>Not applicable for an application ingestion task, database ingestion task, or streaming ingestion task.</p>
Customer Master Key ID	<p>The customer master key ID or alias name generated by AWS Key Management Service (AWS KMS) or the Amazon Resource Name (ARN) of your custom key for cross-account access.</p> <p><b>Note:</b> Cross-account access is not available for mappings in advanced mode.</p> <p>You must generate the customer master key for the same region where the Amazon S3 bucket resides.</p> <p>You can specify the following master keys:</p> <ul style="list-style-type: none"> <li>- Customer generated customer master key. Enables client-side or server-side encryption.</li> <li>- Default customer master key. Enables client-side or server-side encryption. Only the administrator user of the account can use the default customer master key ID to enable client-side encryption.</li> </ul> <p>Not applicable for an application ingestion task, database ingestion task, or streaming ingestion task.</p>
S3 Account Type	<p>The type of the Amazon S3 account.</p> <p>Select from the following options:</p> <ul style="list-style-type: none"> <li>- Amazon S3 Storage. Enables you to use the Amazon S3 services.</li> <li>- S3 Compatible Storage. Enables you to use the endpoint for a third-party storage provider such as Scalify RING or MinIO.</li> </ul> <p>Default is Amazon S3 storage.</p>
REST Endpoint	<p>The S3 storage endpoint required for S3 compatible storage. Enter the S3 storage endpoint in HTTP or HTTPs format.</p> <p>For example, <a href="http://s3.isv.scality.com">http://s3.isv.scality.com</a>.</p>

Property	Description
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>
Federated SSO IdP <sup>1</sup>	<p>SAML 2.0-enabled identity provider for the federated user single sign-on to use with the AWS account.</p> <p>Amazon S3 V2 connector supports only the ADFS 3.0 identity provider. Select <b>None</b> if you don't want to use federated user single sign-on.</p> <p><b>Note:</b> Federated user single sign-on is not applicable to mappings in advanced mode.</p> <p><b>Note:</b> Federated user single sign-on is not applicable to application ingestion tasks, database ingestion tasks, and streaming ingestion tasks.</p>
Other Authentication Type <sup>1</sup>	<p>Select one the following authentication types:</p> <ul style="list-style-type: none"> <li>- NONE</li> <li>- Credential Profile File Authentication</li> </ul> <p>Select the Credential Profile File Authentication option to access the Amazon S3 credentials from a credential file that contains the access key and secret key.</p> <p>Enter the credential profile file path and the profile name to establish the connection with Amazon S3.</p> <p>You can use permanent IAM credentials or temporary session tokens when you configure the Credential Profile File Authentication.</p> <p>Default is NONE.</p>

Property	Description
Credential Profile File Path <sup>1</sup>	<p>Specifies the credential profile file path.</p> <p>If you don't enter the credential profile path, the Secure Agent uses the credential profile file present in the following default location in your home directory:</p> <pre>~/.aws/credentials</pre> <p><b>Note:</b> Mass Ingestion Databases has not been certified with the <b>Credential Profile File Path</b> and <b>Profile Name</b> connection properties. Mass Ingestion Databases finds AWS credentials by using the default credential provider chain that is implemented by the DefaultAWSCredentialsProviderChain class, which includes the credential profile file.</p>
Profile Name <sup>1</sup>	<p>Name of the profile in the credential profile file used to get the credentials.</p> <p>If you don't enter the profile name, the credentials from the default profile in the credential profile file are used.</p>
S3 VPC Endpoint Type <sup>1</sup>	<p>The VPC endpoint type for Amazon S3.</p> <p>You can enable private communication with Amazon S3 by selecting a VPC endpoint. Select one of the following VPC endpoint types:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- Gateway Endpoint</li> <li>- Interface Endpoint</li> </ul> <p>Default is None.</p> <p>This property is not applicable to an application ingestion task and database ingestion task.</p>
Endpoint DNS Name for Amazon S3 <sup>1</sup>	<p>The DNS name for the Amazon S3 interface endpoint.</p> <p>Enter the DNS name in the following format:</p> <pre>bucket.&lt;DNS name of the interface endpoint&gt;</pre> <p>This property is not applicable to an application ingestion task and database ingestion task.</p>
STS VPC Endpoint Type <sup>1</sup>	<p>Applicable when you select the S3 VPC interface endpoint.</p> <p>The VPC endpoint type for AWS STS.</p> <p>When you select <b>IAM Role ARN</b> or <b>Federated SSO IdP</b>, configure the STS VPC endpoint.</p> <p>This property is not applicable to an application ingestion task, streaming ingestion task, and database ingestion task.</p>
Endpoint DNS Name for AWS STS service <sup>1</sup>	<p>The DNS name for the AWS STS interface endpoint.</p> <p>This property is not applicable to an application ingestion task and database ingestion task.</p>
KMS VPC Endpoint Type <sup>1</sup>	<p>Applicable when you select the interface endpoint.</p> <p>The VPC endpoint type for the AWS KMS.</p> <p>When you select <b>Customer Master Key ID</b>, configure the KMS VPC endpoint.</p> <p>This property is not applicable to an application ingestion task and database ingestion task.</p>
Endpoint DNS Name for AWS KMS service <sup>1</sup>	<p>The DNS name for the AWS KMS interface endpoint.</p> <p>This property is not applicable to an application ingestion task and database ingestion task.</p>
<sup>1</sup> Applies only to mappings.	

## Federated user single sign-on connection properties

Configure the following properties when you select ADFS 3.0 in Federated SSO IdP:

Property	Description
Federated User Name	User name of the federated user to access the AWS account through the identity provider.
Federated User Password	Password for the federated user to access the AWS account through the identity provider.
IdP SSO URL	Single sign-on URL of the identity provider for AWS. Not applicable for a streaming ingestion task.
SAML Identity Provider ARN	ARN of the SAML identity provider that the AWS administrator created to register the identity provider as a trusted provider.
Role ARN	ARN of the IAM role assumed by the federated user.

## Anaplan V2 connection properties

When you set up an Anaplan V2 connection, you must configure the connection properties.

The following table describes the Anaplan V2 connection properties:

Connection property	Description
Connection Name	A name for the Anaplan V2 connection. This name must be unique within the organization.
Description	Description of the Anaplan V2 connection.
Type	Type of connection. Select Anaplan V2.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Auth Type	The type of authentication that the connector must use to log in to Anaplan. Select the authentication method that the connector must use to login to the Anaplan. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Auth. Requires Anaplan account username and password to connect to Anaplan.</li><li>- Cert Auth. Requires Certificate Authority (CA) to obtain an authentication token.</li><li>- OAuth Device Flow. Requires an OAuth 2.0 client credential to authenticate user data across apps.</li></ul> Default is Basic Auth.
Username	The user name to log in to Anaplan. For example, <code>firstname.lastname@anaplan.com</code> . <b>Note:</b> Do not leave this field blank. Even though you want to establish a connection using certificate based authentication, you need to enter a random value or string in this field.
Password	Password that is associated with the user name that is specified in the Username property.

Connection property	Description
Certificate Path Location	<p>Path to the Anaplan authentication certificate. Certificate Path Location is required only if you want to configure a connection with the certificate issued by Anaplan and you want to use API version 1.3.</p> <p>This implies that the Certification Path Location is required only if Auth type = Cert Auth, Major Version = 1, and Minor Version = 3 .</p>
Workspace ID	<p>The name or ID of the workspace.</p> <p>To fetch the ID, open the Anaplan model and copy the value after <code>selectedWorkspaceId=</code> from the URL.</p>
Model ID	<p>The name or ID of the model.</p> <p>To fetch the ID, open the Anaplan model and copy the value after <code>selectedModelId=</code> from the URL.</p>
API Base URL	Enter the API Base URL. For example, <code>https://api.anaplan.com</code>
Auth URL	<p>Specifies the URL for the authentication service required to generate the authentication token.</p> <p>For example, <code>https://us1a.app.anaplan.com</code></p>
API Major Version	<p>The Anaplan API version has two parts: Major Version and Minor Version.</p> <p>Example: For API version 1.3, the Major Version is 1 and the Minor Version is 3.</p> <p>By default, the API Major Version is set to 1.</p> <ul style="list-style-type: none"> <li>- To use certificate issued by Anaplan, select 1. API version 1.x supports certificate issued by Anaplan.</li> <li>- To use certificate issued by a certificate authority, select 2. API version 2.x supports certificate issued by a certificate authority.</li> </ul>
API Minor Version	<p>By default, the API Minor Version is set to 3.</p> <ul style="list-style-type: none"> <li>- Select 3 if you want to use API version x.3. For example, version 1.3</li> <li>- Select 0 if you want to use API version x.0. For example, version 2.0</li> </ul>
Max Task Retry Count	<p>By default, the Max Task Retry Count is set to 2.</p> <p>If you select a greater value, it may slow down the synchronization tasks.</p>
Error Dump Path Location	<p>The absolute path of the error file on the Secure Agent machine.</p> <p>The Secure Agent creates a sub-folder in the Error Dump Path Location for each process operation.</p>
Use API Based Metadata	You can import API based metadata from Anaplan and use API based field mapping instead of File based field mapping in a synchronization task. When you import API based metadata, Anaplan V2 Connector reads the column header information from Anaplan APIs directly without referring to files in Anaplan.
KeyStore Path Location	<p>Path to the JAVA KeyStore file on the system with the Secure Agent.</p> <p><b>Note:</b> The KeyStore Path Location, KeyStore Alias, and Keystore Password is required only if you want to configure a connection with the certificate issued by a certificate authority and you want to use API version 2.0.</p>
KeyStore Alias	Alias of the certificate saved in the KeyStore file.
Keystore Password	Password for the certificate alias in the KeyStore file.

Connection property	Description
ClientId	Required for OAuth Device Flow. The client identifier issued to the client during the application registration process.
Token	Required for OAuth Device Flow. The refresh token is used to get new access tokens. You can select one of the following options: <ul style="list-style-type: none"> <li>- Rotatable. Uses the refresh token once during the lifespan.</li> <li>- Non-rotatable. Uses the refresh token several times. The non-rotatable token does not expire.</li> </ul>

## Ariba V2 connection properties

When you set up an Ariba V2 connection, you must configure the connection properties.

You can create an ITK or SOAP connection. When you create an ITK connection, Ariba allows authentication using shared secret or SSL certificate.

The following table describes the Ariba V2 connection properties:

Connection Property	Description
Connection Name	Name of Ariba V2 Connector.
Description	Description of Ariba V2 Connector.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Connection Type	Type of Connection. You can select SOAP or ITK.
Service URL	URL for the Ariba service.
Realm/Site	Realm of the Ariba instance.
Data Dictionary File Location	Location of the data dictionary file on your local machine.
Use SSL Certificate	Applicable for ITK connection. Determines whether the Secure Agent establishes a secure connection to Ariba. When you select this option, the Secure Agent establishes an encrypted connection. SSL authentication requires Client Keystore, Client Keystore Password, and Client Key Password.
Shared Secret	Shared Secret for the ITK connection. Leave the Shared Secret blank if you authenticate using SSL certificate on Ariba Network.
Client Keystore	The location of the client keystore file.
Client Keystore Password	The password for the client keystore file required for secure communication.
Client Key Password	The password for the client key.

Connection Property	Description
User Name	Required for a SOAP connection. User name for the Ariba account.
Password	Required for a SOAP connection. Password for the Ariba account.

## AS2 connection properties

Configure connection properties for an AS2 server.

Configure the following properties on the **Connection** page in Administrator:

- AS2 connection properties, which define the connection and enable access to the AS2 server.
- Message properties, which specify access to private and public keys and message encryption preferences. The message properties also define how to pass messages to the organization such as whether to compress messages and whether to send or receive message receipts.
- Receipt properties, which specify whether to request MDN receipts, certificate and transfer encoding properties, and method of receiving MDN receipts.
- Proxy properties, which specify whether to use a proxy server and the proxy server details.

## Connection properties

The following table describes AS2 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
URL	URL of the server that receives the messages. The URL syntax must refer to a valid server and location. The host name can be an IP address or a domain name. The port number is the port on which the AS2 server listens.
AS2 From ID	Name or ID of the sender. If the receiving server filters by this ID, the IDs must match. Value is case sensitive and can contain 1 to 128 ASCII printable characters in length. The value cannot contain white spaces.
AS2 To ID	Name or ID of the recipient. Value is case sensitive and can contain 1 to 128 ASCII printable characters in length. The value cannot contain white spaces.
Username	User name to connect to the remote AS2 server.
Password	Password to connect to the remote AS2 server.

Connection property	Description
Connection Timeout	Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection does not occur in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 60 seconds.
Read Timeout	Maximum number of seconds to wait when attempting to read a file from the server. A timeout occurs if the file is not read in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 0 seconds.
Connection Retry Attempts	Number of times to retry connecting to the AS2 server if a successful connection does not occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections. If the value is blank, no retries are attempted. Default is blank.
Connection Retry Interval	Number of seconds to wait between each connection retry attempt. For example, to retry to connect up to 10 times with a five second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5. If the value is blank, the interval is 0 seconds. Default is blank.
Follow Redirects	Whether or not to follow redirect links when creating a connection. Default is false.
User Agent	Value used in the message header to indicate what application created or sent the message.
Use Chunked Encoding	Whether or not to pre-calculate the length of the request or send the request in chunks. Pre-calculating the content length might slow performance when sending large files. However, not all AS2 servers support chunked encoding. Default is false.
Client Certificate Alias	Alias of the key within the default keystore to use for client authentication when required by the receiving AS2 server.
SSL Context Protocol	Protocol to use when creating the SSLContext. The protocol that you specify depends on the security providers installed in the Java Runtime Environment (JRE). <b>Note:</b> In most cases, the default value of SSL is appropriate. However, for some IBM JRE implementations, the default value of SSL will not work if the server you are connecting to does not support SSLv3. Default is SSL.

Enter the actual information in this section (optional).

### Connection properties

## Message properties

The following table describes AS2 connection message properties:

Connection property	Description
Trust Store Location	Path to the truststore that stores the public key certificates. Must be on the Secure Agent machine or on a server accessible to the Secure Agent.
Trust Store Password	Password to access the truststore.
Encrypt Messages	Whether or not to encrypt messages during transmission. Encrypting the message within the encrypted tunnel is optional, but highly recommended. Default is false.
Encryption Algorithm	Algorithm to use to encrypt messages. Choose one of the following algorithms: <ul style="list-style-type: none"><li>- AES128</li><li>- AES256</li><li>- CAST5</li><li>- IDEA</li><li>- TRIPLE-DES</li><li>- RC2</li></ul> Default is AES128.
Encryption Certificate Alias	Certificate alias to use in the default trusted certificate keystore to encrypt the outgoing message.
Sign Messages	Whether or not to sign the message with a digital signature. Signing messages is optional, but highly recommended. Default is false.
Private Keystore Location	Location of the keystore that stores private keys and associated certificates. Applicable when signing messages is enabled.
Private Keystore Password	Password to access the keystore. Applicable when signing messages is enabled.
Signature Algorithm	Algorithm to use to sign messages. Applicable when signing messages is enabled. Choose one of the following algorithms: <ul style="list-style-type: none"><li>- SHA1</li><li>- SHA224</li><li>- SHA256</li><li>- SHA384</li><li>- SHA512</li><li>- MD5</li></ul> Default is SHA1.
Signature Certificate Alias	Private key alias to use to sign the message. The private key is located in the default private keystore.
Compress Messages	Whether or not to compress messages to reduce bandwidth. If you enable this option, Informatica Intelligent Cloud Services compresses messages using the zlib format. Default is false.

## Receipt properties

The following table describes AS2 connection receipt properties:

Connection property	Description
Receipt Certificate Alias	<p>Alias for the receipt certificate. Applicable when you configure the connection to require a signed receipt.</p> <p>AS2 Connector uses the receipt certificate to verify that the certificate that signed the receipt is a certificate in the default trusted certificate keystore.</p> <p>Optional if the receipt signature contains an embedded certificate. If the receipt signature does not contain an embedded certificate, you must specify the receipt certificate alias.</p>
Receipt Transfer Encoding	<p>Type of encoding to use for message receipts. This is useful when the receipt does not include the transfer encoding.</p> <p>Use one of the following values:</p> <ul style="list-style-type: none"><li>- base64</li><li>- quoted-printable</li><li>- 7bit</li><li>- 8bit</li><li>- binary</li></ul>
Request Receipt	<p>Whether or not to request a MDN receipt when the server receives the message. Select one of the following options:</p> <ul style="list-style-type: none"><li>- None. Do not require a receipt.</li><li>- Signed. Require a receipt signed with a digital signature.</li><li>- Unsigned. Require a receipt without a digital signature.</li></ul> <p>Default is none.</p>
Destination	<p>Mode with which to receive the MDN. Applicable when you request a receipt.</p> <p>Select one of the following values:</p> <ul style="list-style-type: none"><li>- Joblog. Receive MDN in the job log, accessible in Monitor.</li><li>- File. Receive MDN in a file.</li><li>- Email. Receive MDN in an email.</li><li>- URL. Receive MDN through an URL.</li><li>- Discard. Discard MDN.</li></ul> <p>Default is joblog.</p>
File	<p>Path including the file name to store the MDN. Applicable for a file destination.</p>
When File Exists	<p>Determines how to resolve name conflict when a receipt file already exists. Applicable for a file destination.</p> <p>Select one of the following values:</p> <ul style="list-style-type: none"><li>- Rename. Rename the new receipt file by adding a sequential number. For example, fileMdn 2.txt, fileMdn 3.txt</li><li>- Append. Append receipt to the existing file.</li><li>- Overwrite. Overwrite contents of the existing receipt file.</li><li>- Skip. Do not upload the receipt.</li><li>- Error. Duplicate file name causes error.</li></ul> <p>Default is rename.</p>
Email Address	<p>Email address to send the receipts. Applicable for an email destination.</p>
Receipt URL	<p>URL to post the receipts. Applicable for an URL destination.</p>

## Proxy properties

The following table describes AS2 connection proxy properties:

Connection property	Description
Enabled	Determines if a proxy server is enabled for the connector. Default is disabled.
Proxy Type	Type of proxy server to use for the connection. Select one of the following types: <ul style="list-style-type: none"><li>- SOCKS. You can use SOCKS version 4 or 5.</li><li>- HTTPS.</li><li>- Informatica File Server proxy.</li></ul> Verify with your network administrator which proxy server type to use.
Host	Host name or IP address of the proxy server on your network.
Alternate Host	Host name or IP address of an alternate proxy server on your network. The alternate proxy server is used when the primary proxy server is unavailable.
Port	Port number of the proxy server on your network. If left blank, the default port for HTTP is 80 and the default port for SOCKS is 1080.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server. Required if your network uses the proxy server to create HTTP or HTTPS connections.

## Birst Cloud Connect connection properties

When you set up a Birst Cloud Connect connection, you must configure the connection properties.

The following table describes the Birst Cloud Connect connection properties:

Connection property	Description
Connection Name	Name of Birst Cloud Connect Connector.
Description	Description of Birst Cloud Connect Connector.
Type	Select Birst Cloud Connect connection.
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	User name for Birst Cloud Connect application.
Password	Password for Birst Cloud Connect application.
Endpoint URL	Birst Web Services end-point URL.

Connection property	Description
Space ID	UDID of Birst Space in which you want to upload data.
Enable Debug Logger	Select to enable debug logging.
Configuration Location	Temporary storage for internal configuration.

## Business 360 connection properties

When you create the Business 360 connection, you must configure the connection properties.

The following table describes the Business 360 connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+= {[}] \\:;'"'<,> . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360</b> .
Runtime Environment	The name of the runtime environment where you want to run the mappings. Specify a Secure Agent, Hosted Agent, or a serverless runtime environment.
Runtime Parameter	A system-generated job instance ID to process the ingress and export jobs. <b>Note:</b> Ensure that you do not modify this attribute.

# Business 360 Events connection properties

When you create the Business 360 Events connection, you must configure the connection properties.

The following table describes the Business 360 Events connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360 Events</b> .
Runtime Environment	The name of the runtime environment where you want to run the mappings. Specify a Secure Agent, Hosted Agent, or a serverless runtime environment.
Start Timestamp	A system-generated timestamp variable to set the start of a time range for which you want to get events from the Business 360 data store. <b>Note:</b> You can't modify this attribute.
End Timestamp	A system-generated timestamp variable to set the end of a time range for which you want to get events from the Business 360 data store. <b>Note:</b> You can't modify this attribute.

# Business 360 FEP Connection Properties

When you create the Business 360 FEP connection, you must configure the connection properties.

The following table describes the Business 360 FEP connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360 FEP Connector</b> .

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the mappings. Specify a Secure Agent, Hosted Agent, or a serverless runtime environment.
Runtime Parameter	A system-generated job instance ID to process the ingress jobs. <b>Note:</b> Ensure that you do not modify this attribute.

## CallidusCloud Commissions connection properties

When you create a CallidusCloud Commissions connection, you must configure the connection properties.

The following table describes the CallidusCloud Commissions connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
UserName	User name for the CallidusCloud portal login.
Password	Password of the CallidusCloud portal login.
BaseURL	The base URL to connect to the CallidusCloud application. Use the following sample to specify the base URL: <code>https://&lt;domainName&gt;/TrueComp-SaaS/services/rest/</code>
PageSize	The page size for the read operation. Default value is 10.

### Guidelines for a CallidusCloud Commissions connection

You can set the values for the session timeout properties as per your requirement through the JVM options for the Secure Agent.

You can configure the following properties:

- Session timeout: The time in seconds after which the session with the CallidusCloud Commissions endpoint times out.
- Attempts: The number of attempts to reconnect to the CallidusCloud Commissions endpoint.
- Wait time to re-attempt: The time in seconds between 2 attempts.

You must set the values for the properties higher than the default values, else the default values are considered.

The default values are:

```
-Dconnection.sessionTimeout=50
```

```
-Dconnection.attempts=3
```

```
-Dconnection.waitTimeToReattempt=5
```

Perform the following steps to configure the JVM options:

1. In Administrator, select the Secure Agent listed on the **Runtime Environments** tab.
2. Click **Edit**.
3. In the **System Configuration Details** section, select **Data Integration Server** as the service and **DTM** as the type.
4. Specify the values for the JVM options.

Custom Configuration Details

Service	Type	Sub-type	Name	Value	
Data Integration Server ▼	DTM ▼	▼	JVMOption6	-Dconnection.sessionTimeout=60	⊕ ✖
Data Integration Server ▼	DTM ▼	▼	JVMOption7	-Dconnection.attempts=4	⊕ ✖
Data Integration Server ▼	DTM ▼	▼	JVMOption8	-Dconnection.waitTimeToReattempt=5	⊕ ✖

5. Click **Save**.

## CallidusCloud File Processor connection properties

When you create a CallidusCloud File Processor connection, you must configure the connection properties.

The following table describes the CallidusCloud File Processor connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
UserName	The user name to use for connecting to the SFTP server.
Password	The password to use for connecting to the SFTP server.
SFTP Key	The private key to use for connecting to the SFTP server. You must specify the SFTP key in a single line.
SFTP Key Pass Phrase	The pass phrase to connect to the SFTP server. You must specify the SFTP Key Pass Phrase in a single line
Host	The host name of the SFTP server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 22.
Remote Directory	The directory on the SFTP host accessible to the Secure Agent. <b>Note:</b> Add / at the end of the specified path.

Property	Description
Charset	<p>Specify the character set to use for encoding data.</p> <p>CallidusCloud File Processor Connector supports the following character sets:</p> <ul style="list-style-type: none"> <li>- Big5</li> <li>- Big5-HKSCS</li> <li>- CESU-8</li> <li>- EUC-JP</li> <li>- EUC-KR</li> <li>- GB18030</li> <li>- GB2312</li> <li>- GBK</li> <li>- IBM00858</li> <li>- IBM01140</li> <li>- IBM01141</li> <li>- IBM01142</li> <li>- IBM01143</li> <li>- IBM01144</li> <li>- IBM01145</li> <li>- UTF-8</li> </ul> <p>The default value is UTF-8, which works well for all character data.</p>
Delimiter	<p>Delimiter used in the file to separate columns of data.</p> <p>Select the delimiter. The default delimiter is Comma.</p>
Compression Mode	<p>The compression format for binary files. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- gzip</li> </ul> <p>Default is None.</p>
Encryption Mode	<p>The type of encryption that the SFTP server uses to encrypt the data. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- GPG</li> </ul> <p>Default is None.</p>
Encryption Public Key	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the public key in a single line to encrypt data.</p>
Encryption Private Key	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the private key in a single line to decrypt data.</p>
Encryption Pass Phrase	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the pass phrase in a single line to encrypt data.</p>

For more information about converting multiline key file or pass phrase to single line key string, see the CallidusCloud File Processor documentation.

## Chatter connection properties

To use the Chatter Connector in a synchronization task, you must create a connection in Data Integration and configure the connection properties.

The following table describes the Chatter connection properties:

Connection property	Description
Connection Name	Name of the connection.
Type	Type of connection. Select <b>Chatter</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
User Name	User name of the Chatter account.
Password	Password of the Chatter account.
Security Token	The security token generated from Salesforce.
Service URL	The service endpoint URL with the API version. The Chatter Connector supports up to API version 34.0. For example: <a href="https://login.salesforce.com/services/Soap/u/34.0">https://login.salesforce.com/services/Soap/u/34.0</a>
Attachment Path	The path where the attachments of the feeds need to be copied.

## Concur V2 connection properties

When you set up a Concur V2 connection, you can specify a hybrid OAuth 2 or OAuth 2 connection to authenticate users and authorize access to Concur data. Informatica recommends that you use the OAuth 2 connection type.

The following table describes the Concur V2 connection properties for a hybrid OAuth 2 connection type:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication	The Secure Agent uses OAuth 2 to authenticate users and authorize access to Concur data.
User name	The user name to log in to the Concur web page.
Password	The password associated with the user name.

Connection property	Description
Consumer Key	The key that is generated when a Concur administrator registers a partner application for your organization. <b>Note:</b> Informatica intends to drop consumer key authentication support in a future release. Informatica requests you to transition to use OAuth authentication before the consumer key authentication is dropped.
Folder	The relative path to the objects that you want to access from Concur. For example, if the URL for API invocation is <a href="https://us-impl.api.concursolutions.com">https://us-impl.api.concursolutions.com</a> and the absolute path to invoke the API to retrieve the expense reports from Concur is <a href="https://us-impl.api.concursolutions.com/api/expense/report">https://us-impl.api.concursolutions.com/api/expense/report</a> , enter the following relative path: <i>/expense/report</i>

The following table describes the connection properties for the OAuth 2 connection type:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication	The Secure Agent uses OAuth 2 to authenticate users and authorize access to Concur data.
Username	The user name to log in to the Concur web page.
Password	The password associated with the user name.
Use OAuth 2	The Secure Agent uses OAuth 2 to authenticate users and authorize access to Concur data. Contact SAP Concur to get the new OAuth 2 credentials. If you do not specify to use OAuth 2, hybrid OAuth 2 connection type is used.
Base URL for authentication	The URL for authentication that you received from Concur when you created your account. The base URL for authentication is derived from the authorization URL. For example, if the authorization URL is <a href="https://us-impl.api.concursolutions.com/oauth2/v0/token">https://us-impl.api.concursolutions.com/oauth2/v0/token</a> , the base URL for authentication is <a href="https://us-impl.api.concursolutions.com">https://us-impl.api.concursolutions.com</a> .
Base URL for API Invocation	The URL for API invocation that you received from Concur when you created your account.
Client ID	The unique ID of your application to complete the OAuth Authentication in the Active Directory.
Secret ID	The password of your application to complete the OAuth Authentication in the Active Directory.
Folder	The relative path to the objects that you want to access from Concur. For example, if the URL for API invocation is <a href="https://us-impl.api.concursolutions.com">https://us-impl.api.concursolutions.com</a> and the absolute path to invoke the API to retrieve the expense reports from Concur is <a href="https://us-impl.api.concursolutions.com/api/expense/report">https://us-impl.api.concursolutions.com/api/expense/report</a> , enter the following relative path: <i>/expense/report</i>

# Cassandra V2 connection properties

When you create a Cassandra V2 connection, you must configure the connection properties.

The following table describes the Cassandra V2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Cassandra V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Cassandra server.
Port	Port number of the Cassandra server. Default is <b>9042</b> .
Datacenter	Name of the Cassandra Datacenter to connect to. Default is <b>datacenter1</b> .
Keyspace	Name of the Cassandra Keyspace within the Cassandra Datacenter to connect to.
Username	User name to access the Cassandra server.
Password	Password to access the Cassandra server.
SSL Enabled	Choose from the following options: - Yes. Enable the SSL encryption. - No. Disable the SSL encryption. Default is <b>No</b> .
SSL KeyStore File Path	Applicable if you enable SSL. Absolute path of the SSL KeyStore file in the Secure Agent machine that contains private keys and certificates for the SSL server.
SSL KeyStore Password	Applicable if you enable SSL. Password for the SSL KeyStore.
SSL TrustStore File Path	Applicable if you enable SSL. Absolute path of the SSL TrustStore file in the Secure Agent machine that contains private keys and certificates for the SSL server.
SSL TrustStore Password	Applicable if you enable SSL. Password for the SSL TrustStore.

# Couchbase connection properties

When you create a Couchbase connection, you must configure the connection properties.

The following table describes the Couchbase connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ ; , ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Couchbase</b> .
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Host Name	Host name or IP address of the Couchbase server.
Port	Couchbase server port number. Default is 9042.
Username	User name to access the Couchbase server.
Password	Password corresponding to the user name to access the Couchbase server.
SSL Mode	Not applicable for Couchbase Connector. Select <b>disabled</b> .
SSL Certificate Path	Not applicable for Couchbase Connector.
Additional Connection Properties	Enter one or more JDBC connection parameters in the following format: <param1>=<value>;<param2>=<value>;<param3>=<value> Couchbase Connector supports the following connection parameters: <b>QueryMode</b> It is used to send queries to Couchbase Server. <b>LogLevel</b> Species whether the Secure Agent logs error messages in the session log. <b>LogPath</b> The complete path to the folder where the driver saves log files when logging is enabled. <b>AuthMech</b> The authentication mechanism that the driver uses to connect to the Couchbase server.

# Coupa V2 connection properties

When you create a Coupa V2 connection, you must configure the connection properties.

The following table describes the Coupa V2 connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication	Select <b>Coupa V2</b> .
Base Url	Base URL to connect to Coupa API. Specify the base URL in the following format: <code>https://{instance_name}.coupahost.com/</code> For example, <code>https://companyname.coupahost.com/</code>
Authentication Type	Type of authentication for the Coupa V2 connection. You can select the API Key authentication or OAuth 2.0 authentication. <b>Note:</b> Informatica recommends you to use OAuth 2.0 authentication to connect to Coupa.
COUPA API KEY	Required for API key authentication. A unique API key to connect to the Coupa instance. For more information about creating an Coupa API key, see the <a href="#">Coupa documentation</a> .
Client ID	Required for OAuth 2.0 authentication. The Coupa client ID required to generate a valid access token. Specify the Coupa identifier as the client ID.
Client Secret	Required for OAuth 2.0 authentication. The Coupa client secret required to generate a valid access token. Specify the Coupa secret as the client secret.

Property	Description
Scope	<p>Required for OAuth 2.0 authentication.</p> <p>The scope used to authorize access to Coupa.</p> <p>Enter the scope defined for the user in Coupa. To enter multiple scopes, separate each scope with a space.</p>
Custom Field Config	<p>Specify custom fields for Coupa objects.</p> <p>Specify the custom fields in Coupa using the following format, where <b>FieldName</b> is value of the custom field name in Coupa, <b>FieldType</b> is the type of custom field, and <b>IsAPIGlobalNamespace</b> determines whether a custom field appears under root tag or custom-field tag in the <b>Field Mapping</b> tab:</p> <pre>Object1=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName3,FieldType,DataType,IsAPIGlobalNamespace Object2=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType, IsAPIGlobalNamespace Object3=FieldName1,FieldType,DataType,IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType,IsAPIGlobalNamespace;\ FieldName3,FieldType,DataType,IsAPIGlobalNamespace</pre> <p><b>Coupa V2 Connector supports only simple custom fields.</b></p> <p><b>For example:</b></p> <pre>user-summary=custom_field1,Simple,String,true;\ custom_field2,Simple,String, false requisition-header=requisition_cf1,Simple,String,true;\ requisition_cf2,Simple,Integer,false;\ requisition_cf3,Simple,Integer user=user_customfield1,Simple,String,false;\ user_customfield_2,Simple,String,true</pre> <p><b>Note:</b> The Secure agent replaces underscore in the custom field name with hyphen and displays the custom field name in the <b>Field Mapping</b> tab.</p>

## Cvent connection properties

When you set up a Cvent connection, configure the connection properties.

The following table describes the Cvent connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Cvent connection type.

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment for a mapping.
Account Number	Specify the account number.
User Name	User name of the Cvent API.
Password	Password for the Cvent API.
Endpoint Url	The endpoint URL of the Cvent application.
Batch Size	Number of records to be retrieved at a time. Maximum is 200.
UTC Time Zone	Cvent UTC time zone. Enter the timezone in the date and time fields. The time zone is appended to the filter values for the date and time fields.
Enable Logging	Enables logging for the task. When you enable logging, you can view the session log for the log details.

## Databricks Delta connection properties

When you set up a Databricks Delta connection, configure the connection properties.

You can configure the connection properties for both SQL warehouse and Databricks clusters.

The following table describes the Databricks Delta connection properties that are required to connect to Databricks Delta:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Databricks Delta connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode. You cannot run an application ingestion, database ingestion, or streaming ingestion task on a Hosted Agent or serverless runtime environment.

Property	Description
Databricks Token	<p>Required for SQL warehouse and Databricks clusters.</p> <p>Personal access token to access Databricks.</p> <p>Ensure that you have permissions to attach to the cluster identified in the <b>Cluster ID</b> property.</p> <p>For mappings, you must have additional permissions to create Databricks clusters.</p>
SQL Warehouse JDBC URL	<p>Required for SQL warehouse.</p> <p>Databricks SQL Warehouse JDBC connection URL.</p> <p>To get the SQL Warehouse JDBC URL, go to the Databricks console and select the JDBC driver version <b>2.6.22 or earlier</b> from the JDBC URL menu.</p> <p>Use the following syntax:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/&lt;SQL endpoint cluster ID&gt;;</pre> <p>The JDBC URL versions <b>2.6.25 or later</b> that begin with the prefix <code>jdbc:databricks://</code> are not applicable to Data Integration tasks and mappings.</p> <p>Application ingestion and database ingestion tasks can use JDBC URL version <b>2.6.25 or later</b> or <b>2.6.22 or earlier</b>. The URLs must begin with the prefix <code>jdbc:databricks://</code>, as follows:</p> <pre>jdbc:databricks://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/&lt;SQL endpoint cluster ID&gt;;</pre> <p>This field is required to connect to the Databricks SQL warehouse.</p> <p>Ensure that you set the required environment variables in the Secure Agent.</p> <p><b>Note:</b> The Databricks Host, Organization ID, and Cluster ID properties are not considered if you configure the SQL warehouse JDBC URL property.</p>
Cluster Environment	<p>Required for SQL warehouse and Databricks clusters.</p> <p>The cloud provider where the Databricks cluster is deployed.</p> <p>Choose from the following options:</p> <ul style="list-style-type: none"> <li>- AWS</li> <li>- Azure</li> </ul> <p>Default is AWS.</p> <p>You cannot switch between clusters once you establish a connection. Databricks Delta does not support multi-level dependent connection attributes across clusters.</p> <p>Cluster properties are required in the following scenarios:</p> <ul style="list-style-type: none"> <li>- When you create and run mappings to write data to Databricks Delta.</li> <li>- When you create and run mappings in advanced mode to read from and write to Databricks Delta.</li> </ul> <p>The connection attributes depend on the cluster environment you select. For more information, see the AWS cluster properties and Azure cluster properties sections.</p>
Databricks Host	<p>Required for Databricks cluster. The host name of the endpoint the Databricks account belongs to.</p> <p>Use the following syntax:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/&lt;Org Id&gt;/&lt;Cluster ID&gt;;AuthMech=3;UID=token;PWD=&lt;personal-access-token&gt;</pre> <p><b>Note:</b> You can get the URL from the Advanced Options of JDBC or ODBC in the Databricks Delta analytics cluster or all purpose cluster.</p> <p>The value of PWD in Databricks Host, Organization Id, and Cluster ID is always <code>&lt;personal-access-token&gt;</code>.</p>

Property	Description
Cluster ID	<p>Required for Databricks cluster.</p> <p>The ID of the Databricks analytics cluster.</p> <p>You can get the cluster ID from the JDBC URL.</p> <p>Use the following syntax:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/ default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/&lt;Org Id&gt;/ &lt;Cluster ID&gt;;AuthMech=3;UID=token;PWD=&lt;personal-access-token&gt;</pre>
Organization ID	<p>Required for Databricks cluster.</p> <p>The unique organization ID for the workspace in Databricks.</p> <p>Use the following syntax:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/ default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/&lt;Organization Id&gt;/&lt;Cluster ID&gt;;AuthMech=3;UID=token;PWD=&lt;personal-access-token&gt;</pre>
Database	<p>Optional for SQL warehouse and Databricks clusters.</p> <p>The database name that you want to connect to in Databricks Delta.</p> <p>Specify a database name or specify <code>default</code> to enable the default database name.</p> <p>For Data Integration, by default, all databases available in the workspace are listed.</p>
JDBC Driver Class Name	<p>Optional for SQL warehouse and Databricks clusters.</p> <p>The name of the JDBC driver class.</p> <p>Optional. If you do not specify the driver class, the following class name is used as default: <code>com.simba.spark.jdbc.Driver</code></p> <p>For application ingestion and database ingestion tasks, specify the driver class name as: <code>com.databricks.client.jdbc.Driver</code></p>
Min Workers <sup>1</sup>	<p>Required for Databricks cluster.</p> <p>The minimum number of worker nodes to be used for the Spark job. Minimum value is 1.</p>
Max Workers <sup>1</sup>	<p>Optional for Databricks cluster. The maximum number of worker nodes to be used for the Spark job. If you don't want to autoscale, set Max Workers = Min Workers or don't set Max Workers.</p>
DB Runtime Version <sup>1</sup>	<p>Required for Databricks cluster.</p> <p>The Databricks runtime version.</p> <p>Determines the version of Databricks cluster to spawn when you connect to Databricks cluster to process mappings.</p> <p>Select the runtime version 9.1 LTS.</p>
Worker Node Type <sup>1</sup>	<p>Optional for Databricks cluster. The worker node instance type that is used to run the Spark job.</p> <p>For example, the worker node type for AWS can be <code>i3.2xlarge</code>. The worker node type for Azure can be <code>Standard_DS3_v2</code>.</p>
Driver Node Type <sup>1</sup>	<p>Optional for Databricks cluster. The driver node instance type that is used to collect data from the Spark workers.</p> <p>For example, the driver node type for AWS can be <code>i3.2xlarge</code>. The driver node type for Azure can be <code>Standard_DS3_v2</code>.</p> <p>If you don't specify the driver node type, Databricks uses the value you specify in the worker node type field.</p>

Property	Description
Instance Pool ID <sup>1</sup>	Optional for Databricks cluster. The instance pool ID used for the Spark cluster. If you specify the Instance Pool ID to run mappings, the following connection properties are ignored: <ul style="list-style-type: none"> <li>- Driver Node Type</li> <li>- EBS Volume Count</li> <li>- EBS Volume Type</li> <li>- EBS Volume Size</li> <li>- Enable Elastic Disk</li> <li>- Worker Node Type</li> <li>- Zone ID</li> </ul>
Enable Elastic Disk <sup>1</sup>	Optional for Databricks cluster. Enables the cluster to get additional disk space. Enable this option if the Spark workers are running low on disk space.
Spark Configuration <sup>1</sup>	Optional for Databricks cluster. The Spark configuration to use in the Databricks cluster. The configuration must be in the following format: "key1"="value1";"key2"="value2";... For example: "spark.executor.userClassPathFirst"="False" Doesn't apply to a data loader task or to Mass Ingestion tasks.
Spark Environment Variables <sup>1</sup>	Optional for Databricks cluster. The environment variables to export before launching the Spark driver and workers. The variables must be in the following format: "key1"="value1";"key2"="value2";... For example: "MY_ENVIRONMENT_VARIABLE"="true" Doesn't apply to a data loader task or to Mass Ingestion tasks.
<sup>1</sup> Doesn't apply to mappings in advanced mode and when you use SQL warehouse to connect to Databricks Delta.	

## AWS cluster properties

When you set up a Databricks Delta connection, configure the connection properties based on the cluster environment you select.

The following table describes the Databricks Delta connection properties that apply when you select the AWS cluster environment:

Property	Description
S3 Access Key	The key to access the Amazon S3 bucket.
S3 Secret Key	The secret key to access the Amazon S3 bucket.
S3 Data Bucket	The existing bucket to store the Databricks Delta data.
S3 Staging Bucket <sup>1</sup>	The existing bucket to store staging files.

Property	Description
S3 Authentication Mode	The authentication mode to access Amazon S3. You can select one of the following authentication types: <ul style="list-style-type: none"> <li>- Permanent IAM credentials. Uses the S3 access key and S3 secret key to connect to Databricks Delta.</li> <li>- IAM Assume Role<sup>1</sup>. Uses the AssumeRole for IAM authentication to connect to Databricks Delta.</li> </ul>
IAM Role ARN <sup>1</sup>	The Amazon Resource Number (ARN) of the IAM role assumed by the user to use the dynamically generated temporary security credentials. Set the value of this property if you want to use the temporary security credentials to access the Amazon S3 staging bucket. For more information about how to get the ARN of the IAM role, see the AWS documentation.
Use EC2 Role to Assume Role <sup>1</sup>	Optional. Select the check box to enable the EC2 role to assume another IAM role specified in the IAM Role ARN option. The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different AWS account.
S3 Region Name <sup>1</sup>	The AWS cluster region in which the bucket you want to access resides. Select a cluster region if you choose to provide a custom JDBC URL that does not contain a cluster region name in the JDBC URL connection property.
S3 Service Regional Endpoint	The S3 regional endpoint when the S3 data bucket and the S3 staging bucket need to be accessed through a region-specific S3 regional endpoint. Default is <code>s3.amazonaws.com</code> .
Zone ID <sup>1</sup>	The zone ID for the Databricks job cluster. Applies only if you want to create a Databricks job cluster in a particular zone at runtime. For example, <code>us-west-2a</code> . <b>Note:</b> The zone must be in the same region where your Databricks account resides.
EBS Volume Type <sup>1</sup>	The type of EBS volumes launched with the cluster.
EBS Volume Count <sup>1</sup>	The number of EBS volumes launched for each instance. You can choose up to 10 volumes. <b>Note:</b> In a Databricks Delta connection, specify at least one EBS volume for node types with no instance store. Otherwise, cluster creation fails.
EBS Volume Size <sup>1</sup>	The size of a single EBS volume in GiB launched for an instance.
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## Azure cluster properties

When you set up a Databricks Delta connection, configure the connection properties based on the cluster environment that you select.

The following table describes the Databricks Delta connection properties that apply when you select the Azure cluster environment:

**Note:** These properties are required when you run mappings to write data to Databricks Delta and when you run mappings in advanced mode to read from and write to Databricks Delta.

Property	Description
ADLS Storage Account Name	The name of the Microsoft Azure Data Lake Storage account.
ADLS Client ID	The ID of your application to complete the OAuth Authentication in the Active Directory.
ADLS Client Secret	The client secret key to complete the OAuth Authentication in the Active Directory.
ADLS Tenant ID	The ID of the Microsoft Azure Data Lake Storage directory that you use to write data.
ADLS Endpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and client secret is completed.
ADLS Data Filesystem Name	The name of an existing file system to store the Databricks Delta data.
ADLS Staging Filesystem Name <sup>1</sup>	The name of an existing file system to store the staging data.
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## Datacom CDC Connection Properties

When you configure an Datacom CDC connection, you must set the connection properties.

The following table describes Datacom CDC connection properties:

Property	Description
Connection Name	A name for the Datacom CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Datacom CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Datacom CDC, the type must be <b>Datacom CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Datacom change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>ADACDC1A:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Datacom instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Datacom source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>

Property	Description
Map Location	<p>Host name or IP address of the system where the extraction maps reside. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>ADACDC01:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Datacom table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXP) Datacom CDC connections in PowerCenter.</p>

## Datacom Connection Properties

When you configure a Datacom connection, you must set the connection properties.

The following table describes Datacom connection properties:

Property	Description
Connection Name	<p>A name for the Datacom connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the Datacom connection. Maximum length is 4000 characters.

Property	Description
Type	Type of connection. For Datacom, the type must be <b>Datacom</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for Datacom runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name: port_number</i></p> <p>For example:</p> <p>LSNR1:1467?</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.

Property	Description
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Datacom connections in PowerCenter.
Write Mode	Write Mode. Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

## Db2 Data Map connection properties

When you configure a Db2 Data Map connection, you must set the connection properties.

The following table describes the Db2 Data Map connection properties:

Property	Description
Connection Name	A name for the Db2 Data Map connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Optional description for the Db2 Data Map connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 data maps, the type must be <b>Db2 Data Map</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 Data Map runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.

Property	Description
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the filtering of data and bulk data processing to the target.</li> <li>- <b>Filter Before</b>. Filters data on the source system and offloads bulk data processing to the target.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the Secure Agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>The size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds after the initial connection attempt fails that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener. If a connection cannot be established within the retry period, the mapping task fails. The default value is 0, which disables connection retries.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) connections in PowerCenter.</p>

# Db2 for i CDC connection properties

When you configure a Db2 for i CDC connection, you must set the connection properties.

The following table describes Db2 for i CDC connection properties:

Property	Description
Connection Name	<p>A name for the Db2 for i CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code></p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the Db2 for i CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for i CDC, the type must be <b>Db2 for i CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2CDC1A:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Db2 for i instance name that is specified in the <b>Instance</b> field for the registration group that contains the capture registrations for the Db2 source tables. This instance name is also specified in the INST parameter in the AS4J CAPI_CONNECTION statement in the DBMOVER member. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.

Property	Description
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>. Default is Rows.</p>
Map Location	<p>Host name or IP address of the system where the extraction maps reside. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2CDC01:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	<p>A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.</p>
Map Location Password	<p>Password associated with the user name that is specified in <b>Map Location User</b> property.</p>
Event Table	<p>If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 for i table on the CDC source system.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 CDC application connections in PowerCenter.</p>

# Db2 for i connection properties

When you configure a Db2 for i connection, you must set the connection properties.

The following table describes Db2 for i connection properties:

Property	Description
Connection Name	<p>A name for the Db2 for i connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the Db2 for i connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for i, the type must be <b>Db2 for i</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for i runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2ILSNR:14675</p>
Database Name	The Db2 for i subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the Db2 for i source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Isolation Level	<p>The Db2 for i isolation level to use for the source database. Options are:</p> <ul style="list-style-type: none"><li>- ALL</li><li>- CS</li><li>- CHG</li><li>- None</li><li>- RR</li></ul> <p>Default is CS</p>
Database File Overrides:	<p>A value to override the database file default.</p> <p>This value overrides the value in the DB_FILE statement in the PowerExchange DBMOVER configuration file.</p>
Library List:	The name of the Db2 for i Library List to use for the connection.

Property	Description
Environment SQL	SQL commands that run in the database environment.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 for i connections in PowerCenter.
Write Properties	Write Mode. Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> <li>- <b>Asynchronous with Fault Tolerance.</b> Combines the speed of <b>Confirm Write Off</b> with the error detection of <b>Confirm Write On</b>. This mode buffers the data and sends it asynchronously to the PowerExchange Listener. When an SQL error occurs, PowerExchange creates a reject file on the target machine, which contains the data records that the writer could not write to the target. View the file contents to identify and correct the errors without reloading the entire table. You can also specify how to handle specific SQL return codes.</li> </ul> Default is <b>Confirm Write On</b> .
Reject File	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the Write Mode is Asynchronous with Fault Tolerance. <b>Note:</b> Enter PWXDISABLE to prevent creation of the reject files.

# Db2 for i Database Ingestion connection properties

When you define a Db2 for i Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion tasks, which you configure in the Mass Ingestion service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is Db2 for i Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for i instance.
Password	The password to use for connecting to the Db2 for i instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Location Name	The name of the Db2 for i location that you want to access. Your system administrator can determine the name of the Db2 location by using the WRKRDBDIRE command. In the output, find the name of the database that is listed as *LOCAL and then use that value as the value of this property.
JDBC Driver	The type of JDBC driver. Select one of the following options: - Data Direct - JTOpen Default is Data Direct.
Code Page for Bit Data	The code page that Mass Ingestion Databases uses to read character data that is stored as bit data. This value must be a canonical name for the java.io API and java.lang API. For more information, see the supported encodings in the Oracle Java documentation. Specify this property if you have FOR BIT DATA source columns.

Property	Description
Advanced Connection Properties	<p>Advanced properties for the JDBC driver which is used to connect to the Db2 for i source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;).</p> <p>For information about the DataDirect JDBC driver connection properties, see <a href="#">Progress DataDirect documentation</a>. For example, you can set the ConnectionRetryCount property to control the number of times the driver retries attempts to connect to the primary database server.</p> <p>For information about the JTOpen JDBC driver connection properties, see <a href="#">IBM Toolbox for Java JDBC properties</a>.</p>
Encryption Method	<p>The data encryption method for the JTOpen JDBC Driver.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Encryption</li> <li>- SSL</li> </ul> <p>Default is No Encryption.</p> <p>If you select SSL, you must add the required certificates to the Informatica Cloud Secure Agent JRE cacerts keystore in one of the following locations:</p> <p>For Linux:</p> <pre>Secure Agent Directory\jdk\jre\lib\security\cacerts</pre> <p>For Windows:</p> <pre>Secure Agent Directory\apps\jdkLatestVersion\jre</pre>

## Db2 for LUW CDC connection properties

When you configure a Db2 for LUW CDC connection, you must set the connection properties.

The following table describes Db2 for LUW CDC connection properties:

Property	Description
Connection Name	<p>A name for the Db2 for LUW CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name.</p> <p>Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the Db2 for LUW CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for LUW CDC, the type must be <b>Db2 for LUW CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for LUW run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2RHL1:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	Db2 instance name that is specified in the <b>Database</b> field of the registration group that contains capture registrations for the Db2 source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>

Property	Description
Map Location	<p>Enter the host name or IP address of the system that contains the extraction maps. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2UNIX2B:25100</p> <p>The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 CDC connections in PowerCenter.</p>

# Db2 for LUW Database Ingestion connection properties

When you define a Db2 for LUW Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion tasks, which you configure in the Mass Ingestion service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is Db2 for LUW Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for LUW instance.
Password	The password to use for connecting to the Db2 for LUW instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Database Name	The name of the Db2 for LUW database that you want to access.
Advanced Connection Properties	<p>Advanced properties for the Progress DataDirect JDBC DB2 driver, which is used to connect to the Db2 for LUW source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;).</p> <p>The driver properties that you can enter in this field are described in the Progress DataDirect <a href="#">connection properties</a>. For example, you can set the EncryptionMethod property to control whether data is encrypted and decrypted when transmitted over the network between the driver and database server.</p>

# Db2 for z/OS Bulk Load connection properties

When you configure a Db2 for z/OS Bulk Load connection, you must set the connection properties.

The following table describes Db2 for z/OS Bulk Load connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Bulk Load connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Bulk Load connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Bulk Load, the type must be <b>Db2 for z/OS Bulk Load</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Bulk Load runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: LSNR1:1467?
Database Name	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Environment SQL	SQL commands that run in the database environment.
Correlation ID	A value to use as the Db2 Correlation ID for Db2 requests. This value overrides the value in the SESSID statement in the PowerExchange DBMOVER configuration file.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.

Property	Description
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Write Mode	Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXP) Db2 for z/OS Bulk Load connections in PowerCenter.

## Db2 for z/OS CDC connection properties

When you configure a Db2 for z/OS CDC connection, you must set the connection properties.

The following table describes Db2 for z/OS CDC connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS CDC, the type must be <b>Db2 for zOS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <p style="text-align: center;"><i>host_name:port_number</i></p> For example: DB2CDC1A:1467

Property	Description
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Db2 for z/OS subsystem ID or data-sharing group name that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Db2 source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <div style="text-align: center;"><i>host_name:port_number</i></div> For example: DB2CDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.

Property	Description
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 for z/OS table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 CDC connections in PowerCenter.

## Db2 for z/OS connection properties

When you configure a Db2 for z/OS connection, you must set the connection properties.

The following table describes Db2 for z/OS connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS, the type must be <b>Db2 for z/OS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: LSNR1:1467?

Property	Description
DB2 Subsystem ID	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Environment SQL	SQL commands that run in the database environment.
Correlation ID	A value to use as the Db2 Correlation ID for Db2 requests. This value overrides the value in the SESSID statement in the PowerExchange DBMOVER configuration file.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> Default is No.
Offload Threads	The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning. Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 for z/OS connections in PowerCenter.

Property	Description
Asynchronous With Fault Tolerance	Combines the speed of <b>Confirm Write Off</b> with the error detection of <b>Confirm Write On</b> . This mode buffers the data and sends it asynchronously to the PowerExchange Listener. When an SQL error occurs, PowerExchange creates a reject file on the target machine, which contains the rows that the writer could not write to the target. View the file contents to identify and correct the errors without reloading the entire table. You can also specify how to handle specific SQL return codes. To stop session execution when the session encounters non-fatal errors, specify a value greater than 0 in the <b>Stop on errors</b> session attribute on the <b>Config Object</b> tab of the Edit Tasks dialog box. Default is <b>Confirm Write On</b> .
Write Properties	Write Mode. Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On</b>. Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off</b>. Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>
Reject File	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the Write Mode is Asynchronous with Fault Tolerance. <b>Note:</b> Enter PWXDISABLE to prevent creation of the reject files.

## Db2 for z/OS Image Copy connection properties

When you configure a Db2 for z/OS Image Copy connection, you must set the connection properties.

The following table describes Db2 for z/OS Image Copy connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Image Copy connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Image Copy connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Image Copy, the type must be <b>Db2 for z/OS Image Copy</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Image Copy runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: LSNR1:1467?</p>
DB2 Subsystem ID	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.

Property	Description
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPCL) Db2 for z/OS Image Copy connections in PowerCenter.

## Db2 for z/OS Unload File connection properties

When you configure a Db2 for z/OS Unload File connection, you must set the connection properties.

The following table describes the Db2 for z/OS Unload File connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Unload File connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Unload File connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Unload Files, the type must be <b>Db2 for z/OS Unload File</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Unload File runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.

Property	Description
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before.</b> Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For VSAM data sets and Db2 for z/OS Unload Files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 for z/OS Unload File connections in PowerCenter.</p>

# Db2 for zOS Database Ingestion connection properties

When you define a Db2 for zOS Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion tasks, which you configure in the Mass Ingestion service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is Db2 for zOS Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for zOS instance.
Password	The password to use for connecting to the Db2 for zOS instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Location Name	The name of the Db2 for zOS location that you want to access. For DB2 for z/OS, your system administrator can determine the name of your DB2 location using the command DISPLAY DDF.
Code Page for Bit Data	The code page that Mass Ingestion Databases uses to read character data that is stored as bit data. This value must be a canonical name for the java.io API and java.lang API. For more information, see the supported encodings in the Oracle Java documentation. Specify this property if you have FOR BIT DATA source columns.
CDC Stored Procedure Schema	For incremental change data capture processing, the name of the schema for the z/OS stored procedure that is required to collect change data from the Db2 log. This value is specified in the #STPINST data set that you customized when setting up the stored procedure on z/OS. No default value is provided.
CDC Stored Procedure Name	For incremental change data capture processing, the name of the z/OS stored procedure that is required to collect change data from the Db2 log. This value is specified in the #STPINST data set that you customized when setting up the stored procedure on z/OS. The default value is INFALOG.
Advanced Connection Properties	Advanced properties for the Progress DataDirect JDBC DB2 driver, which is used to connect to the Db2 for z/OS source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;). The driver properties that you can enter in this field are described in the Progress DataDirect documentation at <a href="https://docs.progress.com/bundle/datadirect-connect-jdbc-51/page/Connection-Properties_10.html">https://docs.progress.com/bundle/datadirect-connect-jdbc-51/page/Connection-Properties_10.html</a> . For example, you can set the ConnectionRetryCount property to control the number of times the driver retries attempts to connect to the primary database server.

# DB2 Loader connection properties

When you set up a DB2 Loader connection, configure the connection properties.

The following table describes the DB2 Loader connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Select db2loader from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select the Secure Agent from the list as the runtime environment.
Host Name	Name of the machine that hosts the DB2 database server.
Database	The DB2 database name.
Port	The port number that connects to the DB2 database server. Default is 50000.
Schema	Not applicable.
User Name	User name for the DB2 database login.
Password	Password for the DB2 database login.
Connection String	Alias name to connect to the DB2 database.
Operation Mode	Operation mode of the DB2 external loader. Select one of the following operation modes based on the mode that you selected in the DB2 external loader: <ul style="list-style-type: none"><li>- Insert. Adds data to the table.</li><li>- Replace. Deletes all existing data from the table and then adds data to the table.</li><li>- Restart. Restarts a previously interrupted load operation.</li><li>- Terminate. Terminates a previously interrupted load operation and rolls back the operation to the starting point, even if consistency points are passed.</li></ul> Default is Insert.
Is Staged	Method to load data. Select <b>Is Staged</b> to load data to a flat file staging area before loading to the DB2 database. Default is disabled.

Property	Description
Recoverable	Sets the DB2 tablespace in backup pending state. Before you enable the <b>Recoverable</b> option and run a mapping, you need to fully back up the database to perform any other operation on the tablespace. Default is enabled.
DB2 Server Location	Location of the DB2 database server relative to the Secure Agent machine. Select one of the following locations from the list: - Remote. The DB2 database server resides on another machine. - Local. The DB2 database server resides on the Secure Agent machine. Default is Remote.
External Loader Executable	File name of the DB2 external loader executable file of the IBM data server client 9.5 version and later. Default is db2load.

## Db2 Warehouse on Cloud connection properties

When you set up a Db2 Warehouse on Cloud connection, you must configure the connection properties.

The following table describes the Db2 Warehouse on Cloud connection properties:

Connection property	Description
Connection name	The name of the connection.
Description	Description of the Db2 Warehouse on Cloud connection. Maximum length is 255 characters.
Type	Type of connection. Select <b>Db2 Warehouse on Cloud</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
User ID	User ID to log into IBM Db2 Warehouse on Cloud.
Password	Password for the user ID to connect to IBM Db2 Warehouse on Cloud.
Host name	Host name of IBM Db2 Warehouse on Cloud.
Port number	Network port number used to connect to the IBM Db2 Warehouse server.
Database name	Database name of IBM Db2 Warehouse that you want to connect to.

Connection property	Description
SSL connection	Determines whether the Secure Agent establishes a secure connection with IBM Db2 Warehouse. Select SSL to establish a secure connection to IBM Db2 Warehouse. <b>Note:</b> When you use a serverless runtime environment, you cannot configure a Db2 Warehouse connection to use SSL to securely communicate with the Db2 Warehouse database.
Advanced connection properties	Optional. Additional connection parameters that you want to use. Specify the connection parameters as key-value pairs in the following format, and separate each key-value pair with a semicolon: <param1>=<value>&<param2>=<value>&<param3>=<value>...
Schema	The schema name in IBM Db2 Warehouse on Cloud from where you want to fetch the metadata. <b>Note:</b> The Secure Agent browses all schemas in IBM Db2 Warehouse on Cloud if you do not specify a schema name.

## Domo connection properties

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

The following table describes the Domo connection properties:

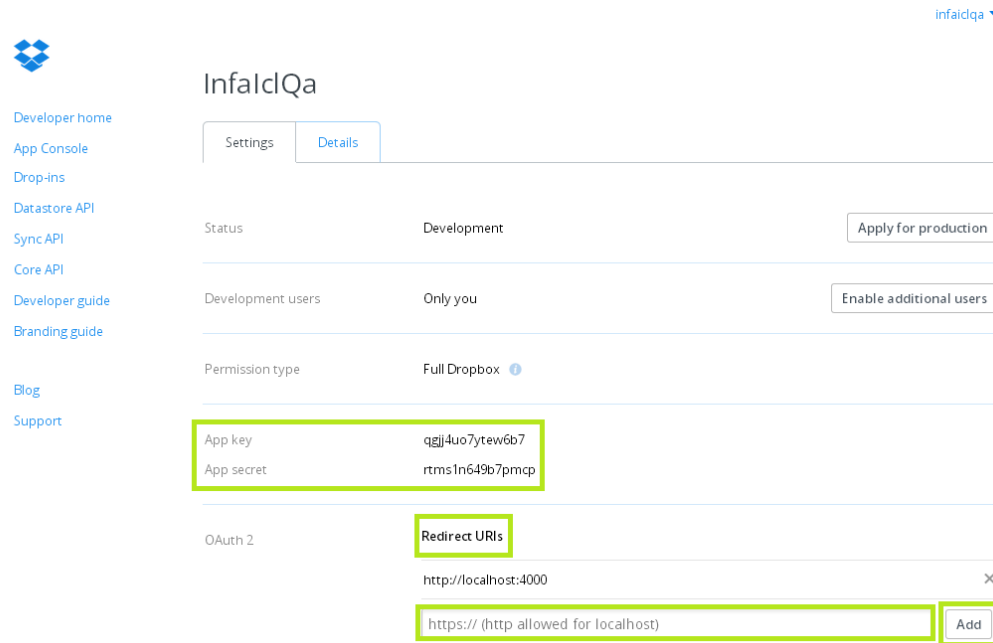
Connection property	Description
Connection Name	Name of the Domo connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Domo connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Customer	User name to connect to the Domo account.
Dev Token	Access token to connect to the Domo account.
UpdateMode	You can select one of the following options to update data: <ul style="list-style-type: none"> <li>- APPEND</li> <li>- REPLACE</li> <li>- UPSERT</li> </ul>
Upsert Keys	Applicable for UPSERT mode. Enter unique values and separate each value with a comma.

# Dropbox connection properties

The following table lists the connection properties for a Dropbox Connection:

Connection property	Description
Connection Name	Name for the connection.
Description	Description for the connection.
Type	Type of connection. Select Dropbox from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
App Key	Dropbox account name. Enter the App Key obtained from the <b>Dropbox App Console</b> .
App Secret	Dropbox account password. Enter the App Secret obtained from the <b>Dropbox App Console</b> .
Agent Hosted on this system	Specify if the system hosts the agent or not.
Authorization code	<ul style="list-style-type: none"><li>- Not applicable, when the system hosts the Secure Agent.</li><li>- When system does not host the Secure Agent, you need to enter the authorization code to get the access token. After specifying the Target folder in connection parameters, test the connection. When you test the connection, an URL link appears in the connection page which specifies the Authorization code.</li></ul>
Access Token	Access token obtained after testing the connection.
Target Folder	Location of target directory to save the files that Dropbox downloads. For example, <code>\\...\Dropbox\Target\</code>
Enable Logging	Logs the user, who creates the connection. Select the checkbox to enable logging.

**Note:** While creating a connection, mention the redirect URI `http://localhost:4000` in the Dropbox App settings page.



The screenshot shows the 'InfalclQa' application settings page. The 'Details' tab is selected. The 'App key' is 'qgij4uo7ytew6b7' and the 'App secret' is 'rtms1n649b7pmcp'. The 'OAuth 2' section is expanded, showing 'Redirect URIs'. The first URI is 'http://localhost:4000'. A second URI, 'https:// (http allowed for localhost)', is being added, highlighted with a green box, next to an 'Add' button.

## Elasticsearch connection properties

When you create an Elasticsearch connection, you must configure the connection properties.

The following table describes the Elasticsearch connection properties:

Property	Description
Connection Name	The 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: <code>_ . + -</code> . Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Elasticsearch connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Elasticsearch server.

Property	Description
Port	Elasticsearch server port number. Default is 9243.
Authentication	Authentication method to access the Elasticsearch resources. Basic authentication uses user name and password credentials to connect to the Elasticsearch server.
User Name	User name to access the Elasticsearch server.
Password	Password corresponding to the user name to access the Elasticsearch server.

## Eloqua Bulk API connection properties

When you create an Eloqua Bulk API connection, configure the connection properties.

The following table describes the Eloqua Bulk API connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Eloqua Bulk API connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Base URL	The base URL to connect to the Eloqua application. Use one of the following format to specify the base URL: - https://secure.eloqua.com - https://<host>.eloqua.com/api/bulk/<version number> For the host, you can enter secure, www02.secure, or secure.p03 based on the pod that hosts the Eloqua instance. In https://<host>.eloqua.com/api/bulk/2.0 URL, 2.0 represents the version number. When you do not mention the version number in the base URL, the Secure Agent considers the default version. To determine the base URL to connect to the Eloqua application, see <a href="#">Determining Base URL</a> .
Authentication Type	The type of user authentication to connect to the Eloqua application.
Domain Name	The company name of your Eloqua application.
User name	The user name of your Eloqua account.

Property	Description
Password	The password for your Eloqua account.
Client ID	The client ID to complete the OAuth 2.0 authentication to connect to Eloqua. Applies if you select the OAuth 2.0 authentication type.
Client Secret	The client secret key to complete the OAuth 2.0 authentication to connect to Eloqua. Applies if you select the OAuth 2.0 authentication type.
Time Zone Offset	The time zone in the Eloqua application relative to GMT.
Enable Debug Logger	Enables the debug logger to register the SOAP request and response in the session log.
Fetch Data for Preview	Fetches the first 10 rows of the first five columns in an Eloqua Bulk API object for preview. Default is selected.
Activities or Custom Fields Configuration	The Activities object and custom fields of Contact and Account objects in sources and targets. Enter the Activities object and custom fields in JSON format.

## Eloqua REST connection properties

When you create an Eloqua REST connection, you must configure the connection properties.

The following table describes the Eloqua REST connection properties:

Property	Description
Runtime Environment	Runtime environment that contains Secure Agent used to access Eloqua.
Base Url	Endpoint URL of the Eloqua application server. Do not specify the query parameters with the Base URL. For example, <a href="https://rest.apisandbox.eloqua.com">https://rest.apisandbox.eloqua.com</a>
Username	User name of the Eloqua application.
Domain	Domain of the Eloqua application.
Password	Password for the Eloqua application.
Client ID	The client ID created in the Eloqua application. You must enter the client ID if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Client Secret	The client secret key created in the Eloqua application. You must enter the client secret key if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .

Property	Description
Authentication Type	The type of user authentication to connect to the Eloqua application. Select the authentication type that Eloqua REST Connector must use to login to the Eloqua application. You can select the following authentication types: <ul style="list-style-type: none"> <li>- Basic Auth</li> <li>- OAuth 2.0</li> </ul> Default is OAuth 2.0.
Enable Debug Logger	Displays the message in the session logs to debug the mapping. Default is false.
Eloqua Swagger	The swagger file that you want to use for the Eloqua REST connection. Select <b>Eloqua Swagger API V1_2017_09_06</b> .

## FHIR connection properties

When you configure a Fast Healthcare Interoperability Resources (FHIR) connection, you must configure the connection properties.

The following table describes the FHIR connection properties:

Property	Description
Connection Name	A name for the FHIR connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -  Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the FHIR connection. Maximum length is 4000 characters.
Type	Type of connection. For FHIR connection, the type must be <b>FHIR</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Host	Host name or IP address of the FHIR server. It also includes the port number. Enter the value in the following format, where host_name can be a host name or IP address: <code>host_name:port_number</code>
HTTP Method	Select one of the following HTTP methods: <ul style="list-style-type: none"> <li>- HTTP</li> <li>- HTTPS</li> </ul> Default is HTTP.
Connection Timeout	Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection does not occur in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 30 seconds.

Property	Description
Keep Alive	Specify whether or not to keep the connection open for multiple HTTP requests or responses. Default is true.
Follow Redirects	Whether or not to follow redirect links when creating a connection. Default is true.
Connection Retry Attempts	Number of times to retry connecting to the FHIR server if a successful connection does not occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections. Default is 0. Specify 0 to disable the retry attempts.
Connection Retry Interval	Number of seconds to wait between each connection retry attempt. For example, to retry to connect up to 10 times with a five second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5. Default is 0.
Base Path	The base path for the FHIR server. The initial URL segment of the api.
Content Type	The media type of the request. Select one of the following options: <ul style="list-style-type: none"> <li>- application/fhir+xml</li> <li>- application/fhir+json</li> <li>- application/xml</li> <li>- application/json</li> </ul>
Accept	The media type of the response. Select one of the following options: <ul style="list-style-type: none"> <li>- application/fhir+xml</li> <li>- application/fhir+json</li> <li>- application/xml</li> <li>- application/json</li> </ul>
Authentication Type	The authentication method that the connector must use to connect to the REST endpoint. You can use one of the following options: <ul style="list-style-type: none"> <li>- None</li> <li>- Basic</li> <li>- OAuth 2.0 authorization code. For more information, see <a href="#">"OAuth 2.0 authorization code authentication" on page 102</a>.</li> <li>- OAuth 2.0 client credentials. For more information, see <a href="#">"OAuth 2.0 client credentials authentication" on page 103</a>.</li> </ul> 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 Basic authentication.
Trust Store 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.
Trust Store Password	The password for the truststore file that contains the SSL certificate.

Property	Description
Key Store 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.
Key Store Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: <ul style="list-style-type: none"> <li>- No Proxy. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Platform Proxy. Considers proxy configured at the agent level.</li> <li>- Custom Proxy. Considers proxy configured at the connection level.</li> </ul> Proxy is not applicable when you a serverless runtime environment.
Proxy Config	Host name or IP address of the proxy server. It also includes the port number. Enter the value in the following format, where host_name can be a host name or IP address: <code>host_name:port_number</code>

## OAuth 2.0 authorization code authentication

Configure authentication properties in the FHIR connection to use an OAuth 2.0 authorization code.

To use authorization code authentication, 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 you receive error code 400, 401, or 403 in the response, the Informatica redirect URL tries to connect to the endpoint and retrieve a new access token. Note that the Informatica redirect URL is usually outside the organization firewall.

The following table describes the authentication properties for a FHIR connection that uses an OAuth 2.0 authorization code:

Property	Description
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	Specifies access control if the API endpoint defines custom scopes. Separate scope attributes using a space. For example: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>

Property	Description
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in JSON format. For example: [{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]
Client Authentication	Select an option to send the client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .
Access Token	Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To generate the access token through a proxy server, configure an unauthenticated proxy server on the Secure Agent. The FHIR connection-level proxy configuration doesn't apply when generating the access token.
Refresh Token	Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent generates a new access token through the refresh token. If the refresh token expires, you must either enter a valid refresh token or generate a new refresh token by clicking <b>Generate Access Token</b> .

## OAuth 2.0 client credentials authentication

Configure authentication properties in the FHIR connection to use OAuth 2.0 client credentials.

The following table describes the authentication properties for a FHIR connection that uses OAuth 2.0 client credentials:

Property	Description
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	Specifies access control if the API endpoint defines custom scopes. Separate scope attributes using a space. For example: root_readonly root_readwrite manage_app_users
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in JSON format. For example: [{"Name": "resource", "Value": "https://<serverName>"}]
Client Authentication	Select an option to send the client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .
Access Token	Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To generate the access token through a proxy server, configure an unauthenticated proxy server on the Secure Agent. The FHIR connection-level proxy configuration doesn't apply when generating the access token.

# FileIO connection properties

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

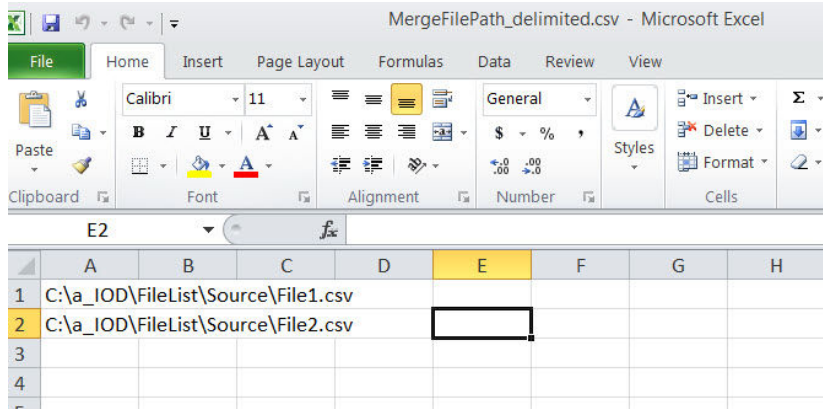
The following table describes the FileIO connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select <b>Fileio</b> from the list.
Secure Agent	Select the appropriate secure agent from the list.
Parent Directory	Enter the parent directory path. The parent directory is the folder that contains the files to perform read and write operations. The parent directory must contain an <code>.infaccess</code> empty file. Create a folder within the parent directory with any name other than <code>inprocess</code> , <code>success</code> , and <code>error</code> . For example, you can create a <code>read</code> , <code>write</code> , or <code>test</code> folder. The empty file will be listed as objects when you select this connection as source or target in the task.
Process File Content As	Select the required option from the list of available options to process the file content. The following file processing options are available: <ul style="list-style-type: none"><li>- Binary: When you select Binary, you must map <code>FileContentAsBinary</code> in the <b>Field Mapping</b> tab of the synchronization task.</li><li>- base64 encoded string: By default this option is selected. When you select this option, you must map <code>FileContentAsBase64String</code> in the <b>Field Mapping</b> tab of the synchronization task.</li></ul>
Overwrite Target Files	Check the box to enable overwrite target files. Otherwise the file containing same names will be created in the incrementing naming order using a counter. For example, when you do not enable overwrite target file option, the existing file ABCD will not be overwritten. Instead a new file ABCD(1) will be created.
Auto Archive Source Files	Check the box to enable automatic archiving of source files. This option allows you to move the files from source directory after the file is processed.
In Process Directory	Mention the directory path to be used for file processing. By default, parent directory is considered.
Success Directory	Mention the directory path where the files will be moved after processing. By default, parent directory is considered. Mention the success directory path only when <b>Auto Archive Source Files</b> option is enabled.
Error Directory	Mention the error directory path. When there are issues/errors in file processing. Such files are moved to error directory.

# File List connection properties

When you set up a File List connection, you must configure the connection properties.

The following table describes the File List connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a description for the connection.
Type	Select File List from the list.
Secure Agent	Select the Secure Agent from the list.
File Type	Select the file format from the list. The connection supports fixed-width and delimiter file types.
Delimiter	Select the delimiter. The default delimiter is Comma.
Schema File Path	Specify the schema file path. A sample schema file is present in Informatica Secure Agent folder. The path is <Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<plugin ID>
Custom Header File Path	Specify the header file path. You can find header.hdr file in Informatica Secure Agent folder. The path is <Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<plugin ID>
Skip First N lines	Specify the number of rows you want to skip while merging the files. This helps you to skip the rows from the beginning of the file.
Skip Last N lines	Specify the number of rows you want to skip while merging the files. This helps you to skip the rows from the end of the file.
Merge File Path	<p>It is the file which contains details of all the multiple files you need to merge using the File List Connector.</p> <p>Provide the path where this file resides. The following image shows a sample of merge file path where file1 and file 2 are the two files to be merged:</p> 

Connection property	Description
Rows Per Batch	Mention the required batch size to optimize the performance. The default value is 100.
Date Format	Mention the Date format. The default date format is dd-MM-yyyy HH:mm:ss.

## File Processor connection properties

When you set up a File Processor connection, you must configure the connection properties.

The following table describes the File Processor connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Source File Directory	The location that contains files you want to transfer.
Target File Directory	The location where you want to place the transferred files.
Select File	The files that you want to transfer. You can select files based on the fields.
File Pattern	<p>The pattern of the files that you want to transfer.</p> <p>For example, to select a file based on a date pattern, you can specify the date format as DD/MM/YYYY, MM-dd-yyyy, yyyy-MM-dd, or yyyy-MM-d in the file pattern field.</p> <p>Note: The File Pattern field is not applicable when you select <b>all</b> in the <b>Select File</b> connection property.</p>
Days Calculation	<p>Selects files that are created or modified before the specified date or after the specified date. Select files based on Contains Date Pattern and specify the <b>days calculation</b> value so that you can select files that are modified before or after the specified date. Specify the value in terms of days. You cannot specify the value in terms of month and year.</p> <p>You can specify the following date formats: DD/MM/YYYY, MM-dd-yyyy or yyyy-MM-d format.</p> <p>For example, to select a file based on Contains Date Pattern and use the data filters to specify the LastModDate as 02/02/2016, and specify days calculation as -1. Files that are modified till 01/02/2016 are selected.</p>
PassKey	The credentials to connect to FTP or SFTP server. For example, you can specify the password and passphrase of the FTP or SFTP server as passkey1 and passkey2 values.

# Flat file connections

Flat file connections enable you to create, access, and store flat files. You can use flat file connections in mappings and in tasks such as mapping tasks, PowerCenter tasks, replication tasks, and synchronization tasks.

When you configure a flat file connection, you must select the runtime environment to be used with the connection. If you select a runtime environment with Secure Agents that run on Linux, you cannot specify a Windows directory for a flat file target.

A flat file connection cannot use a Secure Agent that runs on NTT. Therefore, do not select a runtime environment with Secure Agents that run on NTT.

In a serverless runtime environment that has data disks configured, you can choose one of the mounted directories or their sub directories to use in the flat file connection.

When you select a flat file connection in a mapping or task, you choose the formatting options for the flat file. When you choose the formatting options in a Source, Lookup, or Target transformation, you specify whether the flat file is a delimited flat file or a fixed-width flat file. If the flat file is a fixed-width flat file, you select a fixed-width format from a list of fixed-width formats that you configured. If you plan to use a fixed-width flat file, you need to create at least one fixed-width format before you select a fixed-width flat file in the Mapping Designer.

## Flat file connection properties

Defines the properties you need to assign to for a flat file source connection.

The following table describes the flat file connection properties:

Connection Property	Description
Runtime Environment	Runtime environment that contains the Secure Agent to use to access the flat files. <b>Note:</b> Do not select a runtime environment with Secure Agents that run on NTT. A flat file connection cannot use a Secure Agent that runs on NTT. Or, a serverless runtime environment that contains the mounted EFS or NFS directories which contain the flat files.
Directory	Directory where the flat file is stored. Must be accessible by all Secure Agents in the selected runtime environment. Enter the full directory or click <b>Browse</b> to locate and select the directory. When you use the connection, you can select a file that's contained in the directory or in any of its subdirectories. When a data disk is configured for a serverless runtime environment, the directory specified here Maximum length is 100 characters. Directory names can contain alphanumeric characters, spaces, and the following special characters: / \ : _ ~ The directory is the service URL for this connection type. <b>Note:</b> On Windows, the <b>Browse for Directory</b> dialog box does not display mapped drives. You can browse My Network Places to locate the directory or enter the directory name in the following format: \\<server_name>\<directory_path>. If network directories do not display, you can configure a login for the Secure Agent service. Do not include the name of the flat file. You specify the file name when you create the task. In a serverless runtime environment, this directory must be one of the mounted directories or their sub directories in the data disk.

Connection Property	Description
Browse button	Use to locate and select the directory where flat files are stored.
Date Format	Date format for date fields in the flat file. Default date format is: MM/dd/yyyy HH:mm:ss
Code Page	<p>The code page of the system that hosts the flat file. Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data</li> <li>- UTF-8. Select for Unicode data</li> <li>- UTF-16 encoding of Unicode (Big Endian)</li> <li>- UTF-16 encoding of Unicode (Lower Endian)</li> <li>- UTF-32 encoding of Unicode (Lower Endian)</li> <li>- ISO 8859-1 Western European.</li> <li>- IBM EBCDIC French</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European)</li> <li>- ISO 8859-2 Eastern European</li> <li>- ISO 8859-3 Southeast European</li> <li>- ISO 8859-5 Cyrillic</li> <li>- ISO 8859-9 Latin 5 (Turkish)</li> <li>- ISO 8859-10 Latin 6 (Nordic) *</li> <li>- IBM EBCDIC International Latin-1</li> <li>- Japanese EUC (with \ &lt;-&gt; Yen mapping)</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- Chinese EUC</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- EBCDIC Hebrew (updated with new sheqel, control characters)</li> <li>- IBM EBCDIC US English IBM037</li> </ul> <p>In advanced mappings, flat file objects in cloud storage connections must use UTF-8 encoding.</p> <p>If the file contains supplementary characters with UTF-16 encoding, the task fails.</p> <p><b>Note:</b> When you use a flat file connection with the Shift-JIS code page and a UTF data object, be sure to install fonts that fully support Unicode.</p>
<p>* Data preview uses a similar ISO 8859-4 Scandinavian/Baltic code page, but runtime processing uses ISO 8859-10 Latin 6 (Nordic), so data preview and runtime encoding won't match.</p>	

## Configuring a locale in Linux for flat file connections

On Linux, for synchronization or replication tasks that use a flat file connection, to support multibyte data you need to set the default locale to UTF-8.

1. To display the current locale, in a shell command line, enter `locale`.
2. To set the default locale to UTF-8, see the following examples:

- For bash and related UNIX shells:

```
export LC_ALL=en_US.UTF-8
```

- For csh and related UNIX shells:  
`setenv LC_ALL en_US.UTF-8`

3. Restart the Secure Agent.

## 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.
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.

Connection property	Description
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: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> <li>- Japanese EUC (with \ &lt;-&gt; Yen mapping)</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- Chinese EUC</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- EBCDIC Hebrew (updated with new sheqel, control characters)</li> </ul>
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.

## Google Ads connection properties

When you create a Google Ads connection, you must configure the connection properties.

The following table describes the Google Ads connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client ID	Required. The OAuth 2.0 client ID from Google Developer Console.
Client Secret	Required. The OAuth 2.0 client secret from Google Developer Console.
Refresh Token	Required. The OAuth 2.0 refresh token received after you exchange the authorization code for Google Ads.
Developer Token	Required. The developer token from the Google Ads manager account.
Account Customer ID	Required. Unique login customer ID to access the Google Ads account through a manager account.

# Google Analytics connection properties

When you create a Google Analytics connection, configure the connection properties.

The following table describes the Google Analytics connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Google Analytics connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Service Account ID	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.
APIVersion	API used to read from Google Analytics reports. You can choose from the following values: <ul style="list-style-type: none"><li>- Core Reporting API v3</li><li>- Analytics Reporting API v4</li><li>- Google Analytics 4</li></ul>
AccountId	Applicable when you select Core Reporting API v3 or Analytics Reporting API v4 in the APIVersion property. The Google Analytics Account ID associated with the Google Analytics project. Applies only when you read data from the following reports: <ul style="list-style-type: none"><li>- Content Grouping</li><li>- Ecommerce</li><li>- Goal Conversions</li></ul> When you read data from any other report, leave the property blank.
PropertyId	The Google Analytics Property ID associated with the Google Analytics project. Applies only when you read data from the following reports: <ul style="list-style-type: none"><li>- Content Grouping</li><li>- Ecommerce</li><li>- Goal Conversions</li></ul> When you read data from any other report, leave the property blank.
ViewId	Applicable when you select Core Reporting API v3 or Analytics Reporting API v4 in the APIVersion property. The Google Analytics View ID associated with the Google Analytics project. <b>Note:</b> Applies only when you read data from Goal Conversions report. When you read data from any other report, leave the property blank.

# Google Analytics Mass Ingestion connection properties

When you set up a Google Analytics Mass Ingestion connection, you must configure the connection properties.

The following table describes the connection properties for a Google Analytics Mass Ingestion connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Service Account ID	Specifies the client_email value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value present in the JSON file that you download after you create a service account.

## Google BigQuery connection properties

When you create a Google BigQuery connection, you must configure the connection properties.

The following table describes the Google BigQuery connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The Google BigQuery connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service Account ID	Specifies the client_email value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value present in the JSON file that you download after you create a service account.

Property	Description
Connection mode	<p>The mode that you want to use to read data from or write data to Google BigQuery.</p> <p>Select one of the following connection modes:</p> <ul style="list-style-type: none"> <li>- Simple. Flattens each field within the Record data type field as a separate field in the mapping.</li> <li>- Hybrid. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the mapping.</li> <li>- Complex. Displays all the columns in the Google BigQuery table as a single field of the String data type in the mapping.</li> </ul> <p>Default is Simple.</p>
Schema Definition File Path	<p>Specifies a directory on the Secure Agent machine where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. The JSON file name is the same as the Google BigQuery table name.</p> <p>Alternatively, you can specify a storage path in Google Cloud Storage where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. You can download the JSON file from the specified storage path in Google Cloud Storage to a local machine.</p> <p>The schema definition file is required if you configure complex connection mode in the following scenarios:</p> <ul style="list-style-type: none"> <li>- You add a Hierarchy Builder transformation in a mapping to read data from relational sources and write data to a Google BigQuery target.</li> <li>- You add a Hierarchy Parser transformation in a mapping to read data from a Google BigQuery source and write data to relational targets.</li> </ul>
Project ID	<p>Specifies the project_id value present in the JSON file that you download after you create a service account.</p> <p>If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.</p>
Dataset ID	<p>Name of the dataset that contains the source table and target table that you want to connect to.</p> <p><b>Note:</b> Google BigQuery supports the datasets that reside only in the US region.</p>
Storage Path	<p>This property applies when you read or write large volumes of data. Required if you read data in staging mode or write data in bulk mode.</p> <p>Path in Google Cloud Storage where the Secure Agent creates a local stage file to store the data temporarily.</p> <p>You can either enter the bucket name or the bucket name and folder name.</p> <p>For example, enter <code>gs://&lt;bucket_name&gt;</code> or <code>gs://&lt;bucket_name&gt;/&lt;folder_name&gt;</code></p>

**Note:** Ensure that you specify valid credentials in the connection properties. The test connection is successful even if you specify incorrect credentials in the connection properties.

## Connection modes

You can configure a Google BigQuery connection to use one of the following connection modes:

### Simple mode

If you use simple mode, Google BigQuery Connector flattens each field within the Record data type field as a separate field in the field mapping.

### Hybrid mode

If you use hybrid mode, Google BigQuery Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the field mapping.

### Complex mode

If you use complex mode, Google BigQuery displays all the columns in the Google BigQuery table as a single field of the String data type in the field mapping.

### Connection mode example

Google BigQuery Connector reads and writes the Google BigQuery data based on the connection mode that you configure for the Google BigQuery connection.

You have a Customers table in Google BigQuery that contains primitive fields and the **Address** field of the Record data type. The Address field contains two primitive sub-fields, **City** and **State**, of the String data type.

The following image shows the schema of the Customers table in Google BigQuery:

<b>ID</b>	INTEGER	NULLABLE
<b>Name</b>	STRING	NULLABLE
<b>Address</b>	RECORD	NULLABLE
<b>Address.City</b>	STRING	NULLABLE
<b>Address.State</b>	STRING	NULLABLE
<b>Mobile</b>	STRING	REPEATED
<b>Totalpayments</b>	FLOAT	NULLABLE
<b>age</b>	INTEGER	REPEATED

The following table shows the Customers table data in Google BigQuery:

ID	Name	Address.City	Address.State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
				+1-8267389993	
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33

ID	Name	Address.City	Address.State	Mobile	Totalpayments
				+1-9876553784	
				+1-8456437848	

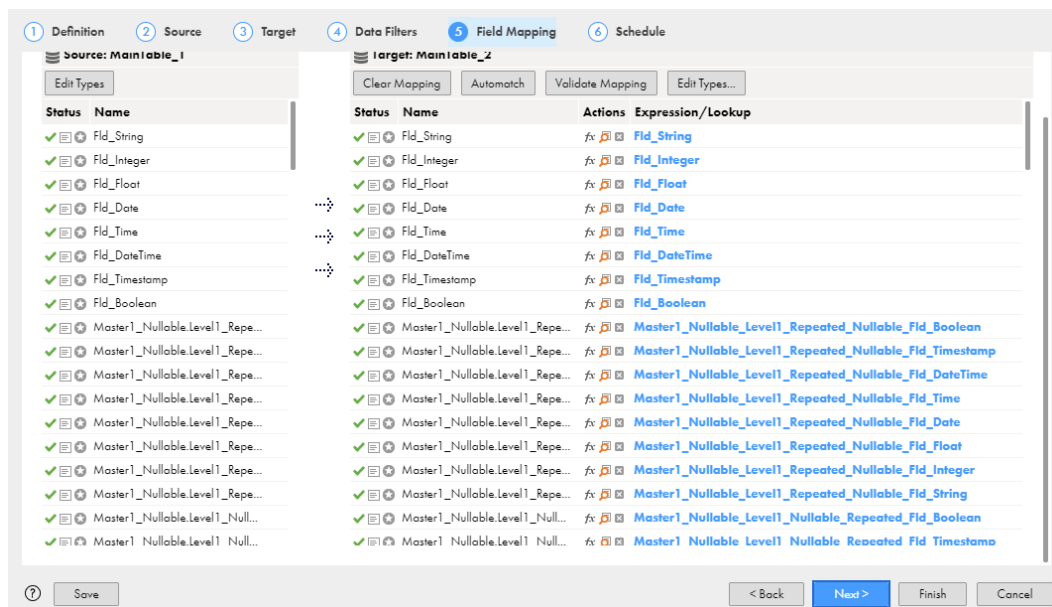
## Simple mode

If you use simple connection mode, Google BigQuery Connector flattens each field within the Record data type field as a separate field in the **Field Mapping** tab.

The following table shows two separate fields, Address\_City and Address\_State, for the respective sub-fields within the Address Record field in the Customers table:

ID	Name	Address_City	Address_State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
14	John	LOS ANGELES	CALIFORNIA	+1-8267389993	18433.90
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
29	Jane	BOSTON	MANHATTAN	+1-9876553784	28397.33
29	Jane	BOSTON	MANHATTAN	+1-8456437848	28397.33

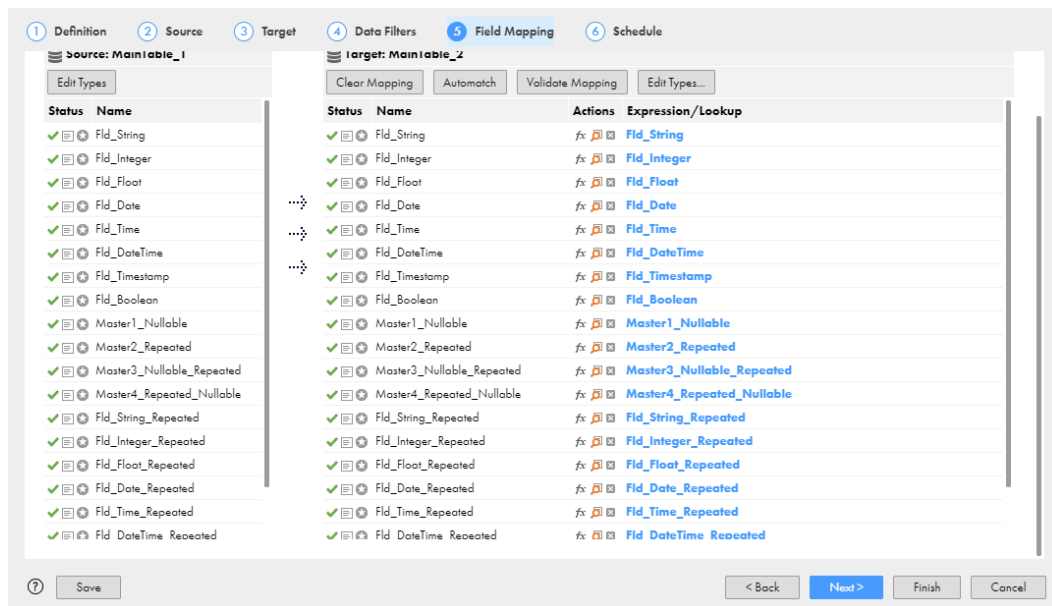
The following image shows the fields in the **Field Mapping** tab of a synchronization task:



## Hybrid mode

If you use hybrid connection mode, Google BigQuery Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the **Field Mapping** tab.

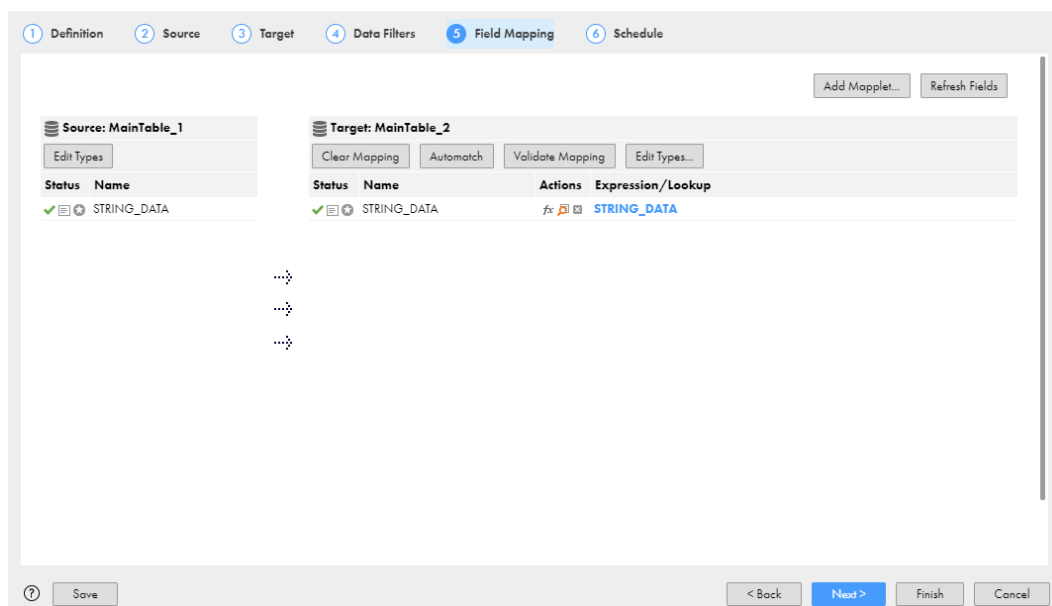
The following image shows the **Field Mapping** tab of a synchronization task:



## Complex mode

If you use complex connection mode, Google BigQuery Connector displays all the columns in the Google BigQuery table as a single field of the String data type in the **Field Mapping** tab.

The following image shows the STRING\_DATA field in the **Field Mapping** tab of a synchronization task:



## Rules and guidelines for Google BigQuery connection modes

### Simple mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use simple connection mode:

- You cannot create a Google BigQuery target table that contains repeated columns using the **Create Target** option.
- If the Google BigQuery source table contains repeated columns, you cannot configure data filters for these columns.
- If the Google BigQuery table contains more than one repeated column, you cannot preview data.
- If the Google BigQuery target table contains repeated columns, you cannot configure update and delete operations for these columns.
- You cannot configure upsert operations for columns of the Record data type and repeated columns.
- When you read data from a Google BigQuery source, you must not map more than one repeated column in a single mapping. You must create multiple mappings for each repeated column.

### Hybrid mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use hybrid connection mode:

- You cannot preview data.
- You cannot create a Google BigQuery target table using the **Create Target** option.
- If the Google BigQuery source table contains columns of the Record data type and repeated columns, you cannot configure data filters for these columns.
- You cannot configure update, upsert, and delete operations for columns of the Record data type and repeated columns.
- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties. You can use CSV format as the data format of the staging file unless the Google BigQuery table contains columns of the Record data type or repeated columns.
- The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows

### Complex mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use complex connection mode:

- You cannot preview data.
- You cannot create a Google BigQuery target table using the **Create Target** option.
- When you configure a Google BigQuery source connection to use complex connection mode, you cannot configure data filters for the source.
- You cannot configure update, upsert, and delete operations.
- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties.

- You cannot use CSV format as the data format of the staging file. The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows
- You cannot use key range partitioning for Google BigQuery sources.

## Google BigQuery V2 connection properties

When you create a Google BigQuery V2 connection, configure the connection properties.

The following table describes the Google BigQuery V2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Google BigQuery V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or serverless runtime environment.
Service Account ID	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.
Project ID	The project_id value in the JSON file that you download after you create a service account. If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.
Storage Path	Path in Google Cloud Storage where the agent creates a local stage file to store the data temporarily. Applies to tasks that read or write large volumes of data. Use this property when you read data in staging mode or write data in bulk mode. You can either enter the bucket name or the bucket name and folder name. Use one of the following formats: <ul style="list-style-type: none"> <li>- gs://&lt;bucket_name&gt;</li> <li>- gs://&lt;bucket_name&gt;/&lt;folder_name&gt;</li> </ul>

Property	Description
Connection mode	<p>The mode that you want to use to read data from or write data to Google BigQuery.</p> <p>Select one of the following connection modes:</p> <ul style="list-style-type: none"> <li>- Simple. Flattens each field within the Record data type field as a separate field in the mapping.</li> <li>- Hybrid<sup>1</sup>. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery V2 Connector displays the top-level Record data type field as a single field of the String data type in the mapping.</li> <li>- Complex<sup>1</sup>. Displays all the columns in the Google BigQuery table as a single field of the String data type in the mapping.</li> </ul> <p>Default is Simple.</p>
Schema Definition File Path <sup>1</sup>	<p>Directory on the Secure Agent machine where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. The JSON file name is the same as the Google BigQuery table name.</p> <p>Alternatively, you can specify a storage path in Google Cloud Storage where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. You can download the JSON file from the specified storage path in Google Cloud Storage to a local machine.</p> <p>The schema definition file is required if you configure complex connection mode in the following scenarios:</p> <ul style="list-style-type: none"> <li>- You add a Hierarchy Builder transformation in a mapping to read data from relational sources and write data to a Google BigQuery target.</li> <li>- You add a Hierarchy Parser transformation in a mapping to read data from a Google BigQuery source and write data to relational targets.</li> </ul> <p><b>Note:</b> When you use a serverless runtime environment, you must specify a storage path in Google Cloud Storage.</p>
Use Legacy SQL For Custom Query <sup>1</sup>	<p>Select this option to use a legacy SQL to define a custom query. If you clear this option, you must use a standard SQL to define a custom query.</p> <p><b>Note:</b> Not applicable when you configure the Google BigQuery V2 connection in hybrid or complex mode.</p>
Dataset Name for Custom Query <sup>1</sup>	<p>When you define a custom query, you must specify a Google BigQuery dataset.</p>
Region Id	<p>The region name where the Google BigQuery dataset that you want to access resides.</p> <p><b>Note:</b> You must ensure that you specify a bucket name or the bucket name and folder name in the <b>Storage Path</b> property that resides in the specified region.</p> <p>For more information about the regions supported by Google BigQuery, see <a href="#">Dataset locations</a>.</p>
Staging Dataset <sup>1</sup>	<p>The Google BigQuery dataset name where you want to create the staging table to stage the data. You can define a Google BigQuery dataset that is different from the source or target dataset.</p>

Property	Description
Optional Properties <sup>1</sup>	Specifies whether you can configure source and target functionality through custom properties. You can select one of the following options: <ul style="list-style-type: none"> <li>- None. If you do not want to configure any custom properties, select None.</li> <li>- Required. If you want to specify custom properties to configure the source and target functionalities.</li> </ul> Default is None.
Provide Optional Properties <sup>1</sup>	Comma-separated key-value pairs of custom properties in the Google BigQuery V2 connection to configure certain source and target functionalities. Appears when you select <b>Required</b> in the Optional Properties. For more information about the list of custom properties that you can specify, see the Informatica Knowledge Base article: <a href="https://kb.informatica.com/faq/7/Pages/26/632722.aspx">https://kb.informatica.com/faq/7/Pages/26/632722.aspx</a>

<sup>1</sup> Doesn't apply to mappings in advanced mode.

**Note:** Ensure that you specify valid credentials in the connection properties. The test connection is successful even if you specify incorrect credentials in the connection properties.

## Retry Strategy

When you read data from Google BigQuery in staging mode and write data to Google BigQuery in bulk mode, you can configure the retry strategy when the Google BigQuery V2 connection fails to connect to the Google BigQuery. The retry strategy is not applicable in the CDC and streaming modes when you write data to a Google BigQuery target.

The following table describes the retry properties for the Google BigQuery V2 connection. These retry properties apply only to mappings.

Property	Description
Enable Retry	Indicates that the Secure Agent attempts to retry the connection when there is a failure. Select this option to enable connection retry. Default is unselected.
Maximum Retry Attempts	The maximum number of retry attempts that the Secure Agent performs to receive the response from the Google BigQuery endpoint. If the Secure Agent fails to connect to Google BigQuery within the maximum retry attempts, the connection fails. Default is 6. Appears when you select the <b>Enable Retry</b> property.
Initial Retry Delay	The initial wait time in seconds before the Secure Agent attempts to retry the connection. Default is 1. Appears when you select the <b>Enable Retry</b> property.
Retry Delay Multiplier	The multiplier that the Secure Agent uses to exponentially increase the wait time between successive retry attempts up to the maximum retry delay time. Default is 2.0. Appears when you select the <b>Enable Retry</b> property.

Property	Description
Maximum Retry Delay	The maximum wait time in seconds that the Secure Agent waits between successive retry attempts. Default is 32. Appears when you select the <b>Enable Retry</b> property.
Total Timeout	The total time duration in seconds that the Secure Agent attempts to retry the connection after which the connection fails. Default is 50. Appears when you select the <b>Enable Retry</b> property.

## Connection modes

You can configure a Google BigQuery V2 connection to use one of the following connection modes:

### Simple mode

If you use simple mode, Google BigQuery V2 Connector flattens each field within the Record data type field as a separate field in the field mapping.

### Hybrid mode

If you use hybrid mode, Google BigQuery V2 Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery V2 Connector displays the top-level Record data type field as a single field of the String data type in the field mapping.

### Complex mode

If you use complex mode, Google BigQuery displays all the columns in the Google BigQuery table as a single field of the String data type in the field mapping.

## Connection mode example

Google BigQuery V2 Connector reads and writes the Google BigQuery data based on the connection mode that you configure for the Google BigQuery V2 connection.

You have a Customers table in Google BigQuery that contains primitive fields and the **Address** field of the Record data type. The Address field contains two primitive sub-fields, **City** and **State**, of the String data type.

The following image shows the schema of the Customers table in Google BigQuery:

<b>ID</b>	INTEGER	NULLABLE
<b>Name</b>	STRING	NULLABLE
<b>Address</b>	RECORD	NULLABLE
<b>Address.City</b>	STRING	NULLABLE
<b>Address.State</b>	STRING	NULLABLE
<b>Mobile</b>	STRING	REPEATED
<b>Totalpayments</b>	FLOAT	NULLABLE
<b>age</b>	INTEGER	REPEATED

The following table shows the Customers table data in Google BigQuery:

ID	Name	Address.City	Address.State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
				+1-8267389993	
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
				+1-9876553784	
				+1-8456437848	

### Simple mode

If you use simple connection mode, Google BigQuery V2 Connector flattens each field within the Record data type field as a separate field in the **Field Mapping** tab.

The following table shows two separate fields, Address\_City and Address\_State, for the respective sub-fields within the Address Record field in the Customers table:

ID	Name	Address_City	Address_State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
14	John	LOS ANGELES	CALIFORNIA	+1-8267389993	18433.90
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
29	Jane	BOSTON	MANHATTAN	+1-9876553784	28397.33
29	Jane	BOSTON	MANHATTAN	+1-8456437848	28397.33

The following image shows the fields in the **Field Mapping** tab of the Target transformation:

Field map options: Automatic Note: This option will automatically map any fields added later by name. Options

Incoming Fields: (112 of 112 mapped)

Find

Field Name
Fld_String
Fld_Integer
Fld_Float
Fld_Date
Fld_Time
Fld_DateTime
Fld_Timestamp
Fld_Boolean
Master1_Nullable_Level1_Repeated_Nullable_Fld_Boolean
Master1_Nullable_Level1_Repeated_Nullable_Fld_Timestamp
Master1_Nullable_Level1_Repeated_Nullable_Fld_DateTime
Master1_Nullable_Level1_Repeated_Nullable_Fld_Time
Master1_Nullable_Level1_Repeated_Nullable_Fld_Date
Master1_Nullable_Level1_Repeated_Nullable_Fld_Float
Master1_Nullable_Level1_Repeated_Nullable_Fld_Integer

Target Fields: (112 of 112 mapped)

Find

Field Name	Mapped Field
Fld_String	Fld_String
Fld_Integer	Fld_Integer
Fld_Float	Fld_Float
Fld_Date	Fld_Date
Fld_Time	Fld_Time
Fld_DateTime	Fld_DateTime
Fld_Timestamp	Fld_Timestamp
Fld_Boolean	Fld_Boolean
Master1_Nullable_Level1_Repeated_Nullable_Fld_Boolean	Master1_Nullable_Level1_Repeated_Nullable_Fld_Boolean
Master1_Nullable_Level1_Repeated_Nullable_Fld_Timestamp	Master1_Nullable_Level1_Repeated_Nullable_Fld_Timestamp
Master1_Nullable_Level1_Repeated_Nullable_Fld_DateTime	Master1_Nullable_Level1_Repeated_Nullable_Fld_DateTime
Master1_Nullable_Level1_Repeated_Nullable_Fld_Time	Master1_Nullable_Level1_Repeated_Nullable_Fld_Time
Master1_Nullable_Level1_Repeated_Nullable_Fld_Date	Master1_Nullable_Level1_Repeated_Nullable_Fld_Date
Master1_Nullable_Level1_Repeated_Nullable_Fld_Float	Master1_Nullable_Level1_Repeated_Nullable_Fld_Float
Master1_Nullable_Level1_Repeated_Nullable_Fld_Integer	Master1_Nullable_Level1_Repeated_Nullable_Fld_Integer

## Hybrid mode

If you use hybrid connection mode, Google BigQuery V2 Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery V2 Connector displays the top-level Record data type field as a single field of the String data type in the **Field Mapping** tab.

The following image shows the **Field Mapping** tab of the Target transformation:

Field map options: Automatic Note: This option will automatically map any fields added later by name. Options

Incoming Fields: (20 of 20 mapped) Find

Field Name
Fld_String
Fld_Integer
Fld_Float
Fld_Date
Fld_Time
Fld_DateTime
Fld_Timestamp
Fld_Boolean
Master1_Nullable
Master2_Repeated
Master3_Nullable_Repeated
Master4_Repeated_Nullable
Fld_String_Repeated
Fld_Integer_Repeated
Fld_Float_Repeated

Target Fields: (20 of 20 mapped) Find

Field Name	Mapped Field
Fld_String	Fld_String
Fld_Integer	Fld_Integer
Fld_Float	Fld_Float
Fld_Date	Fld_Date
Fld_Time	Fld_Time
Fld_DateTime	Fld_DateTime
Fld_Timestamp	Fld_Timestamp
Fld_Boolean	Fld_Boolean
Master1_Nullable	Master1_Nullable
Master2_Repeated	Master2_Repeated
Master3_Nullable_Repeated	Master3_Nullable_Repeated
Master4_Repeated_Nullable	Master4_Repeated_Nullable
Fld_String_Repeated	Fld_String_Repeated
Fld_Integer_Repeated	Fld_Integer_Repeated
Fld_Float_Repeated	Fld_Float_Repeated

## Complex mode

If you use complex connection mode, Google BigQuery V2 Connector displays all the columns in the Google BigQuery table as a single field of the String data type in the **Field Mapping** tab.

The following image shows the STRING\_DATA field in the **Field Mapping** tab of the Target transformation:

Field map options: Automatic Note: This option will automatically map any fields added later by name. Options

Incoming Fields: (1 of 1 mapped) Find

Field Name
STRING_DATA

Target Fields: (1 of 1 mapped) Find

Field Name	Mapped Field
STRING_DATA	STRING_DATA

## Rules and guidelines for Google BigQuery V2 connection modes

### Simple mode

Consider the following rules and guidelines when you configure a Google BigQuery V2 connection to use simple connection mode:

- You cannot configure mappings in advanced mode.
- You can read data from a repeated column from a Google BigQuery source table only when you select **Direct** as the **Read Mode**.
- You cannot create a Google BigQuery target table that contains repeated columns using the **Create Target** option.
- If the Google BigQuery source table contains repeated columns, you cannot configure data filters for these columns.
- If the Google BigQuery table contains more than one repeated column, you cannot preview data.
- If the Google BigQuery target table contains a repeated column of the Record data type, you cannot configure update, upsert, and delete operations for these columns.
- You can use CSV format as the data format of the staging file only when the Google BigQuery table does not contain columns of the Record data type or repeated columns.
- If the Google BigQuery target table contains columns of the Record data type and repeated columns, you cannot configure update, upsert, and delete operations for these columns when you do not use the Merge query.

- When you read data from a Google BigQuery source, you must not map more than one repeated column in a single mapping. You must create multiple mappings for each repeated column.
- You cannot import multiple source tables in a Source transformation.

### Hybrid mode

Consider the following rules and guidelines when you configure a Google BigQuery V2 connection to use hybrid connection mode:

- You cannot preview data.
- You cannot use a legacy SQL statement to define a custom query. You must use a standard SQL to define a custom query
- If the Google BigQuery source table contains columns of the Record data type and repeated columns, you cannot configure data filters for these columns.
- When you do not use the Merge query and the key field is a column of the Record data type or a repeated column, you cannot configure update, upsert, and delete operations.
- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties. You can use CSV format as the data format of the staging file only when the Google BigQuery table does not contain columns of the Record data type or repeated columns.
- The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows

### Complex mode

Consider the following rules and guidelines when you configure a Google BigQuery V2 connection to use complex connection mode:

- You cannot configure mappings in advanced mode.
- You cannot import multiple source tables in a Source transformation.
- You cannot preview data.
- You cannot use a legacy SQL statement to define a custom query. You must use a standard SQL to define a custom query
- You cannot create a Google BigQuery target table using the **Create Target** option.
- You cannot truncate the Google BigQuery target table before loading data to the target using the **Truncate target table** option.
- When you configure a Google BigQuery source connection to use complex connection mode, you cannot configure data filters for the source.
- You cannot configure update, upsert, and delete operations.
- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties.
- You cannot use CSV format as the data format of the staging file. The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows
- You cannot use key range partitioning for Google BigQuery sources.

# Google Bigtable connection properties

When you create a Google Bigtable connection, you must configure the connection properties.

The following table describes the Google Cloud Bigtable connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>googleBigTable</b> connection type.
Runtime Environment	Runtime environment that contains the Secure Agent used to access Google Cloud Bigtable.
Project ID	Specifies the project_id value present in the JSON file that you download after you create a service account.
Service Account ID	Specifies the client_email value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value present in the JSON file that you download after you create a service account.

# Google Cloud Spanner connection properties

When you create a Google Cloud Spanner connection, configure the connection properties.

The following table describes the Google Cloud Spanner connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Google Cloud Spanner connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.

Property	Description
Project ID	The project_ID value in the JSON file that you download after you create a service account. If you have created multiple projects with the same service account, enter the ID of the project that contains the Cloud Spanner instance that you want to connect to.
Instance ID	Name of the instance that you created in Google Cloud Spanner.
Service Account ID	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.

## Google Cloud Storage connection properties

When you create a Google Cloud Storage connection, you must configure the connection properties.

The following table describes the Google Cloud Storage connection properties:

Property	Description
Runtime Environment	Runtime environment that contains the Secure Agent used to access Google Cloud Storage.
Project ID	Specifies the project_id value present in the JSON file that you download after you create a service account. If you have created multiple projects with the same service account, enter the ID of the project that contains the bucket that you want to connect to.
Service Account ID	Specifies the client_email value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value present in the JSON file that you download after you create a service account.
File Path	Path in Google Cloud Storage where you want to read or write data. You can either enter the bucket name or the bucket name and folder name. For example, enter <bucket name> or <bucket name>/<folder name>

# Google Cloud Storage V2 connection properties

When you create a Google Cloud Storage V2 connection, configure the connection properties.

The following table describes the Google Cloud Storage connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Google Cloud Storage V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task or streaming ingestion task on a Hosted Agent or serverless runtime environment.
Service Account ID	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.
Project ID	The project_id value in the JSON file that you download after you create a service account. If you created multiple projects with the same service account, enter the ID of the project that contains the bucket that you want to connect to.
Is Encrypted File <sup>1</sup>	Specifies whether a file is encrypted. Select this option when you import an encrypted file from Google Cloud Storage. Default is unselected.
Private Key ID	The private_key_id value in the JSON file that you download after you create a service account. This property applies only to a database ingestion or streaming ingestion task.
Client ID	The client_id value in the JSON file that you download after you create a service account. This property applies only to a database ingestion or streaming ingestion task.

Property	Description
Bucket Name	<p>The Google Cloud Storage bucket name that you want to connect to.</p> <p>When you select a source object or target object in a mapping, the Package Explorer lists files and folder available in the specified Google Cloud Storage bucket.</p> <p>If you do not specify a bucket name, you can select a bucket from the Package Explorer to select a source or target object.</p>
Optimize Object Metadata Import	<p>Optimizes the import of metadata for the selected object without parsing other objects, folders, or sub-folders available in the bucket.</p> <p>Directly importing metadata for the selected object can improve performance by reducing the overhead and time taken to parse each object available in the bucket.</p> <p>Default is not selected.</p>

<sup>1</sup> Applies only to mappings in advanced mode.

## Google Drive connection properties

When you create a Google Drive connection, you must configure the connection properties.

The following table describes the Google Drive connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client ID	The Client ID from Google Developer Console.
Client Secret	The Client Secret from Google Developer Console.
Refresh Token	The Refresh Token received after exchanging authorization code.
File Download Path	The directory where file needs to be downloaded.
File Upload Path	The directory where file is stored and needs to be uploaded.
PageSize	The page size for the read operation. Default value is 10.

# Google PubSub connection properties

When you create a Google PubSub connection, you must configure the connection properties.

The following table describes the Google PubSub connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+=[{]} \:;'"<,>.?/
Description	Optional. The description of the connection. The description must not exceed 4,000 characters.
Type	The <b>GooglePubSub</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service Account ID	Specifies the client_email value available in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value available in the JSON file that you download after you create a service account in a secured way.
Project ID	Specifies the project_id value available in the JSON file that you download after you create a service account.
maxMessageForBatch	Specifies the number of messages that the Secure Agent can publish in a batch. Default is 100. The maximum value is 1000.

# Google PubSub V2 connection properties

When you create a Google PubSub V2 connection, you must configure the connection properties.

The following table describes the Google PubSub V2 connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+=[{]} \:;'"<,>.?/
Description	Optional. The description of the connection. The description must not exceed 4,000 characters.
Type	The <b>GooglePubSubV2</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.

Property	Description
Service Account ID	Specifies the <code>client_email</code> value available in the JSON file that you download after you create a service account.
Service Account Key	Specifies the <code>private_key</code> value available in the JSON file that you download after you create a service account in a secured way.
Project ID	Specifies the <code>project_id</code> value available in the JSON file that you download after you create a service account.

## Google PubSub - Mass Ingestion Streaming connection properties

When you define a Google PubSub Mass Ingestion Streaming connection, you must configure connection properties. You can use this connection type in streaming ingestion tasks, which you configure in the Mass Ingestion service.

The following table describes the Google PubSub connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you use to identify the connection. The description must not exceed 4,000 characters.
Type	The <b>Google PubSub</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client Email	The <code>client_email</code> value available in the JSON file that you download after you create a service account.
Client ID	The <code>client_id</code> value available in the JSON file that you download after you create a service account.
Private Key ID	The <code>private_key_id</code> value available in the JSON file that you download after you create a service account.
Private Key	The <code>private_key</code> value available in the JSON file that you download after you create a service account.
Project ID	The <code>project_id</code> value available in the JSON file that you download after you create a service account.

**Note:** The test connection for the Google PubSub connector does not fail even if you enter incorrect values for **Client ID** and **Private Key ID**.

## Google Sheets connection properties

When you create a Google Sheets connection, you must configure the connection properties.

The following table describes the Google Sheets connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
ClientId	Required. The Client ID from Google Developer Console.
ClientSecret	Required. The Client Secret from Google Developer Console.
RefreshTokenForSheet	Required. The Refresh Token received after exchanging authorization code for Google Sheets.
RefreshTokenForDrive	Optional. The Refresh Token received after exchanging authorization code for Google Drive. This option is required when you enter the spreadsheet name in the <b>SpreadSheetName</b> field.
SpreadSheetName	Name of the spreadsheet in Google Sheets.
SpreadSheetId	ID of the spreadsheet in Google Sheets.
InitialColumnRange	Specifies the first column name from a data range in a Google Sheets spreadsheet from where you want to start reading the data. For example, specify the InitialColumnRange value as Sheet1!C5.
FinalColumnRange	Specifies the last column name from a data range in a Google Sheets spreadsheet from where you want to stop reading the data. For example, specify the FinalColumnRange value as Sheet1!G20.
HeaderPresent	Select this option to indicate that the sheet contains a header. If you select this option and the sheet does not contain a header, the first row is treated as the header.
CreateNewSpreadsheet	Select this option to create a new spreadsheet in Google Sheets. The Google Sheets Connector creates an empty spreadsheet with the name that you specified in the <b>SpreadSheetName</b> field. Once you test the connection, disable this option. Otherwise, the Google Sheets Connector will create a new spreadsheet with the same name everytime

## Google Sheets V2 connection properties

When you create a Google Sheets V2 connection, you must configure the connection properties.

The following table describes the Google Sheets V2 connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client ID	Required. The client ID from Google Developer Console.
Client Secret	Required. The client secret from Google Developer Console.
Refresh Token	Required. The refresh token received after you exchange authorization code for Google Sheets.
Spreadsheet ID	ID of the spreadsheet in Google Sheets.
Header Present	Indicates that the sheet contains a header. If you select this option and the sheet does not contain a header, the first row is treated as the header.

## Greenplum connection properties

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

The following table describes the Greenplum connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Host Name	Host name or IP address of the Greenplum server.
Port	Greenplum server port number. If you enter 0, the gpload utility reads from the environment variable \$PGPORT. Default is 5432.
Database	Name of the database.
Schema	Name of the schema that contains the metadata for Greenplum sources or targets. Default is public.
Certificate Path	<p>Path where the SSL certificates for the Greenplum server are stored. Specify the path if you want to establish secure communication between the gpload utility and the Greenplum server over SSL.</p> <p>For information about the files that need to be available in the certificates path, see the gpload documentation.</p> <p><b>Note:</b> SSL configuration is applicable only for the Greenplum writer.</p>

Connection property	Description
Metadata Additional Connection Configuration	Additional metadata connection properties that you want to use. Use the following format: <parameter name1>=<value1>, <parameter name2>=<value2>
Driver Name	The driver name. Specify DataDirect 7.1 Greenplum Wire Protocol.
User Name	User name with permissions to access the Greenplum database.
Password	Password to connect to the Greenplum database.

## Hadoop Files V2 connection properties

When you set up a Hadoop Files V2 connection, you must configure the connection properties.

The following table describes the Hadoop Files V2 connection properties:

Connection property	Description
Connection Name	Name of the Hadoop Files V2 connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select <b>Hadoop Files V2</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
User Name	Required to read data from HDFS. Enter a user name that has access to the single-node HDFS location to read data from or write data to.

Connection property	Description
NameNode URI	<p>The URI to access HDFS.</p> <p>Use the following format to specify the name node URI in Cloudera, Amazon EMR, and Hortonworks distributions:</p> <pre>hdfs://&lt;namenode&gt;:&lt;port&gt;/</pre> <p>where,</p> <ul style="list-style-type: none"> <li>- &lt;namenode&gt; is the host name or IP address of the name node.</li> <li>- &lt;port&gt; is the port that the name node listens for remote procedure calls (RPC).</li> </ul> <p>To connect to the Hadoop cluster, specify the name node port <code>fs.defaultFS</code>.</p> <p>If the Hadoop cluster is configured for high availability, you must copy the <code>fs.defaultFS</code> value in the <code>core-site.xml</code> file and append <code>/</code> to specify the name node URI.</p> <p>For example, the following snippet shows the <code>fs.defaultFS</code> value in a sample <code>core-site.xml</code> file:</p> <pre>&lt;property&gt;   &lt;name&gt;fs.defaultFS&lt;/name&gt;   &lt;value&gt;hdfs://nameservice1&lt;/value&gt;   &lt;source&gt;core-site.xml&lt;/source&gt; &lt;/property&gt;</pre> <p>In the above snippet, the <code>fs.defaultFS</code> value is</p> <pre>hdfs://nameservice1</pre> <p>and the corresponding name node URI is</p> <pre>hdfs://nameservice1/</pre> <p><b>Note:</b> Specify either the name node URI or the local path. Do not specify the name node URI if you want to read data from or write data to a local file system path.</p>
Local Path	<p>A local file system path to read and write data. Read the following conditions to specify the local path:</p> <ul style="list-style-type: none"> <li>- You must enter <b>NA</b> in local path if you specify the name node URI. If the local path does not contain <b>NA</b>, the name node URI does not work.</li> <li>- If you specify the name node URI and local path, the local path takes the preference. The connection uses the local path to run all tasks.</li> <li>- If you leave the local path blank, the agent configures the root directory (<code>/</code>) in the connection. The connection uses the local path to run all tasks.</li> <li>- If the file or directory is in the local system, enter the fully qualified path of the file or directory.</li> </ul> <p>For example, <code>/user/testdir</code> specifies the location of a directory in the local system.</p> <p>Default value for Local Path is <code>NA</code>.</p>
Configuration Files Path	<p>The directory that contains the Hadoop configuration files.</p> <p><b>Note:</b> Copy the <code>core-site.xml</code>, <code>hdfs-site.xml</code>, and <code>hive-site.xml</code> from the Hadoop cluster and add them to a folder in Linux Box.</p>
Keytab File	The file that contains encrypted keys and Kerberos principals to authenticate the machine.
Principal Name	Users assigned to the superuser privilege can perform all the tasks that a user with the administrator privilege can perform.
Impersonation Username	You can enable different users to run mappings in a Hadoop cluster that uses Kerberos authentication or connect to sources and targets that use Kerberos authentication. To enable different users to run mappings or connect to big data sources and targets, you must configure user impersonation.

**Note:** When you read from or write to remote files, the **NameNode URI** and **Configuration Files Path** fields are mandatory. When you read from or write to local files, you require only the **Local Path** field.

## Hive connection properties

To use Hive Connector in a mapping task, you must create a connection in Data Integration.

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

The following table describes the Hive connection properties:

Connection property	Description
Authentication Type	<p>You can select one of the following authentication types:</p> <ul style="list-style-type: none"><li>- Kerberos. Select <b>Kerberos</b> for a Kerberos cluster.</li><li>- LDAP. Select <b>LDAP</b> for an LDAP-enabled cluster.</li></ul> <p><b>Note:</b> LDAP is not applicable to mappings in advanced mode.</p> <ul style="list-style-type: none"><li>- None. Select <b>None</b> for a Hadoop cluster that is not secure or not LDAP-enabled.</li></ul>
JDBC URL *	<p>The JDBC URL to connect to Hive.</p> <p>Specify the following format based on your requirement:</p> <ul style="list-style-type: none"><li>- To view and import tables from a single database, use the following format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/&lt;database name&gt;</code></li><li>- To view and import tables from multiple databases, do not enter the database name. Use the following JDBC URL format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/</code></li></ul> <p><b>Note:</b> After the port number, enter a slash.</p> <ul style="list-style-type: none"><li>- To access Hive on a Hadoop cluster enabled for TLS, specify the details in the JDBC URL in the following format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/&lt;database name&gt;;ssl=true;sslTrustStore=&lt;TrustStore_path&gt;;trustStorePassword=&lt;TrustStore_password&gt;</code>, where the truststore path is the directory path of the truststore file that contains the TLS certificate on the agent machine.</li></ul>
JDBC Driver *	The JDBC driver class to connect to Hive.
Username	The user name to connect to Hive in LDAP or None mode.
Password	The password to connect to Hive in LDAP or None mode.
Principal Name	The principal name to connect to Hive through Kerberos authentication.
Impersonation Name	The user name of the user that the Secure Agent impersonates to run mappings on a Hadoop cluster. You can configure user impersonation to enable different users to run mappings or connect to Hive. The impersonation name is required for the Hadoop connection if the Hadoop cluster uses Kerberos authentication.
Keytab Location	The path and file name to the Keytab file for Kerberos login.

Connection property	Description
Configuration Files Path *	<p>The directory that contains the Hadoop configuration files for the client.</p> <p>Copy the site.xml files from the Hadoop cluster and add them to a folder in the Linux box. Specify the path in this field before you use the connection in a mapping to access Hive on a Hadoop cluster:</p> <ul style="list-style-type: none"> <li>- For mappings, you require the core-site.xml, hdfs-site.xml, and hive-site.xml files.</li> <li>- For mappings in advanced mode, you require the core-site.xml, hdfs-site.xml, hive-site.xml, mapred-site.xml, and yarn-site.xml files.</li> </ul>
DFS URI *	<p>The URI to access the Distributed File System (DFS), such as Amazon S3, Microsoft Azure Data Lake Storage, and HDFS.</p> <p><b>Note:</b> For mappings in advanced mode that run on the advanced cluster, Azure Data Lake Storage Gen2 is supported on the Azure HDinsight cluster.</p> <p>Based on the DFS you want to access, specify the required storage and bucket name.</p> <p>For example, for HDFS, refer to the value of the <b>fs.defaultFS</b> property in the <b>core-site.xml</b> file of the Hadoop cluster and enter the same value in the <b>DFS URI</b> field.</p>
DFS Staging Directory	<p>The staging directory in the Hadoop cluster where the Secure Agent stages the data. You must have full permissions for the DFS staging directory.</p> <p>Specify a transparent encrypted folder as the staging directory.</p>
Hive Staging Database	<p>The Hive database where external or temporary tables are created. You must have full permissions for the Hive staging database.</p>
Additional Properties	<p>Applies to mappings in advanced mode.</p> <p>The additional properties required to access the DFS.</p> <p>Configure the property as follows:</p> <p>&lt;DFS property name&gt;=&lt;value&gt;;&lt;DFS property name&gt;=&lt;value&gt;</p> <p>For example:</p> <p>To access the Amazon S3 file system, specify the access key, secret key, and the Amazon S3 property name, each separated by a semicolon:</p> <pre>fs.s3a.&lt;bucket_name&gt;.access.key=&lt;access key value&gt;; fs.s3a.&lt;bucket_name&gt;.secret.key=&lt;secret key value&gt;; fs.s3a.impl=org.apache.hadoop.fs.s3a.S3AFileSystem;</pre> <p>To access the Azure Data Lake Storage Gen2 file system, specify the authentication type, authentication provider, client ID, client secret, and the client endpoint, each separated with a semicolon:</p> <pre>fs.azure.account.auth.type=&lt;Authentication type&gt;; fs.azure.account.oauth.provider.type=&lt;Authentication_provider&gt;; fs.azure.account.oauth2.client.id=&lt;Client_ID&gt;; fs.azure.account.oauth2.client.secret=&lt;Client-secret&gt;; fs.azure.account.oauth2.client.endpoint=&lt;ADLS Gen2 endpoint&gt;</pre>
* These fields are mandatory parameters.	

# HubSpot connection properties

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

The following table describes the HubSpot connection properties:

Connection property	Description
Connection Name	The name of the HubSpot connection.
Description	The description of the connection.
Type	The type of connection. Select the HubSpot connection.
Client Id	The ID of your application to authenticate access to HubSpot. You can get the client ID value from the HubSpot applications.
Client Secret	The client secret key to authenticate access to HubSpot. You can get the client secret value from the HubSpot applications.
RefreshToken	The refresh token that you need to authenticate access to HubSpot.

# IBM MQ connection properties

When you set up an IBM MQ connection, configure the connection properties.

The following table describes the IBM MQ connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The IBM MQ connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select the Secure Agent from the list as the runtime environment.
Host	The machine that hosts the IBM MQ server.
Port	The port number that connects to the Queue Manager component in the IBM MQ server.
User Name	The user name to connect to the connection channel of the Queue Manager component. Don't specify the user name when the channel authentication of the Queue Manager component is not enabled.

Property	Description
Password	The password to connect to the connection channel of the Queue Manager component. Don't specify the password when the channel authentication of the Queue Manager component is not enabled.
Queue Manager	The Queue Manager component from which queues need to be listed to send or receive messages.
Channel	The server-connection channel that connects to a queue in the Queue Manager. If you don't enable the channel authentication of the Queue Manager component, the default user account for the IBM MQ service writes data to the target.
Code Page	The code page of the server that the Secure Agent uses to read from or write to IBM MQ. Select one of the following code pages from the list: <ul style="list-style-type: none"> <li>- UTF-8</li> <li>- UTF-16</li> <li>- MS Windows Latin 1</li> </ul> Default is UTF-8.
SSL	Specifies whether the connection uses an SSL socket to connect to IBM MQ. Default is disabled.
Truststore Password	The password to access the truststore file that contains the SSL certificate.
Truststore File Path	Absolute path and file name of the truststore file that contains the SSL certificate to connect to IBM MQ. Specify both the directory and file name in the following format: <code>/root/&lt;folder name&gt;/&lt;truststore file name&gt;.jks</code>

## IDMS CDC connection properties

When you configure an IDMS CDC connection, you must set the connection properties.

The following table describes IDMS CDC connection properties:

Property	Description
Connection Name	A name for the IDMS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IDMS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For IDMS CDC, the type must be <b>IDMS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for IDMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: LSNR1:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains the capture registrations for the IDMS data sources. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>

Property	Description
Map Location	<p>Host name or IP address of the system where the extraction maps reside. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: CDC01:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The IDMS event table must reside on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) IDMS CDC connections in PowerCenter.</p>

## IDMS connection properties

When you configure an IDMS connection, you must set the connection properties.

The following table describes IDMS connection properties:

Property	Description
Connection Name	<p>A name for the IDMS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the IDMS connection. Maximum length is 4000 characters.

Property	Description
Type	Type of connection. For IDMS, the type must be <b>IDMS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for IDMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>PWXMLSNR:14673</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the IDMS source.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection property for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For IDMS data sources and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> property specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.

Property	Description
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) IDMS connections in PowerCenter.
Write Properties > Write Mode	Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> Default is <b>Confirm Write On</b> .

## IMS CDC Connection Properties

When you configure an IMS CDC connection, you must set the connection properties.

The following table describes IMS CDC connection properties:

Property	Description
Connection Name	A name for the IMS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IMS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For IMS CDC, the type must be <b>IMS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for IMS change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <div style="text-align: center;"><i>host_name:port_number</i></div> For example: ADACDC1A:1467

Property	Description
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The IMS instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the IMS source. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  $host\_name:port\_number$ For example: ADACDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.

Property	Description
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an IMS table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) IMS CDC connections in PowerCenter.

## IMS connection properties

When you configure an IMS connection, you must set the connection properties.

The following table describes the IMS connection properties:

Property	Description
Connection Name	A name for the IMS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IMS connection. Maximum length is 4000 characters.
Type	Type of connection. For IMS, the type must be <b>IMS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for IMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <div style="text-align: center;"><i>host_name:port_number</i></div> For example: PWXMLSNR:14673

Property	Description
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the IMS source.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> Default is No.
Offload Threads	The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs. Valid values are 1 through 64. Default is 0, which disables multithreading. Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.
Array Size	For IMS data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions. For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size. Valid values are from 1 through 5000. Default is 25. To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b> , increase the array size.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.

Property	Description
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) IMS connections in PowerCenter.</p>
Write Properties	<p>Write Mode. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> <p>Default is <b>Confirm Write On.</b></p>

## JDBC connection properties

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

The following table describes JDBC connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
JDBC Connection URL	<p>The JDBC URL string to connect to the database.</p> <p>The format of the JDBC URL is: <code>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</code>, where subprotocol defines the database connectivity mechanism that one or more drivers might support. The contents and syntax of the subname depends on the subprotocol.</p> <p>For information about the formatting requirements for the JDBC URL connection string, see the JDBC driver vendor specific documentation.</p>
JDBC Jar Directory	<p>Optional. The path to the JDBC driver jar file. For example, you can enter the following directory: <code>C:/jdbc</code>. When you do not specify a directory path, the Secure Agent obtains the jar file from the directory that is specified in the CLASSPATH system variable.</p> <p>To use the serverless runtime environment for the JDBC connection, specify the following location: <code>/home/cldagnt/SystemAgent/serverless/configurations/jdbc</code></p>
JDBC Driver Class Name	Optional. Specify the JDBC driver class name if you are using a JDBC driver without auto class load feature. If you do not specify this property, the Secure Agent loads the driver class name from the JDBC jar file.
Schema	<p>Schema name, which varies by database. For example,</p> <ul style="list-style-type: none"> <li>- Informix. Optional. The schema name is the database name.</li> </ul> <p>You must enter a schema name to fetch metadata if the JDBC connection URL does not provide enough context.</p>

Connection property	Description
Username	User name to connect to the database.
Password	Password to connect to the database.

## JDBC V2 connection properties

When you set up a JDBC V2 connection, configure the connection properties.

The following table describes the JDBC V2 connection properties:

Property	Description
Connection Name	Name of the connection.
Description	Description of the connection.
Type	Type of connection. Select JDBC V2 from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent or serverless runtime environment.
User Name	The user name to connect to the database.
Password	The password for the database user name.
Schema Name	Optional. The schema name. If you don't specify the schema name, all the schemas available in the database are listed. To read from or write to Oracle public synonyms, enter PUBLIC.
JDBC Driver Class Name	Name of the JDBC driver class. To connect to Aurora PostgreSQL, specify the following driver class name: org.postgresql.Driver For more information about which driver class to use with specific databases, see the corresponding third-party vendor documentation.
Connection String	Connection string to connect to the database. Use the following format to specify the connection string: <code>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</code> For example, the connection string for the Aurora PostgreSQL database type is <code>jdbc:postgresql://&lt;host&gt;:&lt;port&gt;[/dbname]</code> . For more information about the connection string to use with specific drivers, see the corresponding third-party vendor documentation.

Property	Description
Additional Security Properties	<p>Masks sensitive and confidential data of the connection string that you don't want to display in the session log.</p> <p>Specify the part of the connection string that you want to mask.</p> <p>When you create a connection, the string you enter in this field appends to the string that you specified in the <b>Connection String</b> field.</p>
Database Type	<p>The database type to which you want to connect.</p> <p>You can select one of the following database types:</p> <ul style="list-style-type: none"> <li>- PostgreSQL. Connect to the Aurora PostgreSQL database hosted in the Amazon Web Services or the Microsoft Azure environment.</li> <li>- Azure SQL Database. Connect to Azure SQL Database hosted in the Microsoft Azure environment.</li> <li>- Others. Connect to any database that supports the Type 4 JDBC driver.</li> </ul> <p>Default is Others.</p>
Enable Auto Commit <sup>1</sup>	<p>Specifies whether the driver supports connections to automatically commit data to the database when you run an SQL statement.</p> <p>When disabled, the driver does not support connections to automatically commit data even if the auto-commit mode is enabled in the JDBC driver.</p> <p>Default is disabled.</p>
Support Mixed-Case Identifiers	<p>Indicates whether the database supports case-sensitive identifiers.</p> <p>When enabled, the Secure Agent encloses all identifiers within the character selected for the SQL Identifier Character property.</p> <p>Default is disabled.</p>
SQL Identifier Character	<p>Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type.</p> <p>Select <b>None</b> if the database uses regular identifiers. When the Secure Agent generates SQL queries, it does not place delimited characters around any identifiers.</p> <p>Select a character if the database uses delimited identifiers. When the Secure Agent generates SQL queries, it encloses delimited identifiers within this character.</p>
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## JD Edwards EnterpriseOne connection properties

When you set up a JD Edwards EnterpriseOne connection, you must configure the connection properties.

The following table describes the JD Edwards EnterpriseOne connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Host Name	JD Edwards EnterpriseOne server host name.

Property	Description
Enterprise Port	JD Edwards EnterpriseOne server port number. Default is 6016.
User Name	The JD Edwards EnterpriseOne database user name.
Password	The password for the JD Edwards EnterpriseOne database user.
Environment	Name of the JD Edwards EnterpriseOne environment you want to connect to.
Role	Role of the JD Edwards EnterpriseOne user. Default is *ALL.
User Name	The JD Edwards EnterpriseOne database user name.
Password	Password for the database user.
Driver Class Name	<p>The driver class name that you can enter for the applicable database type. Required to write data in bulk with the interface table write option. Use the following JDBC driver class name:</p> <ul style="list-style-type: none"> <li>- DataDirect JDBC driver class name for Oracle: <code>com.informatica.jdbc.oracle.OracleDriver</code></li> <li>- DataDirect JDBC driver class name for IBM DB2: <code>com.informatica.jdbc.db2.DB2Driver</code></li> <li>- DataDirect JDBC driver class name for Microsoft SQL Server: <code>com.informatica.jdbc.sqlserver.SQLServerDriver</code></li> </ul> <p>For more information about which driver class to use with specific databases, see the vendor documentation.</p>
Connection String	<p>The connection string to connect to the database. Required to write data in bulk with the interface table write option.</p> <p>The JDBC connection string uses the following syntax:</p> <ul style="list-style-type: none"> <li>- For Oracle: <code>jdbc:informatica:oracle://&lt;host name&gt;:&lt;port&gt;,ServiceName=&lt;db service name&gt;</code></li> <li>- For DB2: <code>jdbc:informatica:db2://&lt;host name&gt;:&lt;port&gt;;databaseName=&lt;db name&gt;</code></li> <li>- For Microsoft SQL: <code>jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port&gt;;databaseName=&lt;db name&gt;</code></li> </ul>
JDE Product Code	<p>The product code for the tables and views in JD Edwards EnterpriseOne.</p> <p><b>Note:</b> You must specify only the product code without the description. If you specify a schema that is not valid, a java exception appears.</p>

# JIRA connection properties

When you set up a JIRA connection, configure the connection properties.

The following table describes the JIRA connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The JIRA connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	User name of the JIRA account.
Password	The API token for the JIRA account. For more information on how to create an API token, see Knowledge Base article <a href="#">KB 576517</a> .
URI	The base JIRA URI of JIRA instance to connect. For example, https://<abcd>.atlassian.net/ .
UTC Offset	Select UTC time offset to be appended with datetime field. Default is UTC.
Enable Logging	Enables logging for the task.

# JIRA Cloud connection properties

When you set up a JIRA Cloud connection, you must configure the connection properties.

The following table describes the JIRA Cloud connection properties:

Connection property	Description
Connection Name	Name of the JIRA Cloud connection.
Description	Description of the JIRA Cloud connection.
Type	Type of connection. Select JiraCloud (Informatica) from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent.
Authentication	Authentication type for the connection. Select JiraCloud.

Connection property	Description
URI	The base JIRA URI of JIRA instance to connect. For example, <code>https://abcd.atlassian.net</code> .
Username	User name for the JIRA account.
Password	The API token for the JIRA account. For more information on how to create an API token, see <a href="https://kb.informatica.com/solution/23/Pages/70/576517.aspx">https://kb.informatica.com/solution/23/Pages/70/576517.aspx</a> .

## JMS connection properties

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

The following table describes the connection properties for the JMS connection:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identify the connection. The description cannot exceed 4,000 characters.
Type	The JMS connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Connection URL	URL of the JNDI naming provider. For example, in IBM MQ it is the directory location that contains the .bindings file.
JNDI User Name	Optional. User name to connect to the JNDI context factory.
JNDI Password	Optional. The password of the user account that you use to connect to the JNDI context factory.
JNDI Context Factory	The JMS provider specific initial JNDI context factory implementation for connecting to the JNDI service. This value is a fully qualified class name of the Initial Context Factory. For example, the class name of the Initial Context Factory for ActiveMQ is <code>org.apache.activemq.jndi.ActiveMQInitialContextFactory</code> For more information, see the documentation of the JMS provider.

Property	Description
JNDI Package Prefixes	A colon-delimited list of package prefixes to use when loading URL context factories. These are the package prefixes for the name of the factory class that will create a URL context factory. For more information about the values, see the documentation of the JMS provider.
JMS Connection Factory	The name of the object in the JNDI server that enables the JMS Client to create JMS connections. For example, <code>jms/QCF</code> or <code>jmsSalesSystem</code> .
JMS Connection User Name	Optional. User name to connect to the JMS connection factory.
JMS Connection Password	Optional. The password of the user account that you use to connect to the JMS connection factory.

**Note:** Ensure to copy the external JMS JAR files to the following location:

`<Secure_Agent_home>/ext/connectors/thirdparty/infa.jms`

After copying the external JMS JAR files, restart the Secure Agent.

## JSON Target connection properties

When you create a JSON Target connection, you must configure the connection properties.

The following table describes the JSON Target connection properties:

Connection property	Description
Secure Agent	Select the appropriate Secure Agent from the list.
Sample JSON Schema Name	Enter sample JSON file path. For example, <code>ABCD.JSON</code> .
JSON Working Directory	Enter the folder path for JSON working directory.
Final JSON File Name	Enter final JSON file path with the file name.
Requires JSON Customization	Allows JSON customization. Default is <b>NO</b> .
Final Customized JSON File Name	Enter final customized JSON file path with the file name.

# Kafka connection properties

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

The following table describes the Kafka connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>The name is not case sensitive. It must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <p>~ ` ! \$ % ^ &amp; * ( ) - + = { [ ] }   \ : ; " ' &lt; , &gt; . ? /</p>
Description	<p>Optional. Description that you use to identity the connection.</p> <p>The description cannot exceed 4,000 characters.</p>
Type	<p>The Kafka connection type.</p> <p>If you do not see the connection type, go to the <b>Add-On Connectors</b> page in Administrator to install the connector.</p>
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>Specify a Secure Agent or a serverless runtime environment for a mapping that runs on the advanced cluster.</p>
Kafka Broker List	<p>Comma-separated list of the Kafka brokers.</p> <p>To list a Kafka broker, use the following format:</p> <p><code>&lt;HostName&gt;:&lt;PortNumber&gt;</code></p> <p><b>Note:</b> When you connect to a Kafka broker over SSL, you must specify the fully qualified domain name for the host name. Otherwise, the test connection fails with SSL handshake error.</p>
Retry Timeout	<p>Optional. Number of seconds after which the Secure Agent attempts to reconnect to the Kafka broker to read or write data.</p> <p>Default is 180 seconds.</p> <p>This property is not used by Mass Ingestion Databases. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
Kafka Broker Version	<p>Kafka message broker version. The only valid value is Apache 0.10.1.1 and above.</p> <p>Optional for a streaming ingestion task.</p>
Additional Connection Properties	<p>Optional. Comma-separated list of additional configuration properties of the Kafka producer or consumer.</p> <p>For a streaming ingestion task, ensure that you set the <code>&lt;kerberos name&gt;</code> property if you configure <code>&lt;Security Protocol&gt;</code> as SASL_PLAINTEXT or SASL_SSL.</p>

Property	Description
Schema Registry URL	<p>Location and port of the Confluent schema registry service to access Avro sources and targets in Kafka.</p> <p>To list a schema registry URL, use the following format:</p> <pre>&lt;https&gt;://&lt;HostName or IP&gt;:&lt;PortNumber&gt;</pre> <p>or</p> <pre>&lt;http&gt;://&lt;HostName or IP&gt;:&lt;PortNumber&gt;</pre> <p>Example for the schema registry URL:</p> <pre>https://kafkarnd.informatica.com:8082</pre> <p>or</p> <pre>http://10.65.146.181:8084</pre> <p>Applies only when you import a Kafka topic in Avro format that uses the Confluent schema registry to store the metadata.</p> <p>This property is not used by Mass Ingestion Databases. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
SSL Mode	<p>Required. Determines the encryption type to use for the connection.</p> <p>You can choose a mode from the following SSL modes:</p> <ul style="list-style-type: none"> <li>- Disabled. Establishes an unencrypted connection to the Kafka broker.</li> <li>- One-way. Establishes an encrypted connection to the Kafka broker using truststore file and truststore password.</li> <li>- Two-way. Establishes an encrypted connection to the Kafka broker using truststore file, truststore password, keystore file, and keystore password.</li> </ul> <p>This property is not used by Mass Ingestion Databases. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
SSL TrustStore File Path	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Absolute path and file name of the SSL truststore file that contains the SSL certificate to connect to the Kafka broker.</p>
SSL TrustStore Password	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Password for the SSL truststore.</p>
SSL KeyStore File Path	<p>Required when you use the two-way SSL mode.</p> <p>Absolute path and file name of the SSL keystore file that contains private keys and certificates to connect to the Kafka broker.</p>
SSL KeyStore Password	<p>Required when you use the two-way SSL mode.</p> <p>Password for the SSL keystore.</p>
Additional Security Properties	<p>Optional. Comma-separated list of additional configuration properties to connect to the Kafka broker in a secure way.</p> <p>If you specify two different values for the same property in <b>Additional Connection Properties</b> and <b>Additional Security Properties</b>, the value in <b>Additional Security Properties</b> overrides the value in <b>Additional Connection Properties</b>.</p> <p>This property is not used by Mass Ingestion Databases.</p>

## Schema Registry Security Configuration Properties

When you configure the **Schema Registry URL** connection property, you can configure the schema registry security configuration properties. You can configure one-way SSL, two-way SSL, and basic authentication to connect to the Confluent schema registry in a secure way.

The following table describes the security properties for the Kafka connection when you use the Confluent schema registry:

Property	Description
SSL Mode Schema Registry <sup>1</sup>	<p>Required. Determines the encryption type to use for the connection.</p> <p>You can choose a mode from the following SSL modes:</p> <ul style="list-style-type: none"> <li>- Disabled. Establishes an unencrypted connection to the Confluent schema registry.</li> <li>- One-way. Establishes an encrypted connection to the Confluent schema registry using truststore file and truststore password.</li> <li>- Two-way. Establishes an encrypted connection to the Confluent schema registry using truststore file, truststore password, keystore file, and keystore password.</li> </ul> <p>This property is not used by Mass Ingestion Databases. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
SSL TrustStore File Path Schema Registry <sup>1</sup>	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Absolute path and file name of the SSL truststore file that contains the SSL certificate to connect to the Confluent schema registry.</p>
SSL TrustStore Password Schema Registry <sup>1</sup>	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Password for the SSL truststore.</p>
SSL KeyStore File Path Schema Registry <sup>1</sup>	<p>Required when you use the two-way SSL mode.</p> <p>Absolute path and file name of the SSL keystore file that contains private keys and certificates to connect to the Confluent schema registry.</p>
SSL KeyStore Password Schema Registry <sup>1</sup>	<p>Required when you use the two-way SSL mode.</p> <p>Password for the SSL keystore.</p>
Additional Security Properties Schema Registry	<p>Optional. Comma-separated list of additional security properties to connect to the Confluent schema registry in a secure way.</p> <p>For example, when you configure basic authentication to establish a secure communication with Confluent schema registry, specify the following value:</p> <pre>basic.auth.credentials.source=USER_INFO,basic.auth.user.info=&lt;username&gt;:&lt;password&gt;</pre> <p>If you specify two different values for the same property in <b>Additional Connection Properties</b> and <b>Additional Security Properties Schema Registry</b>, the value in <b>Additional Security Properties Schema Registry</b> overrides the value in <b>Additional Connection Properties</b>.</p> <p>This property is not used by Mass Ingestion Databases.</p>
<sup>1</sup> Does not apply to mappings.	

# LDAP connection properties

When you set up an LDAP connection, you must configure the connection properties.

The following table describes the LDAP connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks. <b>Note:</b> You can specify only the Secure Agent as the run-time environment for an LDAP connection.
Host Name	Required. LDAP directory server host name. You can use the LDAP or LDAPS protocol to connect to LDAP Server. <ul style="list-style-type: none"><li>- To use the LDAP protocol, use one of the following formats:<ul style="list-style-type: none"><li>- <code>ldap://&lt;hostname&gt;</code></li><li>- <code>&lt;hostname&gt;</code></li></ul></li><li>- To use the LDAPS protocol, use the <code>ldaps://&lt;hostname&gt;</code> format.</li></ul> <b>Note:</b> If you use SSL, use the host name that you specify in the SSL certificate.
Port	Required. LDAP directory server port number. Default is 389.
Anonymous Connection	Establishes an anonymous connection with the LDAP directory server. Select anonymous connection to access a directory server as an anonymous user without authentication. <b>Note:</b> You cannot establish an anonymous connection with Active Directory.
User Name	The LDAP user name to connect to the LDAP directory server. Required if you want to connect to Active Directory.
Password	The password to connect to the LDAP directory server. If you do not enter the password, the Client establishes an anonymous connection. Required if you want to connect to Active Directory.
Secure Connection	Establishes a secure connection with the LDAP directory server through the TLS protocol.
TrustStore File Name	The file name of the truststore that contains the TLS certificate to establish a one-way secure connection with the LDAP directory server. Contact the LDAP Administrator for the truststore file name and password.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Name	The file name of the keystore that contains the keys and certificates required to establish a two-way secure communication with the LDAP directory server. Contact the LDAP Administrator for the keystore file name and password.
KeyStore Password	The password for the keystore file required for secure communication.
Base DN	Required. The distinguished name (DN) of the root directory in the LDAP directory server. For example, use the following base DN to connect to the Informatica domain: <code>dc=informatica-connector,dc=com</code> If you do not specify the base DN, the Secure Agent fails to fetch the metadata.

## Litmos connection properties

When you create a Litmos connection, you must configure the connection properties.

The following table describes the Litmos connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
apikey	The API key from the account owner's profile.
source	The source from account owner's profile.
pageSize	The page size for the read operation. Default value is 100.
baseURI	Specify the endpoint URI to connect to the Litmos APIs. For example, <i>https://api.litmos.com/v1.sv</i> .
apiLimit	The number of API calls in a minute. Default value is 100.
waittime	The waiting time to re-attempt an API call after the number of calls to the Litmos API exceeds the API limit.

## Marketo V3 connection properties

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

The following table describes the Marketo V3 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Marketo V3 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure agent, Hosted Agent, or serverless runtime environment.
client_ID	The client ID of the custom service required to generate a valid access token.
client_secret	The client secret of the Marketo custom service required to generate a valid access token.

Property	Description
grant_type	The access permissions for an administrator to invoke the Marketo REST APIs to read data from and write data to Marketo. Marketo supports only the client_credentials grant type.
REST API URL	The URL with which the Secure agent connects to the Marketo REST APIs. The URL has the following format: https://<Host name of the Marketo Rest API Server>. Contact the Marketo Administrator for the REST API URL.
Bypass Proxy	The option to use the proxy server settings defined in the proxy.ini file or use the Secure agent manager to connect to Marketo. When you select Bypass Proxy, you connect to Marketo using the Secure agent manager. When you clear Bypass Proxy, you connect to Marketo using the proxy server. Default is Bypass Proxy. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.

## Microsoft Access connection properties

When you set up a Microsoft Access connection, you must configure the connection properties.

The following table describes the connection properties:

Connection property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Data Source Name	System DSN name.
Code Page	The code page compatible with the Microsoft Access source. Select one of the following code pages: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode and non-Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>

# Microsoft Azure Blob Storage V2 connection properties

When you create a Microsoft Azure Blob Storage V2 connection, you must configure the connection properties.

The following table describes Microsoft Azure Blob Storage V2 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Account Name	Microsoft Azure Blob Storage account name.
Account Key	Microsoft Azure Blob Storage access key.
Container Name	Microsoft Azure Blob Storage container name.

# Microsoft Azure Blob Storage V3 connection properties

When you set up a Microsoft Azure Blob Storage V3 connection, configure the connection properties.

The following table describes the Microsoft Azure Blob Storage V3 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Azure Blob Storage V3 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Account Name	Microsoft Azure Blob Storage account name.
Authentication Type	Authentication type to access the Microsoft Azure Blob Storage account. Select one of the following options: <ul style="list-style-type: none"><li>- Shared Key Authentication. Uses the account key to connect to Microsoft Azure Blob Storage.</li><li>- Shared Access Signature. Uses the SAS token to connect to Microsoft Azure Blob Storage. Use the SAS token to grant access to the resources in the storage account or container for a specific time range without sharing the account key.</li></ul>

Property	Description
Account Key	Applies to shared key authentication. The account key for the Microsoft Azure Blob Storage account.
SAS Token	Applies to shared access signature. The shared access signature token generated in the Azure portal.
Container Name	Microsoft Azure Blob Storage container name.
Endpoint Suffix	Type of Microsoft Azure endpoints. Select one of the following options: <ul style="list-style-type: none"> <li>- core.windows.net. Connects to Azure endpoints.</li> <li>- core.usgovcloudapi.net. Connects to Azure Government endpoints.</li> <li>- core.chinacloudapi.cn. Not applicable.</li> </ul> Default is core.windows.net.

## Microsoft Azure Cosmos DB SQL API connection properties

When you set up a Microsoft Azure Cosmos DB SQL API connection, configure the connection properties.

The following table describes the Microsoft Azure Cosmos DB SQL API connection properties:

Connection 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Azure Cosmos DB SQL API connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode.
Cosmos DB URI	The URI of Microsoft Azure Cosmos DB account.
Key	The primary or secondary key that provides you with the complete administrative access to the resources within the Microsoft Azure Cosmos DB account.
Database	Name of the database that contains the collections from which you want to read or write JSON documents.

# Microsoft Azure Data Lake Storage Gen1 V2 connection properties

When you set up a Microsoft Azure Data Lake Storage Gen1 V2 connection, you must configure the connection properties.

The following table describes the Microsoft Azure Data Lake Storage Gen1 V2 connection properties:

Connection property	Description
Connection Name	Name of the Microsoft Azure Data Lake Storage Gen1 V2 connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Microsoft Azure Data Lake Storage Gen1 V2 connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
ADLS Account Name	The name of the Microsoft Azure Data Lake Storage Gen1 account.
ClientID	The ID of your application to complete the OAuth Authentication in the Active Directory.
Client Secret	The client secret key to complete the OAuth Authentication in the Active Directory.
Directory	The Microsoft Azure Data Lake Storage Gen1 directory that you use to read data or write data. The default is root directory.
AuthEndpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and Client secret is completed.

For more information on creating a client ID, a client secret, and an AuthEndpoint, see *Microsoft Azure Data Lake Storage Gen1 Documentation*.

# Microsoft Azure Data Lake Storage Gen1 V3 connection properties

When you set up a Microsoft Azure Data Lake Storage Gen1 V3 connection, you must configure the connection properties.

The following table describes the Microsoft Azure Data Lake Storage Gen1 V3 connection properties:

Connection property	Description
Connection Name	Name of the Microsoft Azure Data Lake Storage Gen1 V3 connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Microsoft Azure Data Lake Storage Gen1 V3 connection.

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
ADLS Account Name	The name of the Microsoft Azure Data Lake Storage Gen1 account.
Client Id	The ID of your application to complete the OAuth Authentication in the Active Directory.
Client Secret	The client secret key to complete the OAuth Authentication in the Active Directory.
Directory	The Microsoft Azure Data Lake Storage Gen1 directory that you use to read data or write data. The default is root directory.
AuthEndpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and Client secret is completed.
Show Subfolders	Enable subfolders to import objects from the subfolders of the specified directory.

For more information on creating a client ID, a client secret, and an AuthEndpoint, see *Microsoft Azure Data Lake Store Documentation*.

## Microsoft Azure Data Lake Storage Gen2 connection properties

When you set up a Microsoft Azure Data Lake Storage Gen2 connection, configure the connection properties.

The following table describes the Microsoft Azure Data Lake Storage Gen2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Azure Data Lake Storage Gen2 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode. You cannot run a database ingestion or streaming ingestion task on a Hosted Agent or serverless runtime environment.
Account Name	Microsoft Azure Data Lake Storage Gen2 account name or the service name.

Property	Description
Authentication Type	<p>Authentication type to access the Microsoft Azure Data Lake Storage Gen2 account.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Service Principal Authentication. Uses the client ID, client secret, and tenant ID to connect to Microsoft Azure Data Lake Storage Gen2.</li> <li>- Shared Key Authentication. Uses the account key to connect to Microsoft Azure Data Lake Storage Gen2.</li> <li>- Managed Identity Authentication. Select to authenticate using identities that are assigned to applications in Azure to access Azure resources in Microsoft Azure Data Lake Storage Gen2.</li> </ul> <p><b>Note:</b> Mass Ingestion Streaming does not support shared key authentication or managed identity authentication.</p>
Client ID	<p>Applies to Service Principal Authentication and Managed Identity Authentication.</p> <p>The client ID of your application.</p> <p>To use service principal authentication, specify the application ID or client ID for your application registered in the Azure Active Directory.</p> <p>To use managed identity authentication, specify the client ID for the user-assigned managed identity. If the permission is provided by system-assigned managed identity, leave the field empty. If there is no system-assigned identity but only a single user-assigned managed identity, you may also leave the field empty.</p>
Client Secret	<p>Applies to Service Principal Authentication.</p> <p>The client secret key to complete the OAuth authentication in the Azure Active Directory.</p>
Tenant ID	<p>Applies to Service Principal Authentication.</p> <p>The directory ID of the Azure Active Directory.</p>
Account Key	<p>Applies to Shared Key Authentication.</p> <p>The account key for the Microsoft Azure Data Lake Storage Gen2 account.</p>
File System Name	<p>The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.</p>
Directory Path	<p>The path of an existing directory without the file system name.</p> <p>You can select one of the following syntax:</p> <ul style="list-style-type: none"> <li>- / for root directory</li> <li>- /dir1</li> <li>- dir1/dir2</li> </ul> <p>There is no default directory.</p>
Adls Gen2 End-point	<p>The type of Microsoft Azure endpoints.</p> <p>Select one of the following endpoints:</p> <ul style="list-style-type: none"> <li>- core.windows.net. Connects to Azure endpoints.</li> <li>- core.usgovcloudapi.net. Connects to US government Microsoft Azure Data Lake storage Gen2 endpoints.</li> <li>- core.chinacloudapi.cn. Connects to Microsoft Azure Data Lake storage Gen2 endpoints in the China region.</li> </ul> <p>Default is core.windows.net.</p> <p><b>Note:</b> You cannot configure the Azure Government endpoints for mappings in advanced mode.</p>

# Microsoft Azure Event Hub connection properties

When you set up an Azure Event Hub connection, you must configure the connection properties.

The following table describes the Azure Event Hub connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive. It must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ } ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you use to identify the connection. The description cannot exceed 4,000 characters.
Type	The Azure Event Hub connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page in Administrator to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Tenant ID	The ID of the tenant that the data belongs to. This ID is the Directory ID of the Azure Active Directory.
Subscription ID	The ID of the Azure subscription.
Resource Group Name	The name of the Azure resource group associated with the Event Hub namespace.
Client Application ID	The ID of the application created under the Azure Active Directory.
Client Secret Key	The secret key generated for the application.
Event Hub Namespace	The name of the Event Hub namespace that is associated with the resource group name.
Shared Access Policy Name	Optional. The name of the Event Hub Namespace Shared Access Policy. The policy must apply to all data objects that are associated with this connection. To read from Event Hubs, you must have Listen permission. To write to an Event Hub, the policy must have Send permission.
Shared Access Policy Primary Key	Optional. The primary key of the Event Hub Namespace Shared Access Policy.

# Microsoft Azure SQL Data Warehouse - Database Ingestion connection properties

When you define a Microsoft Azure SQL Data Warehouse Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion tasks, which you configure in the Mass Ingestion service.

**Note:** Some properties are for Microsoft Azure Data Lake Storage Gen1. Mass Ingestion Databases uses Microsoft Azure Data Lake Storage Gen1 to stage data in files before sending the data to the Microsoft Azure SQL Database Warehouse target tables.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that you select the type for Microsoft Azure SQL Data Warehouse - Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
Azure DW JDBC URL	<p>The Microsoft Azure SQL Data Warehouse JDBC connection string.</p> <p>Example connection string for Microsoft SQL Server authentication:</p> <pre>jdbc:sqlserver://server.database.windows.net:1433;database=database</pre> <p>Example connection string for Azure Active Directory (AAD) authentication:</p> <pre>jdbc:sqlserver://server.database.windows.net:1433;database=database;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;</pre> <p><b>Note:</b> The default authentication type is Microsoft SQL Server authentication.</p>
Azure DW JDBC Username	The user name to use for connecting to the Microsoft Azure SQL Data Warehouse account. Provide the AAD user name for AAD authentication.
Azure DW JDBC Password	The password to use for connecting to the Microsoft Azure SQL Data Warehouse account.
Azure DW Schema Name	The name of the schema in the Microsoft Azure SQL Data Warehouse target.
ADLS Account Name	The name of the Microsoft Azure Data Lake Storage Gen1 account.
Client Id	The ID of your client application for completing the OAuth Authentication in the Active Directory.
Client Secret	The client secret key for completing the OAuth Authentication in the Active Directory.

Property	Description
Directory	A Microsoft Azure Data Lake Storage Gen1 directory that Mass Ingestion Databases uses to stage data in files. The default is the root directory.
AuthEndpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and Client secret is completed.

## Microsoft Azure SQL Data Warehouse V2 connection properties

The following table describes Microsoft Azure SQL Data Warehouse V2 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Azure DW JDBC URL	<p>Microsoft Azure Data Warehouse JDBC connection string.</p> <p>Example for Microsoft SQL Server authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433;database=&lt;Database&gt;</pre> <p>Example for Azure Active Directory (AAD) authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p>The default authentication is Microsoft SQL Server authentication.</p>
Azure DW JDBC Username	User name to connect to the Microsoft Azure SQL Data Warehouse account. Provide AAD user name for AAD authentication.
Azure DW JDBC Password	Password to connect to the Microsoft Azure SQL Data Warehouse account.
Azure DW Schema Name	Name of the schema in Microsoft Azure SQL Data Warehouse.
Azure Blob Account Name	Name of the Microsoft Azure Storage account to stage the files.
Azure Blob Account Key	Microsoft Azure Storage access key to stage the files.

# Microsoft Azure Synapse SQL connection properties

When you set up a Microsoft Azure Synapse SQL connection, configure the connection properties.

The following table describes the Microsoft Azure Synapse SQL connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Azure Synapse SQL connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode.
Azure DW JDBC URL	<p>The Microsoft Azure Synapse SQL JDBC connection string.</p> <p>Enter the connection string in the following format for Microsoft SQL Server authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;</pre> <p>Enter the connection string in the following format for Azure Active Directory (AAD) authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p>Enter the connection string in the following format for Managed Identity authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;Authentication=ActiveDirectoryMsi;</pre> <p>When you connect to a serverless SQL pool, replace &lt;Server&gt;.database.windows.net:1433 with &lt;Serverless SQL endpoint&gt;:1433 in the connection string for all authentication types.</p> <p>For example,</p> <pre>jdbc:sqlserver://&lt;Serverless SQL endpoint&gt;:1433; database=&lt;Database&gt;;authentication=ActiveDirectoryMsi;</pre> <p>Default is Microsoft SQL Server authentication.</p>
Azure DW JDBC Username	User name to connect to the Microsoft Azure Synapse SQL account. Provide AAD user name for AAD authentication.
Azure DW JDBC Password	Password to connect to the Microsoft Azure Synapse SQL account.
Azure DW Schema Name	Name of the schema in Microsoft Azure Synapse SQL.
Azure DW Client ID	Required if you want to use the user-assigned managed identity for Managed Identity Authentication to connect to Microsoft Azure Synapse SQL. The client ID of the user-assigned managed identity. If the managed identity is system-assigned, leave the field empty.

Property	Description
External Data Source	<p>The name of the external data source that is used to create the external table.</p> <p>Ensure that the external data source exists in Microsoft Azure Synapse SQL and you have the permission to access the external data source.</p> <p>Do not specify the external data source when you use the copy command method to load data from the staging location to Microsoft Azure Synapse SQL.</p> <p>When you run a mapping in advanced mode, you must specify the container or file system used to create the external data source either in the connection properties or in the advanced properties.</p>
Azure Storage Type	<p>Type of Azure storage to stage the files.</p> <p>Select one of the following storage types:</p> <ul style="list-style-type: none"> <li>- Azure Blob. Uses Microsoft Azure Blob Storage to stage the files.</li> <li>- ADLS Gen2. Uses Microsoft Azure Data Lake Storage Gen2 to stage the files.</li> </ul> <p>Default is Azure Blob.</p> <p><b>Note:</b> You cannot select Azure Blob storage type when you connect to a serverless SQL pool.</p>
Authentication Type	<p>Authentication type to connect to Azure storage to stage the files.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Shared Key Authentication. Uses the account name and account key to connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2.</li> <li>- Service Principal Authentication. Applies to Microsoft Azure Data Lake Storage Gen2. Uses the client ID, client secret, and tenant ID to connect to Microsoft Azure Data Lake Storage Gen2. To use Service Principal authentication, register an application in the Azure Active Directory, generate a client secret, and then assign the Storage Blob Contributor role to the application.</li> <li>- Managed Identity Authentication. Applies to Microsoft Azure Data Lake Storage Gen2. Select to authenticate using identities that are assigned to applications in Azure to access Azure resources in Microsoft Azure Data Lake Storage Gen2.</li> </ul> <p><b>Note:</b> You cannot select shared key authentication type when you connect to a serverless SQL pool.</p> <p>In a file ingestion task, if you select Microsoft Azure Synapse SQL with Managed Identity authentication type as the target, then you must select Microsoft Azure Data Lake Storage Gen2 as the source.</p>
Azure Blob Account Name	<p>Applies to Shared Key Authentication for Microsoft Azure Blob Storage.</p> <p>Name of the Microsoft Azure Blob Storage account to stage the files.</p> <p>Doesn't apply to a serverless SQL pool.</p>
Azure Blob Account Key	<p>Applies to Shared Key Authentication for Microsoft Azure Blob Storage.</p> <p>The Microsoft Azure Blob Storage access key to stage the files.</p> <p>Doesn't apply to a serverless SQL pool.</p>
Container Name	<p>Applies to Microsoft Azure Blob Storage.</p> <p>The name of the container in the Azure Blob Storage account.</p> <p>Doesn't apply to a serverless SQL pool.</p>
ADLS Gen2 Storage Account Name	<p>Applies to Shared Key Authentication and Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2.</p> <p>Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.</p>
ADLS Gen2 Account Key	<p>Applies to Shared Key Authentication for Microsoft Azure Data Lake Storage Gen2.</p> <p>The Microsoft Azure Data Lake Storage Gen2 access key to stage the files.</p> <p>Doesn't apply to a serverless SQL pool.</p>

Property	Description
Client ID	<p>Applies to Service Principal Authentication and Managed Identity Authentication for Microsoft Azure Data Lake Storage Gen2.</p> <p>The client ID of your application.</p> <p>To use service principal authentication, enter the application ID or client ID for your application registered in the Azure Active Directory.</p> <p>To use managed identity authentication, enter the client ID for the user-assigned managed identity. If the managed identity is system-assigned, leave the field empty.</p>
Client Secret	<p>Applies to Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2.</p> <p>The client secret for your application.</p>
Tenant ID	<p>Applies to Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2.</p> <p>The directory ID or tenant ID for your application.</p>
File System Name	<p>Applies to Microsoft Azure Data Lake Storage Gen2.</p> <p>The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.</p>
Blob End-point	<p>Type of Microsoft Azure endpoints.</p> <p>Select one of the following endpoints:</p> <ul style="list-style-type: none"> <li>- core.windows.net. Connects to Azure endpoints.</li> <li>- core.usgovcloudapi.net. Connects to US Government Microsoft Azure Synapse SQL endpoints. Doesn't apply to a serverless SQL pool.</li> <li>- core.chinacloudapi.cn. Connects to Microsoft Azure Synapse SQL endpoints in the China region. Doesn't apply to a serverless SQL pool.</li> </ul> <p>Default is core.windows.net.</p>
VNet Rule	<p>Enable to connect to a Microsoft Azure Synapse SQL endpoint residing in a virtual network (VNet).</p> <p>When you use a serverless runtime environment, you cannot connect to a Microsoft Azure Synapse SQL endpoint residing in a virtual network.</p>

## Microsoft Azure Synapse Analytics Database Ingestion connection properties

When you define a Microsoft Azure Synapse Analytics Database Ingestion connection, you must configure connection properties. You can use this connection type in application ingestion tasks and database ingestion tasks, which you configure in the Mass Ingestion service.

**Note:** Some properties are for Microsoft Azure Data Lake Storage Gen2. Mass Ingestion Applications and Mass Ingestion Databases use Microsoft Azure Data Lake Storage Gen2 to stage data in files before sending the data to the Microsoft Azure Synapse Analytics target tables.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is for Microsoft Azure Synapse Analytics - Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run the application ingestion tasks or database ingestion tasks. You define runtime environments in Administrator. <b>Note:</b> You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.
Azure Synapse Analytics JDBC URL	The Microsoft Azure Synapse Analytics (formerly SQL Data Warehouse) JDBC connection string. Example connection string for Microsoft SQL Server authentication: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database</code> Example connection string for Azure Active Directory (AAD) authentication: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;</code> <b>Note:</b> The default authentication type is Microsoft SQL Server authentication.
Azure Synapse Analytics JDBC Username	The user name to use for connecting to the Microsoft Azure Synapse Analytics account. Provide the AAD user name for AAD authentication.
Azure Synapse Analytics JDBC Password	The password to use for connecting to the Microsoft Azure Synapse Analytics account.
Azure Synapse Analytics Schema Name	The name of the schema in the Microsoft Azure Synapse Analytics target.
ADLS Gen2 Account Name	The name of the Microsoft Azure Data Lake Storage Gen2 account.
Client Id	The ID of your client application for completing the OAuth Authentication in the Active Directory.
Client Secret	The client secret key for completing the OAuth Authentication in the Active Directory.
Directory	The Microsoft Azure Data Lake Storage Gen2 directory that Mass Ingestion Applications and Mass Ingestion Databases uses to stage data in files. The default is the root directory.
Filesystem Name	The name of an existing file system in the Microsoft Azure Data Lake Storage Gen2 account.
Tenant ID	The Directory ID of the Azure Active Directory.

# Microsoft CDM Folders V2 connection properties

When you set up a Microsoft CDM Folders V2 connection, configure the connection properties.

The following table describes the Microsoft CDM Folders V2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft CDM Folders V2 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
ADLSGen2 Storage Account Name	Name of the ADLS Gen2 storage account.
Azure AD App Client ID	The client ID of the Azure Active Directory account to authenticate user access to the storage account. You can get the application ID from the Microsoft Azure Active Directory administrator.
Azure AD App Client Secret	The client secret key of the Azure Active Directory application to authenticate access to the storage account. You can get the key value from the Microsoft Azure Active Directory administrator.
Azure Tenant ID	The tenant ID of the Azure Active Directory account to authenticate user access to the storage account. You can get the directory ID from the Microsoft Azure Active Directory administrator.
ADLSGen2 File System Name	The name of the file system that you create in the Azure Storage Explorer application. A file system can contain more than one common data model folders.
CDM Folder Path	The path of the common data model folder that you create within the file system. You can use the following values for CDM folder path: - / - /folder1 - /folder1/folder2 The recommended CDM folder path is /folder1. Default is empty.
Adls Gen2 End-point	The ADLS Gen2 endpoint core.windows.net.

# Microsoft Dynamics 365 for Operations connection properties

When you set up a Microsoft Dynamics 365 for Operations connection, configure the connection properties.

The following table describes the Microsoft Dynamics 365 for Operations connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Dynamics 365 for Operations connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication Type	The authentication method that the connector must use to login to the web application. Select one of the following authentication types: <ul style="list-style-type: none"><li>- OAuth 2.0. Requires the service URL, username, password, and application ID.</li><li>- OAuth 2.0 Client Secret Grant. Requires the service URL, application ID, tenant ID, and client secret.</li><li>- OAuth 2.0 Client Certificate Grant. Requires the keystore file, keystore password, key alias and key password. Not applicable.</li></ul>
Service URL	Enter the URL of the Microsoft Dynamics 365 for Operations service in the following format: <code>https:&lt;server name&gt;:&lt;port number&gt;</code> or <code>http:&lt;server name&gt;:&lt;port number&gt;</code> If you don't specify the port number in the URL, the agent uses port number 443 in the query.
Username	The user name to connect to Microsoft Dynamics 365 for Operations account.
Password	The password to connect to Microsoft Dynamics 365 for Operations account.
Application ID	The native application ID for Microsoft Dynamics 365 for Operations.
Tenant ID	The directory ID for Azure Active Directory.
Client Secret	The client secret for the Microsoft Dynamics 365 for Operations account.
Retry Error Codes	The comma-separated http error codes for which the retries are made.
Retry Count	The number of retries to get the response from an endpoint based on the retry interval. Default is 0.
Retry Interval	The time in seconds to wait before Microsoft Dynamics 365 for Operations Connector retries for a response. Default is 60 seconds.

# Microsoft Dynamics 365 for Sales connection properties

When you set up a Microsoft Dynamics 365 for Sales connection, configure the connection properties.

The following table describes the Microsoft Dynamics 365 for Sales connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Dynamics 365 for Sales connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. If you want to use the Hosted Agent to access Microsoft Dynamics 365 for Sales, the connection must use OAuth 2.0 Password Grant authentication.
Authentication Type	The authentication method that the connector must use to log in to the Microsoft Dynamics 365 for Sales online or on-premises. Select one of the following authentication types: <ul style="list-style-type: none"><li>- OAuth 2.0 Password Grant. Requires the web API URL, username, password, and application ID. You additionally need the security token service URL to access Microsoft Dynamics 365 for Sales on-premises. Applies to Microsoft Dynamics 365 for Sales online and on-premises.</li><li>- OAuth 2.0 Client Certificate Grant. Requires the web API URL, application ID, tenant ID, keystore file, keystore password, key alias, and key password. Applies to Microsoft Dynamics 365 for Sales online.</li><li>- OAuth 2.0 Client Secret Grant. Requires the application ID and client secret. Applies to Microsoft Dynamics 365 for Sales online.</li></ul>
Web API url	The URL of the Microsoft Dynamics 365 for Sales endpoint.
Username	The user name to connect to the Microsoft Dynamics 365 for Sales account.
Password	The password to connect to the Microsoft Dynamics 365 for Sales account.
Application ID	The Azure application ID for Microsoft Dynamics 365 for Sales.
Tenant ID	The directory ID for Azure Active Directory.
Keystore File	The location and the file name of the key store. Not applicable when you use the Hosted Agent. For the serverless runtime environment, specify the following keystore file path in the serverless agent directory: . For example: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<certificate file>
Keystore Password	The password for the keystore file required for secure communication.
Key Alias	The alias name for the individual key.

Property	Description
Key Password	The password for the individual keys in the keystore file required for secure communication. Not applicable when you use the Hosted Agent.
Retry Error Codes	The comma-separated http error codes for which the retries are made.
Retry Count	The number of retries to get the response from an endpoint based on the retry interval. Default is 5.
Retry Interval	The time in seconds to wait before Microsoft Dynamics 365 for Sales Connector retries for a response. Default is 60 seconds.
Client Secret	The client secret key to connect to Microsoft Dynamics 365 for Sales account.
Server Type	The Microsoft Dynamics 365 for Sales server that you want to access. You can select the server type from the following list: - Microsoft Dynamics Online. Connects to Microsoft Dynamics 365 for Sales deployed online. - Microsoft Dynamics On-premise. Connects to Microsoft Dynamics 365 for Sales deployed on-premises.
Security Token Service URL	The Microsoft Dynamics 365 for Sales security token service URL. Applies to the OAuth 2.0 Password Grant to access Microsoft Dynamics 365 for Sales on-premises. For example, <code>https://sts1.&lt;company&gt;.com/adfs/oauth2/token</code>

## Microsoft Dynamics 365 Mass Ingestion connection properties

When you set up a Microsoft Dynamics 365 Mass Ingestion connection, you must configure the connection properties.

The Microsoft Dynamics 365 Mass Ingestion connection requires a native application that is registered in Azure Active Directory (Azure AD) to access the Microsoft Dynamics 365 data. Before you configure the connection, you must register an application in Azure AD to allow the connection to access the Microsoft Dynamics 365 data. For more information about registering an application in Azure AD, see the [Microsoft documentation](#).

The properties of a Microsoft Dynamics 365 Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0 Username-Password Flow:** Authenticates the connection by using the Microsoft Dynamics 365 account login credentials and the client ID of the application registered in Azure AD.
- **OAuth 2.0 Client Secret Flow:** Authenticates the connection by using the client ID and client secret of the application registered in Azure AD.

- **OAuth 2.0 JWT Bearer Flow:** Authenticates the connection by using a X509 Public Key Infrastructure (PKI) certificate and a JSON Web Token (JWT). Use this authentication method to gain secured access to Microsoft Dynamics 365 without sharing sensitive information, such as client secret and Microsoft Dynamics 365 account login credentials.

### Connection properties for OAuth 2.0 Username-Password Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 Username-Password Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Microsoft Dynamics 365 account.
Password	Password for the Microsoft Dynamics 365 account.
Client ID	Client ID of the application registered in Azure AD.
Resource URL	URL of the Microsoft Dynamics 365 organization. You must enter the resource URL in the following format: <code>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</code>
OAuth Token URL	OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint. You must enter the following value in this field: <code>https://login.windows.net/common/oauth2/token</code>

**Note:** For more information about the OAuth 2.0 Username-Password Flow authentication method, see the Microsoft Dynamics 365 documentation.

### Connection properties for OAuth 2.0 Client Secret Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 Client Secret Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the application registered in Azure AD.
Client Secret	Client secret of the application registered in Azure AD.

Connection property	Description
Resource URL	URL of the Microsoft Dynamics 365 organization. You must enter the resource URL in the following format: <code>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</code>
OAuth Token URL	OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint. You must enter the following value in this field: <code>https://login.microsoftonline.com/&lt;tentant_id&gt;/oauth2/token</code>

**Note:** For more information about the OAuth 2.0 Client Secret Flow authentication method, see the Microsoft Dynamics 365 documentation.

### Connection properties for OAuth 2.0 JWT Bearer Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 JWT Bearer Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the application registered in Azure AD.
Certificate Signature	Base64URL string that encodes the hexadecimal value which represents the SHA-1 thumbprint of the X509 certificate.
Keystore Path	Absolute path to the keystore file that contains the X509 certificate required to validate a JSON Web Token (JWT) and establish a secure connection with Microsoft Dynamics 365. The keystore file must be in the Java KeyStore (JKS) format.
Keystore Password	Password for the keystore file.
Private Key Alias	Alias name of the private key used to sign the JWT.
Private Key Password	Password for the private key.
Audience for JWT	URL of the Microsoft Dynamics 365 resource server to which the application that is registered in Azure AD sends the JWT for validation. You must enter the address in the following format: <code>https://login.microsoftonline.com/&lt;tentant_id&gt;/oauth2/token</code>

Connection property	Description
Resource URL	URL of the Microsoft Dynamics 365 organization. You must enter the resource URL in the following format: <code>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</code>
OAuth Token URL	OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint. You must enter the following value in this field: <code>https://login.microsoftonline.com/&lt;tentant_id&gt;/oauth2/token</code>

**Note:** For more information about the OAuth 2.0 Client Secret Flow authentication method, see the Microsoft Dynamics 365 documentation.

## Microsoft Dynamics AX V3 connection properties

When you set up a Microsoft Dynamics AX V3 connection, you must configure the connection properties.

The following table describes the Microsoft Dynamics AX V3 connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Optional. Provide a relevant description for the connection.
Type	Select Microsoft Dynamics AX V3 from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication	Authenticates users who want to access Microsoft Dynamics AX 2012. Microsoft Dynamics AX V3 Connector supports Basic and NTLM authentication.
WSDL URI	Enter the required WSDL file path. <b>Note:</b> To find the WSDL URI, go to <b>System Administration &gt; Inbound Ports</b> in the Microsoft Dynamics AX 2012 instance. For example, the format of WSDL URI is <code>http://&lt;Hostname&gt;:&lt;Port&gt;/&lt;App_Pool_Name&gt;/&lt;Port name&gt;/xppservice.svc</code> .
Username	The user name to login to the Microsoft Dynamics AX 2012 web page.
Password	The password associated with the NT login user.
Company Name	Optional. Enter your company name. You can enter multiple company names separated by semi-colons. For example, <code>ceu;ceed</code> .
Language	Optional. Localizes the data you read from or write to Microsoft Dynamics AX 2012. Specify the language code.

# Microsoft Excel connection properties

When you set up a Microsoft Excel connection, you must configure the connection properties.

The following table describes the Microsoft Excel connection properties:

Connection property	Description
Connection Name	Name of the Microsoft Excel connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select <b>Microsoft Excel</b> source from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Folder URI	The directory that contains the Microsoft Excel file. The Microsoft Excel file must be located on the same machine on which the Secure Agent runs.
TreatFirstRowAsHeader	Specifies whether the first row in the file is a header row.
Filename	The name of the Microsoft Excel file. <b>Note:</b> You must add the <code>.xlsx</code> extension to the file name.

# Microsoft SharePoint connection properties

When you create a Microsoft SharePoint connection, you must configure the connection properties.

The following table describes the Microsoft SharePoint connection properties:

Property	Description
Connection Name	Enter the Microsoft SharePoint connection.
Description	Provide a relevant description for the connection.
Type	Select the type of connection as Microsoft SharePoint connection.
Runtime Environment	Runtime environment that contains the Secure Agent used to access Microsoft SharePoint.
Username	Enter the Microsoft SharePoint account username.
Password	Enter the Microsoft SharePoint account password.
SharePoint URL	Enter the URI for the data source exposed via OData protocol layer. All requests are extensions of this URI. For example, <code>https://infasharepoint.abcd.com/ Site/_vti_bin/Data.svc</code>

Property	Description
UTC Offset	Select the UTC time offset to be appended with datetime field. The default value is UTC. When you use the \$LastRuntime variable in a data filter, use the time zone to offset the \$LastRuntime variable.
Attachment File Path	Optional. Specify the folder path where you want to download and attach the file to Microsoft SharePoint.
Batch Size	Defines the number of rows to be fetched from Microsoft SharePoint server.
Enable Logging	Select the checkbox to enable logging.

## Microsoft Sharepoint Online connection properties

When you create a Microsoft Sharepoint Online connection, you must configure the connection properties.

The following table describes the Microsoft Sharepoint Online connection properties:

Property	Description
Connection Name	Enter the Microsoft Sharepoint Online connection.
Description	Provide a relevant description for the connection.
Type	Select the type of connection as Microsoft Sharepoint Online connection.
Runtime Environment	Runtime environment that contains the Secure Agent used to access Microsoft Sharepoint Online.
Client_Id	The client ID of Microsoft Sharepoint Online required to generate a valid access token.
Client_Secret	The client secret of Microsoft Sharepoint Online required to generate a valid access token.
Refresh_Token	The refresh token of Microsoft Sharepoint Online.
Redirect_URL	Enter the URL where you want to redirect from the Microsoft Sharepoint Online account.
URL	Enter the URL to the Microsoft Sharepoint Online account.
Attachment_File_Path	Specify the folder path where you want to download and attach the file to Microsoft Sharepoint Online.
Subsite_URL	Optional. Enter the subsite URL of the Microsoft Sharepoint Online account. If you do not enter a subsite URL, the Microsoft Sharepoint Online Connector reads the files from the URL that you specify in the <b>URL</b> property.

# Microsoft SQL Server CDC connection properties

When you configure a SQL Server CDC connection, you must set the connection properties.

The following table describes SQL Server CDC connection properties:

Property	Description
Connection Name	A name for the SQL Server CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the SQL Server CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For SQL Server CDC, the type must be <b>SQL Server CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for SQL Server change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example: MSSCDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The SQL Server instance name that is specified in the <b>Instance</b> field of the registration group that contains the registrations for the SQL Server source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Logger DBID	The DBID parameter value that is specified in the PowerExchange Logger for Linux, UNIX, and Windows configuration file, pwxcl.cfg. This value is required only if the PowerExchange Logger extracts change data for articles in multiple publication databases. In this case, you must also set the MULTIPUB parameter to Y in the MSQL CAPI_CONNECTION statement in the PowerExchange dbmover.cfg configuration file. Otherwise, the extraction fails.

Property	Description
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <div style="text-align: center;"><i>host_name:port_number</i></div> For example: MSSCDC2B:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a SQL Server table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXP) Microsoft SQL Server CDC connections in PowerCenter.

## Microsoft SQL Server connection properties

When you set up a Microsoft SQL Server connection, configure the connection properties.

The following table describes the Microsoft SQL Server connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Select SQL Server from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or serverless runtime environment.
SQL Server Version	Microsoft SQL Server database version.

Property	Description
Authentication Mode	<p>Authentication method to access Microsoft SQL Server.</p> <p>Select one of the following methods:</p> <ul style="list-style-type: none"> <li>- SQL Server Authentication. Uses your Microsoft SQL Server user name and password to access Microsoft SQL Server.</li> <li>- Windows Authentication (Deprecated). Uses the Microsoft Windows authentication to access Microsoft SQL Server. This option is available when you access Data Integration or Mass Ingestion by using Microsoft Windows.</li> </ul> <p>When you choose this option, you don't need to enter credentials to access Microsoft SQL Server and ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database.</p> <p>If you use Mass Ingestion Databases and want to use Windows authentication, select this option.</p> <p><b>Note:</b> Windows authentication is not certified for Microsoft SQL Server 2017 version hosted on Linux. You can't configure Windows Authentication when you use a serverless runtime environment.</p> <ul style="list-style-type: none"> <li>- Active Directory Password. Uses the Azure Active Directory user name and password to authenticate and access the Microsoft Azure SQL Database.</li> <li>- Windows Authentication v2. Uses this authentication method to access Microsoft SQL Server from Data Integration using the agent hosted on a Linux or Windows machine.</li> </ul> <p>When you choose this option on Linux, enter your domain name and Microsoft Windows credentials to access Microsoft SQL Server.</p> <p>When you choose this option on Windows, ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database.</p> <p><b>Note:</b> You can't configure Windows Authentication when you use a serverless runtime environment.</p> <ul style="list-style-type: none"> <li>- Kerberos. Uses Kerberos authentication to connect to Microsoft SQL Server.</li> </ul> <p>When you choose this option, ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database. You don't need to enter your credentials to access Microsoft SQL Server.</p> <p><b>Note:</b> You can't configure the Kerberos authentication when you use a Hosted Agent or serverless runtime environment.</p>
Domain	<p>Applies to Windows Authentication v2.</p> <p>The domain name of the Windows user.</p>
User Name	<p>User name for the database login. The user name can't contain a semicolon.</p> <p>To connect to Microsoft Azure SQL Database, specify the user name in the following format: username@host</p> <p>For Windows Authentication v2, specify the Windows NT user name.</p> <p><b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.</p>
Password	<p>Password for the database login. The password can't contain a semicolon.</p> <p>For Windows Authentication v2, specify the Windows NT password.</p> <p><b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.</p>
Host	<p>Name of the machine hosting the database server.</p> <p>To connect to Microsoft Azure SQL Database, specify the fully qualified host name.</p> <p>For example, vmjcmwxsfbheng.westus.cloudapp.azure.com.</p>

Property	Description
Port	Network port number used to connect to the database server. Default is 1433.
Instance Name	Instance name of the Microsoft SQL Server database.
Database Name	Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters. Database names can include alphanumeric and underscore characters.
Schema	Schema used for the target connection.
Code Page	The code page of the database server.
Encryption Method	The method that the Secure Agent uses to encrypt the data sent between the driver and the database server. You can use the encryption method to connect to Microsoft Azure SQL Database. Default is None.
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption.
Validate Server Certificate	When set to True, Secure Agent validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Secure Agent also validates the host name in the certificate.  When set to false, the Secure Agent doesn't validate the certificate that is sent by the database server.
Trust Store	The location and name of the truststore file. The truststore file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication.  For the serverless runtime environment, specify the following certificate path in the serverless agent directory:  <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</code>
Trust Store Password	The password to access the contents of the truststore file.
Host Name in Certificate	Host name of the machine that hosts the secure database. If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.
Metadata Advanced Connection Properties	Additional properties for the JDBC driver to fetch the metadata. If you specify more than one property, separate each key-value pair with a semicolon.
Runtime Advanced Connection Properties	Additional properties for the ODBC driver to run mappings. If you specify more than one property, separate each key-value pair with a semicolon.

# MLLP connection properties

When you configure a Minimal Lower Layer Protocol (MLLP) connection, you must configure the connection properties.

The following table describes the MLLP connection properties:

Property	Description
Connection Name	A name for the MLLP connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the MLLP connection. Maximum length is 4000 characters.
Type	Type of connection. For MLLP connection, the type must be <b>MLLP</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Host	Host name or IP address of the MLLP server.
Port	Port number for the MLLP server. Default is 2575.
Response Timeout	The wait time in seconds to receive a message from the specified MLLP server after sending the message. A timeout value of 0 is interpreted as infinite timeout. Default is 60 seconds.
Connection Timeout	Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection does not occur in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 30 seconds.
Connection Retry Interval	Number of seconds to wait between each connection retry attempt. For example, to retry to connect up to 10 times with a five second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5. Default is 0.
Connection Retry Attempts	Number of times to retry connecting to the MLLP server if a successful connection does not occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections. Default is 0. Specify 0 to disable the retry attempts.
Proxy Type	Type of proxy server to use for the connection. Select one of the following options: <ul style="list-style-type: none"><li>- No Proxy. Bypasses the proxy server configured at the agent or the connection level.</li><li>- HTTP. Uses the HTTP proxy.</li><li>- SOCKS. Uses the SOCKS (version 4 and 5) proxy.</li><li>- Platform Proxy. Considers proxy configured at the agent level.</li></ul> Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	Host name or IP address of the proxy server on your network.

Property	Description
Proxy Port	Port number of the proxy server on your network.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server.

## MongoDB V2 connection properties

When you create a MongoDB V2 connection, you must configure the connection properties.

The following table describes the MongoDB V2 connection properties:

Property	Description
Connection Name	The 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The MongoDB v2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Node name or IP address of the primary shard in the MongoDB cluster.
Service Record Lookup Enabled	The connection format to indicate that the hostname corresponds to a DNS Service Record Lookup. It enables the connector to query the DNS to construct the available server list that runs MongoDB instances. Select this checkbox if the host name corresponds to a DNS SRV record. Port is not considered if this checkbox is selected.
Port	MongoDB server port number. Default is 27017.
Authentication	Authentication method to access the MongoDB resources. Choose one of the following authentication methods: - Username and Password. Uses user name and password credentials to connect to the MongoDB server. - X.509. Uses X.509 certificate to connect to the MongoDB server.
User Name	User name to access the MongoDB server.
Password	Password corresponding to the user name to access the MongoDB server.

Property	Description
SSL KeyStore File Path	<p>The absolute path of the keystore file in the Secure Agent machine that contains the keys and certificates required to establish a secure communication.</p> <p>Ensure that you download the certificates and place them in the Secure Agent machine before you specify this parameter.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;keystore_filename&gt;</pre> <p>For more information, see the <a href="#">"Configure SSL for the serverless runtime environment" on page 190</a> chapter.</p> <p>Applicable if you select X.509 authentication type.</p>
SSL KeyStore Password	<p>The password for the keystore file required for secure communication.</p> <p>Applicable if you select X.509 authentication type.</p>
Database Name	<p>Name of the MongoDB database to connect to.</p>
Additional Properties	<p>Optional properties that you can configure to read data from or write data to Amazon DocumentDB and other non-SSL MongoDB deployments.</p> <p>For information about the additional properties that you can configure, see the <a href="#">"Additional connection properties" on page 189</a> chapter.</p> <p>To specify more than one property, separate the key-value pairs with an ampersand.</p> <p>You can specify the properties in the following format:</p> <pre>propertyName1=&lt;value1&gt;&amp;propertyName2=&lt;value2&gt;</pre>

## Additional connection properties

You can configure additional options in a MongoDB V2 connection.

### Amazon DocumentDB optional properties

Configure additional connection properties in the Additional Properties field to connect to Amazon DocumentDB:

#### ssltruststorefilepath

The absolute path of the truststore file in the Secure Agent machine that contains the keys and certificates required to establish a secure communication.

For example, ssltruststorefilepath= <path\_of\_truststore\_file>

For the serverless runtime environment, specify the following certificate path to the serverless agent directory:

```
/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<truststore_filename>
```

For more information, see ["Configure SSL for the serverless runtime environment" on page 190](#) chapter.

#### ssltruststorepassword

The password for the truststore file required for secure communication.

For example, ssltruststorepassword=<password>.

### Sampling properties

Configure sampling properties in the Additional Properties field:

**samplesize**

The number of documents to scan to infer the schema from the MongoDB source.

For example, samplesize=100.

Default is 100.

**samplemethod**

The method to sample documents to infer the schema from the MongoDB source.

You can specify one of the following methods:

- firstpage. Scans first n documents from MongoDB where n indicates the sample size. MongoDB determines the ordering of rows for scanning.
- random. Scans n number of random documents from MongoDB.
- all. Scans the entire collection to infer schema.

## Other properties

Configure additional connection properties in the Additional Properties field to connect to non-SSL MongoDB deployments:

**ssl**

Determines if the connection uses SSL or non-SSL.

Set this parameter to false in the connection properties to connect to MongoDB deployments that do not use SSL.

Default is true.

**authsource**

Allows you to provide the database name against which you can authenticate user credentials.

For example, authsource=testadmin.

Default is admin.

## Configure SSL for the serverless runtime environment

You can use the serverless runtime environment with MongoDB V2 Connector to connect to an SSL-enabled MongoDB database.

Before you configure a secure MongoDB V2 connection using the serverless runtime environment, you need to perform certain prerequisites:

1. Ensure that the truststore and keystore certificate files are in .jks format.
2. Add the truststore and keystore certificates in the Amazon S3 bucket in the following location in your AWS account: <Supplementary file location>/serverless\_agent\_config/SSL
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<cert_filename>
        - fileCopy:
            sourcePath: SSL/<cert_filename>
```

where the source path is the directory path of the certificate files in AWS.

**Note:** You can add multiple source paths of the certificate files by adding multiple *fileCopy* tags.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS location: `<Supplementary file location>/serverless_agent_config`  
When the .yml file runs, the SSL certificates are copied from the AWS location to the serverless agent directory.
5. Deploy the serverless agent.
6. Specify the following certificate path in the serverless agent directory for the truststore and keystore file path fields: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>`

## MQTT connection properties

When you set up an MQ Telemetry Transport (MQTT) connection, you must configure the connection properties.

The following table describes the MQTT connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identity the connection. The description cannot exceed 4,000 characters.
Type	The MQTT connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Broker URI	The connection URL of the MQTT broker. If specified, this value overrides the URL specified in the main portion of the URL. Sample URL: <code>tcp://&lt;IP Address&gt;:&lt;port&gt;</code>
Client Id	Client identifier of your MQTT client. If this value is left blank, the MQTT server assigns a unique value. This property value must be unique for each MQTT client connecting to a specific MQTT server. Sharing projects without changing the Client ID can lead to connection issues, including disconnections and missing updates.
Username	Username to use when connecting to the broker.
Password	Password to use when connecting to the broker.

Property	Description
Connection Timeout	<p>Maximum time interval the client will wait for the connection to the MQTT server to be established.</p> <p>Default timeout is 30 seconds.</p> <p>A value of 0 disables timeout processing. That is, the client waits until the network connection is made successfully or fails.</p>
Use SSL	<p>Enable this option to use SSL for secure transmission.</p> <p>If you enable the SSL authentication, ensure to provide both keystore and truststore details for using the MQTT connection in a streaming ingestion task.</p>
Keystore Filename	Contains the keys and certificates required for secure communication.
Keystore Password	Password for the keystore filename.
Keystore Type	<p>Type of keystore to use.</p> <p>Keystore type defines the storage and data format of the keystore information and the algorithms used to protect private keys in the keystore.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- JKS. Stores private keys and certificates.</li> <li>- PKCS12. Stores private keys, secret keys. and certificates.</li> </ul>
Truststore Filename	File name of the truststore file.
Truststore Password	Password for the truststore file name.
Truststore Type	<p>Type of truststore to use.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- JKS</li> <li>- PKCS 12</li> </ul>
TLS Protocol	<p>Transport protocols to use.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- SSL</li> <li>- SSLv3</li> <li>- TLS</li> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul>

## MRI Software connection properties

When you set up an MRI Software connection, you must configure the connection properties.

The following table describes the MRI Software connection properties:

Property	Description
Connection Name	Enter a name for the connection.
Description	Optional. Enter a description for the connection.
Type	Type of connection. Select <b>MRI Software</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
URL	Endpoint URL of the MRI Software application.
Username	User name of the MRI Software application.
Password	Password for the MRI Software application.
Client ID	The client ID created in the MRI Software application.
Database Name	Name of the MRI database.
Partner Key	The partner key provided by MRI Software.
API Type	The type of MRI Software API that you want to connect to. Select one of the following options: <ul style="list-style-type: none"><li>- <b>Data Pipeline</b>. Select to connect to the Data Pipeline API to read large amount of data.</li><li>- <b>REST</b>. Select to connect to the REST API.</li></ul>

## MySQL CDC connection properties

When you configure a MySQL CDC connection, you must set the connection properties.

The following table describes MySQL CDC connection properties:

Property	Description
Connection Name	A name for the MySQL CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the MySQL CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For MySQL CDC, the type must be <b>MySQL CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for MySQL change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: MYSCDC1A:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	MySQL instance name that is specified in the <b>Instance</b> field of the registration group that contains capture registrations for the MySQL source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>

Property	Description
Map Location	<p>Host name or IP address of the system that contains the extraction maps. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: MYSCDC2B:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a MySQL table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the the PowerExchange Client for PowerCenter (PWXPC) MySQL CDC connections in PowerCenter.</p>

## MySQL connection properties

When you set up a MySQL connection, configure the connection properties.

The following table describes the MySQL connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -,</p> <p>Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.

Property	Description
Type	Type of connection. Select MySQL from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. <b>Note:</b> You cannot run a database ingestion task on a Hosted Agent or serverless runtime environment.
User Name	User name for the database login. The user name can't contain a semicolon.
Password	Password for the database login. The password can't contain a semicolon.
Host	Name of the machine that hosts the database server.
Port	Network port number used to connect to the database server. Default is 3306.
Database Name	Name of the MySQL database that you want to connect to. <b>Note:</b> The database name is case-sensitive. Maximum length is 64 characters. Database name can contain alphanumeric and underscore characters.
Code Page	The code page of the database server.
Metadata Advanced Connection Properties	Additional properties for the JDBC driver to fetch the metadata. If you specify more than one property, separate each key-value pair with a semicolon.
Runtime Advanced Connection Properties	Additional properties for the ODBC driver to run mappings ingestion jobs. If you specify more than one property, separate each key-value pair with a semicolon.

## SSL properties

You can configure a MySQL connection to use SSL to securely communicate with the MySQL database.

**Note:** You can enable SSL for a MySQL connection only when you use the 8.x MySQL JDBC and ODBC drivers. Ensure that both the MySQL JDBC and ODBC drivers are of 8.x version.

To configure SSL, you must first download and install the MySQL ODBC and JDBC drivers, version 8.x. For information about installing the MySQL ODBC and JDBC drivers, version 8.x, see the Knowledge Base article: [561573](#)

After you install the drivers, in the MySQL connection properties, enable SSL and specify the TLS protocols that you want to use for the secure communication.

When you enable SSL for the MySQL connection, you must configure the SSL properties for both the MySQL JDBC and ODBC drivers. Configure the required SSL properties for the JDBC driver, so that the Secure Agent can access metadata securely from MySQL. Also, configure the required SSL properties for the ODBC driver, so that the Secure Agent runs mappings to securely read from or write data to MySQL.

**Note:** SSL is not applicable when you use the Hosted Agent. You can configure SSL when you use the Secure Agent or the serverless runtime environment.

The following table describes the MySQL connection SSL properties:

Connection property	Description
Use SSL	<p>Determines whether the Secure Agent establishes a secure connection to the MySQL database.</p> <p>When you select this option and the database server supports SSL, the Secure Agent establishes an encrypted connection. If the MySQL database server cannot configure SSL, the connection either fails or the Secure Agent establishes an unencrypted connection depending on whether you enable or disable the <b>Require SSL</b> checkbox.</p> <p>If you do not select the <b>Use SSL</b> checkbox, the Secure Agent attempts to establish an unencrypted connection.</p>
Verify Server Certificate	<p>If you select <b>Use SSL</b> and select this option, the client validates the server certificate that is sent by the database server.</p>
Require SSL	<p>Applicable only if you select <b>Use SSL</b>.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database supports SSL, the Secure Agent establishes an SSL connection.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent attempts to establish an SSL connection but fails.</p> <p>If you clear the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent establishes an unencrypted connection.</p>
TLS Protocols	<p>The TLS protocols used for the secure communication when you select <b>Use SSL</b>.</p> <p>You can select from the following protocols:</p> <ul style="list-style-type: none"> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul> <p>Default is TLSv1.2. The TLSv1 and TLSv1.1 protocols are not applicable.</p>

The following table describes the MySQL connection properties for the JDBC driver version 8.x when you enable **Use SSL**:

Connection property	Description
Trust Certificate Key Store	<p>The path and file name of the truststore file. You must prefix the file path with file colon (file:).</p> <p>For example, file:C:\SSL\mysql_new\truststore</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Trust Certificate Key Store Password	<p>The password for the truststore file.</p>

Connection property	Description
Client Certificate Key Store	<p>The path and file name of the keystore file. You must prefix the file path with file colon (file:).</p> <p>For example, file:C:\SSL\mysql_new\keystore</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</pre>
Client Certificate Key Store Password	The password to access the keystore file.
JDBC Cipher Suites	<p>Colon-separated cipher suite values in RFC format.</p> <p>For example:</p> <pre>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</pre>

The following table describes the MySQL connection properties for the ODBC driver version 8.x when you enable **Use SSL**:

Connection property	Description
SSL Certificate Authority	<p>The path and name of the CA certificate.</p> <p>For example, C:\SSL\mysql_new\ca.pem</p>
SSL Certificate	<p>The path and name of the client certificate.</p> <p>For example, C:\SSL\mysql_new\client-cert.pem</p>
SSL Key	<p>The path and the name of the private key of the client.</p> <p>For example, C:\SSL\mysql_new\client-key.pem</p>
SSL Cipher	<p>Colon-separated cipher-suite values in OpenSSL format.</p> <p>For example:</p> <pre>ECDSA-ECDHE-AES128-GCM-SHA256: ECDSA-ECDHE-AES256-GCM-SHA384: ECDSA-RSA-AES128-GCM-SHA256:</pre>
Verify Server's Identity	<p>Verifies the host name in the certificate while verifying the server CA certificate.</p> <p>This property is applicable only when you enable <b>Verify Server Certificate</b> in the SSL properties.</p>

# Netezza connection properties

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

The following table describes the Netezza connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Database	The name of the Netezza database.
Schemaname	The schema used for the Netezza source or target. Schema name is case sensitive.
Servename	The Netezza database host name.
Port	Network port number used to connect to the database server. Default is 1521.
Driver	The Netezza ODBC driver name, NetezzaSQL, used to connect to the Netezza database.
Runtime Additional Connection Configuration	Additional run-time attributes required to fetch data. For example, <code>securityLevel=preferredUnSecured;caCertFile =</code>
Metadata Additional Connection Configuration	The values to set the optional properties of the JDBC driver to fetch the metadata.
Username	Database user name with the appropriate read and write database permissions to access the database.
Password	Password for the database user name.

# NetSuite Mass Ingestion connection properties

When you set up a NetSuite Mass Ingestion connection, you must configure the connection properties.

**Note:** Before you configure the connection properties, install the SuiteAnalytics Connect JDBC driver and copy the NQjc.jar file to the following directory: <Secure\_Agent>\ext\connectors\thirdparty\informatica.netsuiteami

For more information about installing the SuiteAnalytics Connect JDBC driver, see the [SuiteAnalytics Connect documentation](#).

The following table describes the connection properties for a NetSuite Mass Ingestion connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the NetSuite account. The user name is an email address.
Password	Password for the NetSuite account.
Service Host	Name of the SuiteAnalytics Connect Service host. The value in this field must match the value specified in the <b>Service Host</b> field under the <b>Your Configuration</b> section of the <b>SuiteAnalytics Connect Driver Download</b> page in NetSuite. To access the <b>SuiteAnalytics Connect Driver Download</b> page, log in to NetSuite and click the Set Up SuiteAnalytics Connect link in the Settings portlet.
Service Port	TCP/IP port on which the SuiteAnalytics Connect server is listening. Default is 1708.
Service Datasource	Data source that you want to use to access NetSuite data. You can select one of the following data sources: - NetSuite.com - NetSuite2.com Default is NetSuite2.com. <b>Note:</b> - In connections configured before the August 2022 release, the default value for this field is NetSuite.com. - To use a NetSuite2.com data source, the NetSuite user account must be configured with some specific roles and permissions. For more information about the roles and permissions required to access NetSuite2.com data sources, see the <a href="#">NetSuite documentation</a> .
Account ID	NetSuite account ID. To find your account ID, log in to NetSuite and click <b>Setup &gt; Integration &gt; Web Services Preferences</b> . If you cannot access the <b>Setup</b> menu, navigate to <b>Support &gt; Go to Suite Answers &gt; Contact support by phone</b> . The page displays your account ID.
Role ID	Role ID associated with the NetSuite account.
Additional Connection Properties	Additional properties for the SuiteAnalytics Connect Driver that is used to connect to the NetSuite service data source. Specify the properties in <code>&lt;property&gt;=&lt;value&gt;</code> format. If you want to specify multiple properties, separate each property-value pair with a semicolon (;). You can specify the following connection properties in this field: - <b>ValidateServerCertificate:</b> Determines whether the driver validates the certificate sent by the SuiteAnalytics Connect server. During SSL server authentication, the SuiteAnalytics Connect server sends a certificate issued by a trusted Certificate Authority (CA). The required CAs are usually included in the Java truststore but you can also specify them using the TrustStore property. Valid values for the ValidateServerCertificate property are <i>true</i> and <i>false</i> . - <b>TrustStore:</b> Contains the path to a valid truststore containing the security certificates to be used for server authentication. The TrustStore property is ignored if the ValidateServerCertificate property is set to <i>false</i> . <b>Note:</b> For more information about the additional connection properties, see the <a href="#">NetSuite documentation</a> .

# NICE Satmetrix connection properties

When you set up a NICE Satmetrix connection, you must configure the connection properties.

The following table describes the NICE Satmetrix connection properties:

Connection property	Description
Connection Name	Name of the NICE Satmetrix connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the NICE Satmetrix connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Satmetrix URL	The URL with which the Secure Agent connects to the Satmetrix APIs. The URL has the following format: <i>http://&lt;company name&gt;.satmetrix.com</i>
Username	Username of the Satmetrix integration user account.
Password	Password of the Satmetrix integration user account.

## OData connection properties

When you set up an OData connection, configure the connection properties.

The following table describes the OData connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The OData connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
User Name	User name to connect to the OData service.
Password	Password associated with the user name.
Service Root URI	Root URI for the data source offered through the OData protocol. <b>Note:</b> The service root URI must follow the <a href="#">OData URI Conventions</a> .

Property	Description
OData Parameter File Path	Absolute path to a file that you append to the URL. The file contains key value pairs separated by a new line. You can use this file to check additional parameter values required in the URL. <b>Note:</b> Ensure that you use percent encoding to encode the key value pairs in the file.
Data Serialization Format	The format of data you want to transfer. Choose from ATOM/XML or JSON. Default is ATOM/XML.

## OData V2 Protocol Writer connection properties

When you set up an OData V2 Protocol Writer connection, you must configure the connection properties.

The following table describes the OData V2 Protocol Writer connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={} \ \:;'"<, > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>OData V2 Protocol Writer</b> connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication Type	The type of user authentication to connect to the OData V2 service. You can select from the following authentication types: - <b>Basic Authentication.</b> Requires the user name and password to log in to the OData V2 application. - <b>API Key.</b> Requires a unique API key to connect to the OData V2 application.
Token Type	The token used by the OData V2 application endpoint to perform the required CRUD operations. Default is CSRF Token.
Service Type	The service type of the OData V2 application endpoint to which you want to connect. Default is Catalog Service.

Connection property	Description
Service URL	<p>The OData service URL of the catalog service that contains the APIs exposed by the OData V2 application.</p> <p>For example, enter the service URL to access the data from the SAP catalog service in the following format:</p> <pre>http://&lt;hostname of the SAP server&gt;:&lt;port number&gt;/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre> <p>If the host name and port number is <i>inpha1.informatica.com:8001</i> and the service endpoint is <i>CATALOGSERVICE</i>, enter the following URL:</p> <pre>https://inpha1.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre>
Data Serialization Format	<p>The data serialization format that the OData V2 catalog service supports.</p> <p>You can select from one of the following formats:</p> <ul style="list-style-type: none"> <li>- ATOM/XML</li> <li>- JSON</li> </ul> <p>Default is ATOM XML.</p>
Username	<p>Required for basic authentication.</p> <p>The user name to connect to the OData V2 application.</p>
Password	<p>Required for basic authentication.</p> <p>The password associated with the OData V2 application user name.</p>
API Key	<p>Required for API key authentication.</p> <p>The unique API key that the OData V2 application client provides for authorization when you make API calls to the OData V2 service.</p>

## OData V2 Protocol Reader connection properties

When you set up an OData V2 Protocol Reader connection, you must configure the connection properties.

The following table describes the OData V2 Protocol Reader connection properties:

Connection property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -,</p> <p>Maximum length is 255 characters.</p>
Description	<p>Description of the connection. Maximum length is 4000 characters.</p>
Type	<p>The OData V2 Protocol Reader connection type.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run the tasks.</p> <p>Specify a Secure Agent, Hosted Agent, or serverless runtime environment.</p>

Connection property	Description
Service Type	<p>The service type of the OData V2 application endpoint to which you want to connect.</p> <p>Choose one of the following service types:</p> <ul style="list-style-type: none"> <li>- SAP S/4HANA Catalog. Use the SAP S/4HANA Catalog service type for endpoints such as SAP S/4HANA that exposes specialized OData V2 service to list the services present in the endpoint.</li> <li>- Default. Use the Default service type for all other endpoints.</li> </ul>
Service URL	<p>The service URL for the selected OData V2 service type.</p> <p>For the Default service type, enter the root URL of the service.</p> <p>For example, enter the service URL in the following format:</p> <pre>https://sandbox.api.sap.com/s4hanacloud/sap/opu/odata/sap/API_CHARTOFACCOUNTS_SRV</pre> <p>You can verify if the URL is valid by appending <code>\$metadata</code> to the URL.</p> <p>For SAP S/4HANA catalog service type, enter the URL of the catalog service in SAP S/4HANA.</p> <p>For example, to access the data from the SAP S/4HANA catalog service, enter the service URL in the following format:</p> <pre>http://&lt;hostname of the OData server&gt;:&lt;port number&gt;/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre> <p>If the host name and port number is <code>inphal.informatica.com:8001</code> and the service endpoint is SAP S/4HANA Catalog, enter the following URL:</p> <pre>https://inphal.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre>
Authentication Type	<p>The type of user authentication to connect to the OData service.</p> <p>Choose from the following authentication types:</p> <ul style="list-style-type: none"> <li>- Basic. Requires the user name and password to log in to the OData V2 application.</li> <li>- API Key. Requires a unique API key to connect to the OData V2 application.</li> <li>- OAuth 2.0 authorization code. Requires authorized access to connect to the OData V2 endpoint.</li> <li>- OAuth 2.0 client credentials. Requires client credentials to connect to the OData V2 endpoint.</li> </ul>
Username	<p>Applies to basic authentication.</p> <p>The user name to connect to the OData V2 application.</p>
Password	<p>Applies to basic authentication.</p> <p>The password associated with the OData V2 application user name.</p>
API Key	<p>Applies to API key authentication.</p> <p>Unique API key required to connect to the OData V2 application.</p>

## 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 response returns 401 error code, 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 OData V2 Protocol Reader 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, Hosted Agent, or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the OData V2 endpoint. Select <b>OAuth 2.0 authorization code</b> . Default is Basic.
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 OData V2 endpoint has defined custom scopes. Enter space-separated scope attributes. For example: ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</pre>
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 <b>Send client credentials in body</b> .
Generate Access Token	Generates access token and refresh token based on the specified authentication details.
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 <b>Generate Access Token</b> to populate the access token value.
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 <b>Generate Access Token</b> to populate the refresh token value. If the refresh token expires, you must either provide a valid refresh token or click <b>Generate Access Token</b> to regenerate a new refresh token.

## Client credential authentication

The following table describes the OData V2 Protocol Reader 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, Hosted Agent, or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the OData V2 endpoint. Select <b>OAuth 2.0 client credentials</b> . Default is Basic.
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: ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>
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 <b>Send client credentials in body</b> .
Generate Access Token	Generates access token based on the specified authentication details.
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 <b>Generate Access Token</b> to populate the access token value.

# ODBC connection properties

When you set up an ODBC connection, configure the connection properties.

The following table describes the ODBC connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
User Name	User name for the database login.
Password	Password for the database login. The password cannot contain a semicolon.
Data Source Name	System DSN.
Schema	Schema used for the object.

Property	Description
Code Page	<p>The code page of the database server or flat file defined in the connection. Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> <li>- Japanese Extended UNIX Code (incl. JIS X 0212)</li> <li>- Japanese EUC (with \&lt;-&gt; Yen mapping)</li> <li>- Japanese EUC (Packed Format)</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- Japanese EBCDIC Fujitsu</li> <li>- HITACHI KEIS Japanese</li> <li>- NEC ACOS JIPSE Japanese</li> <li>- UNISYS Japanese</li> <li>- MITSUBISHI MELCOM Japanese</li> <li>- Japanese EBCDIC-Kana Fujitsu</li> <li>- HITACHI KEIS-Kana Japanese</li> <li>- NEC ACOS JIPSE-Kana Japanese</li> <li>- UNISYS-Kana Japanese</li> <li>- MITSUBISHI MELCOM-Kana Japanese</li> <li>- EBCDIC Japanese</li> <li>- EBCDIK Japanese</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- EBCDIC Japanese Katakana SBCS</li> <li>- EBCDIC Japanese Katakana (w/ euro)</li> <li>- EBCDIC Japanese Latin-Kanji (w/ euro)</li> <li>- EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399)</li> <li>- EBCDIC Japanese Latin (w/ euro update)</li> <li>- EBCDIC Japanese Katakana SBCS (w/ euro update)</li> <li>- MS Taiwan Big-5 w/ HKSCS extensions</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/ euro update)</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- PC Chinese GBK (IBM-1386)</li> <li>- Chinese EUC</li> <li>- Simplified Chinese (GB2312-80)</li> <li>- Hong Kong Supplementary Character Set</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- PC Hebrew (w/ euro update)</li> <li>- MS Windows Hebrew (older version)</li> <li>- MS Windows Hebrew (w/o euro update)</li> <li>- Lotus MBCS encoding for Windows Hebrew</li> <li>- EBCDIC Hebrew (updated with sheqel, control characters)</li> <li>- EBCDIC Hebrew (w/ euro)</li> <li>- EBCDIC Hebrew (updated w/ euro and new sheqel, control characters)</li> <li>- Israeli Standard 960 (7-bit Hebrew encoding)</li> </ul>

Property	Description
ODBC Subtype	<p>The ODBC connection subtype that you must select to connect to a specific database. The subtype defines the capabilities that you can configure while you create a mapping.</p> <p>You can select from the following supported subtypes based on the database to which you want to connect:</p> <ul style="list-style-type: none"> <li>- Azure DW. Select Azure DW to enable pushdown optimization when you read from or write to Microsoft Azure SQL Data Warehouse.</li> <li>- DB2. Select DB2 to read from or write to DB2. You can also enable pushdown optimization when you read from or write to DB2.</li> <li>- Google BigQuery. Select Google BigQuery to enable pushdown optimization when you read from or write to Google BigQuery.</li> <li>- PostgreSQL. Select PostgreSQL to enable pushdown optimization when you read from or write to PostgreSQL.</li> <li>- Redshift. Select Redshift to enable pushdown optimization when you read from or write to Amazon Redshift.</li> <li>- SAP IQ. Select SAP IQ to read data from the SAP IQ database.</li> <li>- Snowflake. Select Snowflake to enable pushdown optimization when you read from or write to Snowflake.</li> <li>- Teradata. Select Teradata to enable pushdown optimization when you read from or write data to Teradata. You can also enable SQL transformation in a mapping to call a stored procedure in Teradata or to process SQL saved queries against the Teradata database.</li> </ul> <p><b>Note:</b> If you want to connect to an SSL-enabled ODBC Teradata connection, ensure that the <b>SSL Mode</b> option under <b>WebSocket</b> is set to an appropriate value while configuring the Teradata ODBC driver.</p> <ul style="list-style-type: none"> <li>- Other. Select Other to enable pushdown optimization when you read from or write to Microsoft Access, Microsoft Excel, or Netezza.</li> </ul>
Driver Manager for Linux	<p>When you create a new ODBC connection on Linux platform, you can select a driver manager for the Linux Secure Agent. Select one of the following driver managers:</p> <ul style="list-style-type: none"> <li>- Data Direct</li> <li>- unixODBC2.3.0</li> <li>- unixODBC2.3.4</li> </ul> <p>The default driver manager is UnixODBC2.3.0.</p> <p>To connect to Teradata, you can use only Data Direct as the driver manager on Linux.</p>

## OpenAir connection properties

When you create an OpenAir connection, you must configure the connection properties.

The following table describes the OpenAir connection properties:

Property	Description
Secure Agent	The Secure Agent used to access OpenAir.
Username	User name of the OpenAir account.
Password	Password of the OpenAir account.
Company	Enter the company name.
API NameSpace	Enter the API NameSpace.

Property	Description
API Key	Enter the API Key.
Client Name	Enter the client name.
WSDL Url	Enter WSDL URL.
Endpoint Url	Enter end-point URL.
Batch Size	Enter the OpenAir write batch size. Default is 100.
Version	Enter the version number.
Enable Logging	Select to enable logging.

## Oracle Business Intelligence Publisher V1 connection properties

When you create an Oracle Business Intelligence Publisher V1 connection, you must configure the connection properties.

The following table describes the Oracle Business Intelligence Publisher V1 connection properties:

Connection Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
BI Publisher URL	URL of the Oracle Business Intelligence Publisher application that you want to access. <b>Note:</b> To validate the BI Publisher URL, type the following URL in the web browser: <BI Publisher URL>/xmlpserver/services/ExternalReportWSSService?wsdl If the URL opens a WSDL file, the BI Publisher URL is valid.
Authentication Type	Type of user authentication to connect to the Oracle Business Intelligence Publisher application. You can select <b>Basic Authentication</b> type.
Username	User name of the Oracle Business Intelligence Publisher account.
Password	Password for the Oracle Business Intelligence Publisher account.

Connection Property	Description
Report Directory	<p>The directory path where the reports are stored in the Oracle Business Intelligence Publisher application.</p> <p>You can read a report from the following folders:</p> <ul style="list-style-type: none"> <li>- Shared Folders</li> <li>- My Folders</li> </ul> <p>To read a report from Shared Folders, exclude <code>Shared Folders</code> from the directory path. For example, if the report is in <code>Shared Folders/Samples/Sales</code>, specify the report directory as follows:</p> <pre>/Samples/Sales</pre> <p>To read a report from My Folders, exclude <code>My Folders</code> from the directory path and include <code>~username</code> as the first node in the directory path. For example, if the report is in <code>My Folders/Samples/Sales</code>, and the username is <code>weblogic</code>, specify the report directory as follows:</p> <pre>/~weblogic/Samples/Sales</pre> <p>Default value of the report directory is <code>/Custom</code>.</p>
Output Directory	<p>The directory path where you want to download the <code>.csv</code> files on the Secure Agent machine.</p> <p><b>Note:</b> This field is applicable when you create an Oracle Business Intelligence Publisher connection to read data in the <code>.csv</code> data format.</p>

## Oracle CDC V2 connection properties

When you configure an Oracle CDC connection, you must set the connection properties.

The following table describes Oracle CDC connection properties:

Property	Description
Connection Name	<p>A name for the Oracle CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code></p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the Oracle CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Oracle CDC, the type must be <b>Oracle CDC V2</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for Oracle change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>ORACDC1A:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	Oracle instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains capture registrations for the Oracle source tables and in the ORACLEID statement in the PowerExchange dbmover configuration file. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Source Schema Override	If you created a single capture registration for a set of source tables that have the same table name but different schemas and defined an override schema name in a PowerExchange Logger group definition file, enter that override schema name. Otherwise, PowerExchange cannot extract the change data for the source table that has the override schema from the log files. For more information about PowerExchange Logger group definitions, see the <i>PowerExchange CDC Guide for Linux, UNIX, and Windows</i> .
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>

Property	Description
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	<p>Enter the host name or IP address of the system that contains the extraction maps. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: ORACDC2B:25100</p> <p>The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Oracle table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Oracle CDC connections in PowerCenter.</p>

# Oracle Cloud Object Storage connection properties

When you create an Oracle Cloud Object Storage connection, you must configure the connection properties.

The following table describes the Oracle Cloud Object Storage connection properties:

Property	Description
Connection Name	The 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Oracle Cloud Object Storage connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Authentication Type	Authentication type to connect to Oracle Cloud Object Storage to stage the files. Select one of the following options: <ul style="list-style-type: none"><li>- Simple Authentication. API key-based authentication.</li><li>- ConfigFile Authentication. Identity credential details are provided through a configuration file.</li></ul>
User OCID	The unique identifier of the user in Oracle Cloud Infrastructure. For example, <code>ocidl.user.oc1..aaaaaaaaherdgpkqzrwbd7n5ksokkot7c5jngtx3pgolr7oqb7xzksza</code>
Fingerprint	Fingerprint of the public key.
Tenancy OCID	The unique identifier of the tenancy in Oracle Cloud Infrastructure. The tenancy is the globally unique name of the Oracle Cloud Infrastructure account. For example, <code>ocidl.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq</code>
Configuration File Location	The absolute path of the configuration file on the Secure Agent machine. If you do not enter the value, the Secure Agent uses the following configuration file path: <code>~/.oci/config</code>
Private Key File Location	Location of the private key file in .PEM format on the Secure Agent machine.
Profile Name	Name of the profile in the configuration file that you want to use. Default is <code>DEFAULT</code> .
Bucket Name	The Oracle Cloud Object Storage bucket name that contains the objects and files.
Folder Path	The folder under the specified Oracle Cloud Object Storage bucket. For example, <code>bucket/Dir_1/Dir_2/FileName.txt</code> . Here, <code>Dir_1/Dir_2</code> is the folder path.
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.

# Oracle connection properties

When you create an Oracle connection, configure the connection properties.

The following table describes the Oracle connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Select Oracle from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Oracle Subtype	The Oracle connection subtype that you can use to connect to Oracle on-premises or Oracle Autonomous Database. Select one of the following options: <ul style="list-style-type: none"><li>- Oracle ADB. Connects to Oracle Autonomous Database.</li><li>- Oracle On-premise. Connects to Oracle on-premises.</li></ul>
Authentication Mode	The authentication method to connect to Oracle. Select one of the following authentication modes: <ul style="list-style-type: none"><li>- Oracle Database Authentication. Uses your Oracle user name and password to connect to Oracle.</li><li>- Kerberos. Uses Kerberos authentication to connect to Oracle.</li></ul> <p>When you choose this option, ensure that the user account that starts the Secure Agent service is available in the Oracle database. You don't need to enter your credentials to access Oracle.</p> <p><b>Note:</b> You can't configure Kerberos authentication when you use a Hosted Agent or serverless runtime environment.</p>
User Name	User name for the database login. The user name can't contain a semicolon.
Password	Password for the database login. The password can't contain a semicolon.
Host	Name of the machine that hosts the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: <code>SID:&lt;ORACLE_SID&gt;</code>
Schema	Schema used for the Oracle connection.
Code Page	The code page of the database server.

Property	Description
Encryption Method	<p>The method that the Secure Agent uses to encrypt the data exchanged between the Secure Agent and the database server.</p> <p>Default is No Encryption.</p> <p>Not applicable when you use the Hosted Agent or the serverless runtime environment.</p>
Crypto Protocol Version	<p>Cryptographic protocols to use when you enable SSL encryption.</p> <p>Not applicable when you use the Hosted Agent or the serverless runtime environment.</p>
Validate Server Certificate	<p>Validates the certificate that is sent by the database server. If you specify the <code>HostNameInCertificate</code> parameter, the Secure Agent also validates the host name in the certificate.</p>
Trust Store	<p>The location and name of the truststore file.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Trust Store Password	<p>The password to access the contents of the truststore file.</p>
Host Name in Certificate	<p>Host name of the machine that hosts the secure database.</p> <p>If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
Key Store	<p>The location and the file name of the keystore.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</pre>
Key Store Password	<p>The password for the keystore file required for secure communication.</p>
Key Password	<p>The password for the individual keys in the keystore file required for secure communication.</p>
Connection Retry Period	<p>Number of seconds the Secure Agent attempts to reconnect to the Oracle database if the connection fails. If the Secure Agent can't connect to the database in the retry period, the operation fails.</p> <p>Used for all operations. Default is 0.</p>

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, <code>ConnectionRetryCount=2;</code>  <code>ConnectionRetryDelay=20</code></p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the JDBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;</code>  <code>EncryptionLevel=accepted;DataIntegrityLevel=accepted;</code>  <code>DataIntegrityTypes=SHA1</code></p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver to run mappings.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, <code>charset=sjis;readtimeout=180</code></p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the ODBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;EncryptionLevel=1;</code>  <code>DataIntegrityLevel=1;DataIntegrityTypes=SHA1;</code>  <code>DataIntegrityTypes=SHA1</code></p>

You can configure the following Oracle-specific custom properties under the Secure Agent configuration properties:

Custom property	Description
OdbcDataDirectNonWapi	<p>For mappings, replication tasks, synchronization tasks, and mapping tasks that use relational multibyte data, add the <code>OdbcDataDirectNonWapi</code> property and set the property to 0 to process Unicode data.</p> <p><b>Note:</b> When you set this property to 0, the processing time of single-byte data might increase.</p> <p>Enter the following values:</p> <ul style="list-style-type: none"> <li>- For Type, select <b>DTM</b>.</li> <li>- For Sub-type, select <b>INFO</b>.</li> <li>- For Name, enter <code>OdbcDataDirectNonWapi</code>.</li> <li>- For Value, enter 0.</li> </ul>
oracle.use.varchar.for.number	<p>For mappings, replication tasks, synchronization tasks, and mapping tasks that have an Oracle source and a Salesforce target, set the <code>oracle.use.varchar.for.number</code> custom property if the Oracle source contains many fields with the Number data type. Values for fields with the Number data type don't load correctly in Salesforce.</p> <p>Enter the following values:</p> <ul style="list-style-type: none"> <li>- For Type, select <b>Tomcat</b>.</li> <li>- For Name, enter <code>oracle.use.varchar.for.number</code>.</li> <li>- For Value, enter <code>true</code>.</li> </ul>

# Oracle CRM Cloud V1 connections properties

The following table describes the Oracle CRM Cloud V1 connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Endpoint URL	The URL of CRM application server.
Authentication Type	The type of user authentication to connect to the Oracle CRM Cloud application. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Authentication</li><li>- JWT Authentication</li></ul>
Username	The user name of the Oracle CRM Cloud account.
Password	The password for the Oracle CRM Cloud account.
JWT ID	The ID of the JWT authentication type. Enter the JWT ID if you select the authentication type as <b>JWT Auth</b> .
REST API Version	The version number of the CRM REST API.

# Oracle CRM On Demand connection properties

When you create an Oracle CRM On Demand connection, you must configure the connection properties.

The following table describes the Oracle CRM On Demand connection properties:

Connection property	Description
User Name	Oracle CRM On Demand user name. Use the following format: <domain>/<user_name> For example: domain/jsmith@companyname.com
Password	Oracle CRM On Demand password.
Service URL	URL of the Oracle CRM On Demand service. For example: <a href="https://secure-company.crmondemand.com">https://secure-company.crmondemand.com</a>

# Oracle Database Ingestion connection properties

When you define an Oracle Database Ingestion connection for a database ingestion task, you must configure connection properties.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Oracle Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
User Name	User name for the Oracle database login. The user name cannot contain a semicolon.
Password	Password for the Oracle database login. The password cannot contain a semicolon.
Host	Host name of the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Schema	Schema used for the Oracle connection.
Code Page	The code page of the database server. Database ingestion tasks use the UTF-8 code page. Default is UTF-8.

Property	Description
Encryption Method	<p>For initial load jobs, determines whether the data exchanged between the Secure Agent and the Oracle database server is encrypted:</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>- <b>SSL</b>. Establishes a secure connection using SSL for data encryption. If the Oracle database server cannot configure SSL, the connection fails.</li> <li>- <b>No Encryption</b>. Establishes a connection without using SSL. Data is not encrypted.</li> </ul> <p>Default is No Encryption.</p>
Crypto Protocol Version	<p>If you selected SSL as the encryption method, you must specify a cryptographic protocol or a list of cryptographic protocols supported by your server to use with an encrypted connection. Options are:</p> <ul style="list-style-type: none"> <li>- SSLv2</li> <li>- SSLv3</li> <li>- TLSv1.2</li> </ul> <p>Default is TLSv1.2.</p>
Validate Server Certificate	<p>If you selected SSL as the encryption method, controls whether the Secure Agent validates the server certificate that is sent by the Oracle database server.</p> <ul style="list-style-type: none"> <li>- <b>True</b>. Validate the server certificate.</li> <li>- <b>False</b>. Do not validate the server certificate.</li> </ul> <p>Default is False.</p> <p>If you also specify the <b>Host Name in Certificate</b> property, the Secure Agent also validates the host name in the certificate.</p>
Trust Store	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the client trusts for SSL authentication.</p>
Trust Store Password	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify a password for accessing the contents of the truststore file.</p>
Host Name in Certificate	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the host name of the machine that hosts the Oracle database to provide for additional security. The Secure Agent validates the host name included the connection with the host name in the SSL certificate.</p>
Key Store	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the path and name of the keystore file. The keystore file contains the certificates that the client sends to the Oracle server in response to the server's certificate request.</p>

Property	Description
Key Store Password	If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keystore file.
Key Password	If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keys in the keystore file. Use this property when the keys have a different password than the keystore file.
Database Connect String	A TNS name, an Oracle Net keyword-value pair, or a SQL connect string URL that OCI uses to connect to Oracle.
TDE Wallet Directory	<p>The path to the directory that contains the Oracle wallet file used for Oracle Transparent Data Encryption (TDE). Specify this property value only if you capture change data from TDE-encrypted tablespaces and one of the following conditions are true:</p> <ul style="list-style-type: none"> <li>- The Oracle wallet is not available to the database.</li> <li>- The Oracle database is running on a server that is remote from Oracle redo logs.</li> <li>- The wallet directory is not in the default location on the database host or the wallet name is not the default name of ewallet.p12.</li> <li>- The wallet directory is not available to the Secure Agent host.</li> </ul>
TDE Wallet Password	A clear text password that is required to access the Oracle TDE wallet and get the master key. This property value is required if you need to read and decrypt data from TDE-encrypted tablespaces in the Oracle source database.
Directory Substitution	<p>A local path prefix to substitute for the server path prefix of the redo logs on the Oracle server. This substitute local path is required when the log reader runs on a system other than the Oracle server and uses a different mapping to access the redo log files. Use this property in the following situations:</p> <ul style="list-style-type: none"> <li>- The redo logs reside on shared disk.</li> <li>- The redo logs have been copied to a system other than the Oracle system.</li> <li>- The archived redo logs are accessed by using a different NFS mount.</li> </ul> <p><b>Note:</b> Do not use this statement if you use Oracle Automatic Storage Management (ASM) to manage the redo logs.</p> <p>You can define one or more substitutions. Use the following format:</p> <pre>server_path_prefix,local_path_prefix;server_path_prefix,local_path_prefix;...</pre>

Property	Description
Reader Active Log Mask	<p>A mask that the log reader uses for selecting active redo logs when the Oracle database uses multiplexing of redo logs. The log reader compares the mask against the member names in an active redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Reader Archive Destination 1	<p>The primary log destination from which the log reader reads archived logs, when Oracle is configured to write more than one copy of each archived redo log. Enter a number that corresponds to a <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10.</p> <p>If you set only one of the Reader Archive Destination 1 and Destination 2 properties, the log reader uses that property setting. If you specify neither property, the archive log queries are not filtered by the log destination.</p>
Reader Archive Destination 2	<p>The secondary log destination from which the log reader reads archived logs when the primary destination becomes unavailable or when the logs at the primary destination cannot be read. For example, logs might have been corrupted or deleted. Enter a number that corresponds to the <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10. Usually, this value is a number greater than 1.</p>
Reader ASM Connect String	<p>In an Oracle ASM environment, the Oracle connection string, defined in TNS, that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p>
Reader ASM User Name	<p>In an Oracle ASM environment, an Oracle user ID that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database. This user ID must have SYSDBA or SYSASM authority. To use SYSASM authority, set the <b>Reader ASM Connect As SYSASM</b> property to Y.</p>
Reader ASM Password	<p>In an Oracle ASM environment, a clear text password for the user that is specified in the <b>Reader ASM User Name</b> property. The log reader uses this password and the ASM user name to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p>
Reader ASM Connect As SYSASM	<p>If you use Oracle 11g ASM or later and want the log reader to use a user ID that has SYSASM authority to connect to the ASM instance, select this check box. Also specify a user ID that has SYSASM authority in the <b>Reader ASM User Name</b> property. To use a user ID that has SYSDBA authority, clear this check box. By default, this check box is cleared.</p>

Property	Description
Reader Mode	<p>Indicates the source of and types of Oracle redo logs that the log reader reads. Valid options are:</p> <ul style="list-style-type: none"> <li>- <b>ACTIVE</b>. Read active and archived redo logs from the Oracle online system. Optionally, you can use the <b>Reader Active Log Mask</b> property to filter the active redo logs and use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVEONLY</b>. Read only archived redo logs. Optionally, you can use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVECOPY</b>. Read archived redo logs that have been copied to an alternate file system. Use this option in the following situations: <ul style="list-style-type: none"> <li>- You do not have the authority to access the Oracle archived redo logs directly.</li> <li>- The archived redo logs are written to ASM, but you do not have access to ASM.</li> <li>- The archived log retention policy for the database server causes the archived logs to not be retained long enough.</li> </ul> <p>With this option, the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties are ignored.</p> <p>Default is <b>ACTIVE</b>.</p> </li> </ul>
Reader Standby Log Mask	<p>A mask that the log reader uses for selecting redo logs for an Oracle physical standby database when the database uses multiplexing of redo logs. The log reader compares the mask against the member names in an redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Standby Connect String	<p>An Oracle connection string, defined in TNS, that the log reader uses to connect to the Oracle physical standby database for change capture when the database is not open with read only access.</p>
Standby User Name	<p>A user ID that the log reader uses to connect to the Oracle physical standby database for change capture. This user ID must have SYSDBA authority.</p>
Standby Password	<p>A password that the log reader uses to connect to the Oracle physical standby database for change capture.</p>

Property	Description
RAC Members	<p>The maximum number of active redo log threads, or <i>members</i>, in an Oracle Real Application Cluster (RAC) that can be tracked. For a Data Guard physical standby database that supports a primary database in a RAC environment, this value is the number of active threads for the primary database.</p> <p>Valid values are 1 to 100. Default is 0, which causes an appropriate number of log threads to be determined automatically. If this value is not appropriate for your environment, set this property to a value greater than 0.</p>
BFILE Access	<p>Select this check box in the following circumstances:</p> <ul style="list-style-type: none"> <li>- You use BFILE access to redo logs in physical directories on the local Oracle server file system. BFILE access uses Oracle directory objects to remotely access the redo logs in the file system. This method is an alternative to other log access methods such as ASM or NFS mounts.</li> <li>- You have an Amazon Relational Database Service (RDS) for Oracle source. In this case, this option enables access to the redo logs of a cloud-based database instance deployed in RDS.</li> </ul> <p>By default, this check box is cleared.</p>

## Oracle E-Business Suite connection properties

When you create an Oracle E-Business Suite connection, you must configure the connection properties.

The following table describes the Oracle E-Business Suite connection properties:

Property	Description
Runtime environment	The name of the runtime environment where you want to run the tasks.
Username	The username of the Oracle E-Business Suite account.
Password	The password of the Oracle E-Business Suite account.
Service Config Name	<p>The name of configuration file along with the file extension. For example, EBSWSDLConfig.ini</p> <p>In the configuration file, the first line must contain the URL for user authentication. For example, <code>http://HostName:Port Number/web services/SOAPProvider/plsql/fnd_user_pkg/?wsdl</code></p> <p><b>Note:</b> You must configure the configuration file before you create a new Oracle E-Business Suite connection in the following location: &lt;Secure Agent installation directory&gt;\apps\&lt;Data Integration Server&gt;\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\EBSMidStream</p>

# Oracle E-Business Suite Interface connection properties

When you create an Oracle E-Business Suite Interface connection, you must configure the connection properties.

The following table describes the Oracle E-Business Suite Interface connection properties:

Property	Description
Runtime environment	The name of the runtime environment where you want to run the tasks.
Oracle Host Name	Enter the required Oracle host name.
Oracle Port No	Enter the port number.
Oracle Service Name	Enter the Oracle service name.
Username	The username of the Oracle E-Business Suite Interface account.
Password	The password of the Oracle E-Business Suite Interface account.
Application Username	Enter the application user name of the Oracle E-Business Suite Interface account.

Property	Description
Service Config File Name	<p>The name of configuration file along with the file extension.</p> <p>For example, EBSInterfaceTablesConfig.ini</p> <p>You need the configuration file to set up connection properties to the Oracle E-Business Suite and to add interface table names.</p> <p><b>Note:</b> The interface table names are used only in write operations.</p> <p>You must place the configuration file in the following directory: &lt;Secure Agent installation directory&gt;\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\oraclEBS\</p> <p>The configuration file must be in the following format:  Schema, Concurrent Program Name,  FALSE_TABLELIST_Customer Interface table 1,  Customer Interface table 2....Customer  Interface table n.</p> <p>For example,  AR,RACUST,CustomerInterface,FALSE_TABLELIST_  RA_CUSTOMERS_INTERFACE_ALL,RA_CUSTOMER_PROFI  LES_INT_ALL.</p>
Parameter Config File Name	<p>The name of configuration file along with the file extension.</p> <p>For example, EBSConcurrentProgramConfig.ini</p> <p>You need the configuration file to pass parameters to call the concurrent programs.</p> <p><b>Note:</b> This configuration file is used only in write operation.</p> <p>You must place the configuration file in the following directory: &lt;Secure Agent installation directory&gt;\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\oraclEBS\</p> <p>The configuration file must be in the following format:  Name of the Module_ PARAMLIST_Parameter List  Start, Parameter 1, Parameter2....,  Parameter n, Parameter List End.</p> <p>For example,  CustomerInterface_PARAMLIST_Parameter List  Start,  CREATE_RECIPROCAL_CUSTOMER :=N,ORG_ID :=204,  Parameter List End.</p>

# Oracle Financials Cloud connections properties

The following table describes the Oracle Financials Cloud connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication	Select <b>Oracle Financials Cloud</b> .
ERP Endpoint URL	The endpoint URL of ERP server of the Oracle Financials Cloud application.
Authentication Type	Select the authentication method that the connector must use to login to the Oracle Financials Cloud application. You can select <b>Basic Authentication</b> type.
Username	User name of the Oracle Financials Cloud account.
Password	Password for the Oracle Financials Cloud account.
IO Directory	<p>The directory path where the schema files and data are stored on the machine where the Secure Agent is installed.</p> <p>You must click the <b>Test</b> button after you create an Oracle Financials Cloud connection.</p> <p>The Secure Agent creates following directories under the IO directory:</p> <ul style="list-style-type: none"> <li>- <b>Reader</b>: The reader directory contains an <b>Output</b> sub-directory. The CSV file that you download from the Oracle Financials Cloud application are downloaded as a zip file and stored in the following directory: <code>IO Directory\Reader\Output</code></li> <li>- <b>Note</b>: You can override the directory path where you download the CSV file in the <b>Outbound_Output_Directory</b> advanced property field.</li> <li>- <b>Writer</b>: The writer directory contains <b>Logs</b> and <b>Schema</b> sub-directories. You must place all the XLSM and CTL files after you download them in the following directory: <code>IO Directory\Writer\Schema</code></li> <li>- <b>Temp</b>: The temp directory contains a <b>WorkingDirectory</b> sub-directories that contains the staging files before loading.</li> </ul>
Encryption Mode	<p>Method you want to use to encrypt or decrypt the data based on the encryption method. Select one of the following options:</p> <p><b>NONE</b></p> <p>The data is not encrypted.</p> <p><b>PGPUNSIGNED</b></p> <p>Select this option to encrypt the data using the PGP encryption method.</p> <p>You must use the same encryption key that you configured in the Oracle Financials Cloud application.</p> <p><b>PGPSIGNED</b></p> <p>Select this option to encrypt and sign the data using the PGP encryption method.</p> <p><b>Note</b>: Use this property when you run a mapping to write data to a target.</p>
PassPhrase	<p>Provide the passphrase that you use to encrypt the private key.</p> <p><b>Note</b>: Use this property when you use the PGPSigned encryption method and run a mapping to write data to a target.</p>

Connection property	Description
PrivateKey Path	<p>The file path where the private key is stored on the machine where the Secure Agent is installed.</p> <p>You must provide the private key corresponding to the public key that you uploaded in Oracle Financials Cloud application.</p> <p><b>Note:</b> Use this property when you use the PGPSigned encryption method and run a mapping to write data to a target.</p>
ERP Public Key Path	<p>The file path where the fusion public key is stored on the machine where the Secure Agent is installed.</p> <p>You must raise a service request to Oracle Financials Cloud to retrieve the fusion public key.</p> <p><b>Note:</b> Use this property when you run a mapping to write data to a target.</p> <p>For more information about the fusion public key, refer the Oracle documentation.</p>
ERP Private Key Alias Name	<p>The fusion key alias name that you have generated with the Private-Public key pair in the Oracle Financials application.</p> <p><b>Note:</b> Use this property when you run a mapping to write data to a target.</p>
Customer Public Key Alias Name	<p>The customer public key alias name that you have uploaded with the public key in the Oracle Financials application.</p> <p><b>Note:</b> Use this property when you use the PGPSigned encryption method and run a mapping to write data to a target.</p>

## Oracle Financials Cloud V1 connections properties

The following table describes the Oracle Financials Cloud V1 connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
ERP Endpoint URL	<p>The endpoint URL of the Oracle Financials application server.</p> <p><b>Note:</b> To validate the ERP Endpoint URL, type the following URL in the web browser:            &lt;ERP Endpoint URL&gt;/publicFinancialCommonExpIntegration/ErpIntegrationService?WSDL</p> <p>The URL should open a WSDL file which indicates that the ERP Endpoint URL is valid.</p>
Authentication Type	<p>The type of user authentication to connect to the Oracle Financials Cloud application.</p> <p>You can select <b>Basic Authentication</b> type.</p>
Username	User name of the Oracle Financials Cloud account.
Password	Password for the Oracle Financials Cloud account.

Connection Property	Description
IO Directory	<p>The directory path where the schema files and data are stored. You must store the schema files in the machine on which the Secure Agent is installed.</p> <p>You must click the <b>Test</b> button after you create an Oracle Financials Cloud V1 connection.</p> <p>The Secure Agent creates following directories under the IO directory:</p> <ul style="list-style-type: none"> <li>- <b>Reader:</b> The reader directory contains an <b>Output</b> sub-directory. The .cvs file that you download from the Oracle Financials Cloud application are downloaded as a zip file and stored in the following directory: <code>IO Directory\Reader\Output</code></li> <li>- <b>Note:</b> You can override the directory path where you download the CSV file in the <b>Outbound_Output_Directory</b> advanced property field.</li> <li>- <b>Writer:</b> The writer directory contains <b>Logs</b> and <b>Schema</b> sub-directories. You must place all the XLSM and CTL files after you download them in the following directory: <code>IO Directory\Writer\Schema</code></li> <li>- <b>Temp:</b> The temp directory contains a <b>WorkingDirectory</b> sub-directories that contains the staging files before loading.</li> </ul>
Encryption Mode	<p>The encryption type you want to use to encrypt or decrypt the data when you run a mapping to write data to a target. Select one of the following options:</p> <p><b>NONE</b></p> <p>The data is not encrypted.</p> <p><b>PGPUNSIGNED</b></p> <p>Select this option to encrypt the data when you run a mapping to write data to a target using the PGP encryption method.</p> <p>You must use the same encryption key that you configured in the Oracle Financials Cloud application.</p> <p><b>PGPSIGNED</b></p> <p>Select this option to encrypt and sign the data when you run a mapping to write data to a target using the PGP encryption method.</p>
PassPhrase	<p>The passphrase that you use to encrypt the private key.</p> <p><b>Note:</b> Use this property when you use the PGPSigned encryption method.</p>
PrivateKey Path	<p>The file path of the private key. You must store the private key in the machine on which the Secure Agent is installed.</p> <p>You must provide the private key corresponding to the public key that you uploaded in Oracle Financials Cloud application.</p> <p><b>Note:</b> Use this property when you use the PGPSigned encryption method.</p>
ERP Public Key Path	<p>The file path of the fusion public key. You must store the fusion public key in the machine on which the Secure Agent is installed. You can use the file path of the fusion public key when you run a mapping to write data to a target.</p> <p>You must raise a service request to Oracle Financials Cloud to retrieve the fusion public key. For more information about the fusion public key, refer the Oracle documentation.</p>
ERP Private Key Alias Name	<p>The fusion key alias name that you provided when you generated the private-public key pair in the Oracle Financials application. You can use the fusion key alias name when you run a mapping to write data to a target.</p>
Customer Public Key Alias Name	<p>The customer public key alias name that you have provided when you uploaded the public key in the Oracle Financials application.</p> <p><b>Note:</b> Use this property when you use the PGPSigned encryption method.</p>

# Oracle Fusion Cloud Mass Ingestion connection properties

When you set up an Oracle Fusion Cloud Mass Ingestion connection, you must configure the connection properties.

**Note:** Oracle Fusion Cloud Mass Ingestion connections can access the data of only Enterprise Resource Planning (ERP) and Oracle Supply Chain and Manufacturing (SCM) modules of Oracle Fusion Cloud Applications Suite.

The following table describes the connection properties for an Oracle Fusion Cloud Mass Ingestion connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Authentication	Authentication method of the connection. By default, the connection uses the Basic authentication method.
User Name	User name of the Oracle Cloud account.
Password	Password for the Oracle Cloud account.
Server URL	URL of the Oracle Cloud service that you want to access.
API Version	Version of the Oracle Cloud REST API that you want to use for the connection. Optional for the BICC replication approach.

# Oracle HCM Cloud connection properties

When you create an Oracle HCM Cloud connection, you must configure the connection properties.

The following table describes the Oracle HCM Cloud connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication	Select <b>Oracle HCM Cloud</b> .
WebCenter Content URL	The URL of WebCenter Content Server where Oracle HCM Cloud uploads the output XML data.

Connection property	Description
HCM URL	<p>The URL of HCM Application Server that contains newly created data after the Secure Agent loads the XML data from the WebServer Content Server to the HCM Application Server.</p> <p>The following URL shows a sample HCM URL: <a href="https://adc-xxx-hcm.oracledemo.com/">https://adc-xxx-hcm.oracledemo.com/</a></p> <p><b>Note:</b> Applicable when you create an Oracle HCM Cloud connection to write data to an Oracle HCM Cloud application.</p>
Authentication Type	<p>Select the authentication method that the connector must use to login to the Oracle HCM Cloud application.</p> <p>You can select <b>Basic Authentication</b> type.</p>
Username	User name of the Oracle HCM Cloud account.
Password	Password for the Oracle HCM Cloud account.
Schema Directory	<p>The directory path where HCM extract definitions XSD, XLS, and <code>FlexFieldReport.xls</code> files are stored on the machine where the Secure Agent is installed.</p> <p>You must click the <b>Test</b> button after you create an Oracle HCM Cloud connection. The Secure Agent creates following directories under the schema directory:</p> <p><b>Reader</b></p> <p>The reader directory contains the XSD files. You must place all the XSD files after you generate them under the reader directory.</p> <p><b>Writer</b></p> <p>The writer directory contains the XLS files. You must place all the XLS and <code>FlexFieldReport.xls</code> files after you download them under the writer directory.</p> <p><b>Temp</b></p> <p>The temp directory contains the staging files before loading.</p>
Encryption Mode	<p>Method you want to use to encrypt or decrypt the data based on the encryption method. Select one of the following options:</p> <p><b>NONE</b></p> <p>The data is not encrypted.</p> <p><b>PGPUNSIGNED</b></p> <p>Select this option to encrypt or decrypt the data using the PGPUnsigned encryption method.</p> <p><b>PGPSIGNED</b></p> <p>Select this option to encrypt or decrypt the data using the PGPSigned encryption method.</p> <p><b>Note:</b> When you read data from an Oracle HCM Cloud source, you must specify the same <b>Encryption Mode</b> option that you used in the Oracle HCM Cloud application.</p>
PrivateKey Passphrase	<p>Provide the passphrase that you use to encrypt the private key.</p> <p>For more information about the private key passphrase, refer the Oracle documentation.</p>
PrivateKey Path	<p>The file path where the private key is stored on the machine where the Secure Agent is installed.</p> <p><b>Note:</b> You must provide the private key corresponding to the public key that you uploaded in the Oracle HCM Cloud application.</p>

Connection property	Description
Fusion PublicKey Path	The file path where the fusion public key is stored on the machine where the Secure Agent is installed. <b>Note:</b> You must raise a service request to Oracle HCM Cloud to retrieve the fusion public key. For more information about the fusion public key, refer the Oracle documentation.
Submit Extract	Submits the HCM extract definitions with the parameter values that you provide in the request message. Default is disabled.  When you use the <b>Submit Extract</b> option, the Secure Agent submits the instance of the HCM extract definition that you provide and downloads the latest output data file corresponding to the HCM extract definition from the WebCenter Content Server.  You can also submit the HCM extract definitions from the Oracle HCM Cloud application directly. <b>Note:</b> This property is applicable when you read data from the Oracle HCM Cloud application.

## Oracle HCM Cloud V1 connection properties

When you create an Oracle HCM Cloud V1 connection, you must configure the connection properties.

The following table describes the Oracle HCM Cloud V1 connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
WebCenter Content URL	The URL of WebCenter Content Server where Oracle HCM Cloud uploads the output XML data. <b>Note:</b> To validate the WebCenter Content URL, type the following URL in the web browser: <Webcenter Content URL>/idcws/GenericSoapPort?WSDL If the URL opens a WSDL file then the WebCenter Content URL is valid.
HCM URL	The URL of HCM Application Server that contains newly created data after the Secure Agent loads the XML data from the WebServer Content Server to the HCM Application Server. The following URL shows a sample HCM URL: <a href="https://adc-xxx-hcm.oracleledemo.com/">https://adc-xxx-hcm.oracleledemo.com/</a> To validate the HCM URL, type the following URL in the web browser: <HCM URL>/hcmProcFlowCoreController/FlowActionsService?WSDL If the URL opens a WSDL file then the HCM URL is valid. <b>Note:</b> Applicable when you create an Oracle HCM Cloud V1 connection to write data to an Oracle HCM Cloud application or when you select <b>Submit Extract</b> in the connection properties.
Authentication Type	The type of user authentication to connect to the Oracle HCM Cloud application. You can select <b>Basic Authentication</b> type.
Username	User name of the Oracle HCM Cloud account.
Password	Password for the Oracle HCM Cloud account.

Connection Property	Description
Schema Directory	<p>The directory path where HCM extract definitions XSD and XLSX are stored on the machine where the Secure Agent is installed.</p> <p>You must click the <b>Test</b> button after you create an Oracle HCM Cloud V1 connection. The Secure Agent creates following directories under the schema directory:</p> <p><b>Reader</b></p> <p>The reader directory contains the XSD files. You must place all the XSD files after you generate them under the reader directory.</p> <p><b>Writer</b></p> <p>The writer directory contains the XLSX files. You must place all the XLSX files after you download them under the writer directory.</p> <p><b>Temp</b></p> <p>The temp directory contains the staging files before loading.</p>
Encryption Mode	<p>The encryption type you want to use to encrypt or decrypt the data. Select one of the following options:</p> <p><b>NONE</b></p> <p>The data is not encrypted.</p> <p><b>PGPUNSIGNED</b></p> <p>Select this option to encrypt or decrypt the data using the PGPUnsigned encryption method.</p> <p><b>PGPSIGNED</b></p> <p>Select this option to encrypt or decrypt the data using the PGPSigned encryption method.</p> <p><b>Note:</b> When you read data from an Oracle HCM Cloud V1 source, you must specify the same <b>Encryption Mode</b> option that you used in the Oracle HCM Cloud application.</p>
PrivateKey Passphrase	<p>The passphrase that you used to encrypt the private key.</p> <p>For more information about the private key passphrase, refer the Oracle documentation.</p>
PrivateKey Path	<p>Enter the file path of the private key. You must store the private key in the machine on which the Secure Agent is installed.</p> <p><b>Note:</b> You must provide the private key corresponding to the public key that you uploaded in the Oracle HCM Cloud application.</p>
Fusion PublicKey Path	<p>The file path of the fusion public key. You must store the fusion public key in the machine on which the Secure Agent is installed.</p> <p><b>Note:</b> You must raise a service request to Oracle HCM Cloud to retrieve the fusion public key. For more information about the fusion public key, refer the Oracle documentation.</p>
Submit Extract	<p>Submits the HCM extract definitions with the parameter values that you provide in the request message. Default is disabled.</p> <p>When you use the <b>Submit Extract</b> option, the Secure Agent submits the instance of the HCM extract definition that you provide and downloads the latest output data file corresponding to the HCM extract definition from the WebCenter Content Server.</p> <p>You can also submit the HCM extract definitions from the Oracle HCM Cloud application directly.</p> <p><b>Note:</b> This property is applicable when you read data from the Oracle HCM Cloud application.</p>

# PostgreSQL CDC connection properties

When you configure a PostgreSQL CDC connection, you must set the connection properties.

The following table describes PostgreSQL CDC connection properties:

Property	Description
Connection Name	<p>A name for the PostgreSQL CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code>.</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the PostgreSQL CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For PostgreSQL CDC, the type must be <b>PostgreSQL CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for PostgreSQL change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>MYSCDC1A:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	PostgreSQL instance name that is specified in the <b>Instance</b> field of the registration group that contains capture registrations for the PostgreSQL source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.

Property	Description
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>
Map Location	<p>Host name or IP address of the system that contains the extraction maps. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>PSQCDC2B:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	<p>A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.</p>
Map Location Password	<p>Password associated with the user name that is specified in <b>Map Location User</b> property.</p>
Event Table	<p>If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a PostgreSQL table on the CDC source system.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the the PowerExchange Client for PowerCenter (PWXPC) PostgreSQL CDC connections in PowerCenter.</p>

# PostgreSQL connection properties

When you set up a PostgreSQL connection, configure the connection properties.

The following table describes the PostgreSQL connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Select PostgreSQL from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or in a serverless runtime environment.
Host Name	Host name of the PostgreSQL server to which you want to connect.
Port	Port number for the PostgreSQL server to which you want to connect. Default is 5432.
Schema	The schema name. If you don't specify the schema name, all the schemas available in the database are listed while importing the source object in Data Integration.
Database	The PostgreSQL database name.
User Name	User name to access the PostgreSQL database.
Password	Password for the PostgreSQL database user name.
Encryption Method	Determines whether the data exchanged between the Secure Agent and the PostgreSQL database server is encrypted. Select one of the following encryption methods: <ul style="list-style-type: none"><li>- noEncryption. Establishes a connection without using SSL. Data is not encrypted.</li><li>- SSL. Establishes a connection using SSL. Data is encrypted using SSL. If the PostgreSQL database server can't configure SSL, the connection fails.</li><li>- requestSSL. Attempts to establish a connection using SSL. If the PostgreSQL database server can't configure SSL, the Secure Agent establishes an unencrypted connection.</li></ul> Default is noEncryption. <b>Note:</b> SSL is not applicable when you use the Hosted Agent. You can configure SSL when you use the Secure Agent or the serverless runtime environment.
Validate Server Certificate	Applicable if you select SSL or requestSSL as the encryption method. Select the Validate Server Certificate option so that the Secure Agent validates the server certificate that is sent by the PostgreSQL database server. If you specify the Host Name In Certificate property, the Secure Agent also validates the host name in the certificate.

Property	Description
TrustStore	<p>Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option.</p> <p>The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
TrustStore Password	<p>Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option.</p> <p>The password to access the truststore file that contains the SSL certificate.</p>
Host Name In Certificate	<p>Optional when you select SSL or requestSSL as the encryption method and the Validate Server Certificate option.</p> <p>A host name for providing additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
KeyStore	<p>Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server.</p> <p>The path and the file name of the key store. The keystore file contains the certificates that the PostgreSQL client sends to the PostgreSQL server in response to the server's certificate request.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</pre>
KeyStore Password	<p>Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server.</p> <p>The password for the keystore file required for secure communication.</p>
Key Password	<p>Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server.</p> <p>Required when individual keys in the keystore file have a different password than the keystore file.</p>
Additional Connection Properties	<p>Additional connection parameters that you want to use.</p> <p>Provide the connection parameters as semicolon-separated key-value pairs.</p>
Crypto Protocol Versions	<p>Required if you select SSL or requestSSL as the encryption method.</p> <p>A cryptographic protocol or a list of cryptographic protocols to use with an encrypted connection. You can select one of the following protocols:</p> <ul style="list-style-type: none"> <li>- SSLv3</li> <li>- TLSv1_2</li> </ul> <p>Default is TLSv1_2.</p>

# QuickBooks V2 Connection Properties

When you set up a QuickBooks V2 connection, you must configure the connection properties.

The following table describes the QuickBooks V2 connection properties:

Connection Property	Description
Username	Username of the QuickBooks account.
Password	Password of the QuickBooks account.
Connection URL	The Connection URL to connect to the QuickBooks application.
Schema	The value of Schema is set to default automatically.
QBXML version	QBXML version of the QuickBooks. The default QBXML version is 6.0.
Enable Logging	Enable logging to see the session logs of tasks.

## Redis connection properties

When you create a Redis connection, you must configure the connection properties.

The following table describes the Redis connection properties:

Property	Description
Connection Name	The 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Redis connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Redis server.
Port	Redis server port number.
User	Username to access the Redis server.

Property	Description
Password	Password to access the Redis server.
Max Clients Per Worker	The maximum number of Redis client connections used by each worker node.
Flat Hierarchy	Enable this property to perform the following actions based on the data that you read: <ul style="list-style-type: none"> <li>- Read top-level HASH keys as multiple rows with one row for each key-value pair in the hash.</li> <li>- Read top-level LIST keys as multiple rows with one row for each string value in the list.</li> </ul>
Use TLS	Uses TLS to secure the communication with Redis server.
KeyStore File Path	Absolute path of the KeyStore file in the Secure Agent machine that contains private keys and certificates for the Redis server.
KeyStore Passphrase	Passphrase for the KeyStore file.
TrustStore File Path	Absolute path of the TrustStore file that contains certificates for the Redis server.
TrustStore Passphrase	Passphrase for the TrustStore file.

## REST V2 connection properties

When you set up a REST V2 connection, you must configure the connection properties.

The following table describes the REST V2 connection properties for a Standard authentication type connection:

Connection 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The REST V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.

Connection property	Description
Authentication	The authentication method that the REST V2 Connector must use to connect to the REST endpoint. Select <b>Standard</b> .
Authentication Type	The authentication type that you can use when you select the Standard authentication. You can select one of the following authentication types: <ul style="list-style-type: none"> <li>- BASIC</li> <li>- DIGEST</li> <li>- OAUTH</li> <li>- NONE</li> </ul> Default is <b>NONE</b> .
Auth User ID	The user name to log in to the web service application when you select the Standard authentication. Digest authentication is not applicable.
Auth Password	The password associated with the user name when you select the Standard authentication. Digest authentication is not applicable.
OAuth Consumer Key	The client key associated with the web service application. Required only for OAuth authentication type.
OAuth Consumer Secret	The client password to connect to the web service application. Required only for OAuth authentication type.
OAuth Token	The access token to connect to the web service application. Required only for OAuth authentication type.
OAuth Token Secret	The password associated with the OAuth token. Required only for OAuth authentication type.
Swagger File Path	The path of the Swagger file or OpenAPI file. You can specify one of the following file paths: <ul style="list-style-type: none"> <li>- Absolute path along with the file name</li> <li>- Hosted URL</li> </ul> If you provide the absolute path of the Swagger file or OpenAPI file, the file must be located on the Secure Agent machine. The hosted URL must return the content of the file without prompting for further authentication and redirection. For example, the path of the Swagger file can be: C:\Swagger\sampleSwagger.json The user must have the read permission for the folder and the file.

Connection property	Description
TrustStore File Path	<p>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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;\jre\lib\security\cacerts.</pre> <p>For the serverless runtime environment, specify the truststore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
TrustStore Password	<p>The password for the truststore file that contains the SSL certificate.</p> <p>You can also configure the truststore password as a JVM option.</p>
KeyStore File Path	<p>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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the keystore file name and location as a JVM option or import the certificate to any directory.</p> <p>For the serverless runtime environment, specify the keystore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
KeyStore Password	<p>The password for the keystore file required for secure communication.</p> <p>You can also configure the keystore password as a JVM option.</p>
Proxy Type	<p>Type of proxy. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Proxy. Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy. Considers the proxy configured in the agent.</li> <li>- Custom Proxy. Considers the proxy configured in the connection properties.</li> </ul>

Connection property	Description
Proxy Configuration	<p>The format required to configure proxy.</p> <p>You can configure proxy using the following format: <code>&lt;host&gt;:&lt;port&gt;</code></p> <p>You cannot configure an authenticated proxy server.</p>
Advanced Fields	<p>Enter the arguments that the agent uses when connecting to a REST endpoint.</p> <p>You can specify the following arguments, each separated by a semicolon (;):</p> <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout</b>. The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API.</li> <li>- <b>Note</b>: If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime</b>. The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts</b>. Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema</b>. Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <p>For example,</p> <pre>connectiondelaytime:10000;retryattempts:5</pre> <p><b>Note</b>: In a streaming ingestion task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.</p>

## OAuth 2.0 client credentials authentication

The following table describes the REST V2 connection properties for an OAuth 2.0 - Client Credentials authentication type connection:

Connection property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + ,</code>. Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The REST V2 connection type.
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>
Authentication	<p>The authentication method that the REST V2 Connector must use to connect to the REST endpoint.</p> <p>Select <b>OAuth 2.0-Client Credentials</b>.</p>
Access Token URL	Access token URL configured in your application.

Connection property	Description
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	Specifies access control if the API 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. Parameters must be defined in the JSON format. For example, [{"Name": "resource", "Value": "https://<serverName>"}]
Client Authentication	Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .
Generate Access Token	Generates access token based on the information provided in the above fields.
Access Token	Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server at the Secure Agent level. The REST V2 connection-level proxy configuration does not apply to the generate access token call.
Swagger File Path	The path of the Swagger file or OpenAPI file. You can specify one of the following file paths: - Absolute path along with the file name - Hosted URL If you provide the absolute path of the swagger file or OpenAPI file, the file must be located on the Secure Agent machine. The hosted URL must return the content of the file without prompting for further authentication and redirection. For example, the path of the swagger file can be: C:\swagger\sampleSwagger.json The user must have the read permission for the folder and the file. <b>Note:</b> In a streaming ingestion task, use only a hosted URL of the swagger specification file as the swagger file path.
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. Specify a directory path that is available on each Secure Agent machine. You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory: <Secure Agent installation directory>\jre\lib\security\cacerts. For the serverless runtime environment, specify the truststore file path in the serverless agent directory. For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks

Connection property	Description
TrustStore Password	The password for the truststore file that contains the SSL certificate. You can also configure the truststore password as a JVM option.
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. Specify a directory path that is available on each Secure Agent machine. You can also configure the keystore file name and location as a JVM option or import the certificate to any directory. For the serverless runtime environment, specify the keystore file path in the serverless agent directory. For example, <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</code>
KeyStore Password	The password for the keystore file required for secure communication. You can also configure the keystore password as a JVM option.
Proxy Type	Type of proxy. You can select one of the following options: <ul style="list-style-type: none"> <li>- No Proxy: Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy: Considers the proxy configured in the agent.</li> <li>- Custom Proxy: Considers the proxy configured in the connection properties.</li> </ul>
Proxy Configuration	The format required to configure proxy. You can configure proxy using the following format: <code>&lt;host&gt;:&lt;port&gt;</code> You cannot configure an authenticated proxy server.
Advanced Fields	Enter the arguments that the agent uses when connecting to a REST endpoint. You can specify the following arguments, each separated by a semicolon (;): <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout</b>. The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API. <b>Note:</b> If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime</b>. The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts</b>. Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema</b>. Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> For example, <code>connectiondelaytime:10000;retryattempts:5</code> <b>Note:</b> In a streaming ingestion task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.

## OAuth 2.0 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 V2 connection properties for an OAuth 2.0 - Authorization Code authentication type connection:

Connection 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The REST V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.
Authentication	The authentication method that the REST V2 Connector must use to connect to the REST endpoint. Select <b>OAuth 2.0-Authorization Code</b> .
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	Specifies access control if the API endpoint has defined custom scopes. Enter space separated scope attributes. For example, <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Parameters must be defined in the JSON format. For example, <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Parameters must be defined in the JSON format. For example, <code>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</code>
Client Authentication	Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .

Connection property	Description
Generate Access Token	Generates access token and refresh token based on the information provided in the above fields.
Access Token	Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server at the Secure Agent level. The REST V2 connection-level proxy configuration does not apply to the generate access token call.
Refresh Token	Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent fetches a new access token with the help of refresh token.  If the refresh token expires, you must either provide a valid refresh token or regenerate a new refresh token by clicking <b>Generate Access Token</b> .
Swagger File Path	The path of the Swagger file or OpenAPI file. You can specify one of the following file paths: <ul style="list-style-type: none"> <li>- Absolute path along with the file name</li> <li>- Hosted URL</li> </ul> If you provide the absolute path of the swagger file or OpenAPI file, the file must be located on the Secure Agent machine.  The hosted URL must return the content of the file without prompting for further authentication and redirection.  For example, the path of the swagger file can be: C:\swagger\sampleSwagger.json  The user must have the read permission for the folder and the file. <b>Note:</b> In a streaming ingestion task, use only a hosted URL of the swagger specification file as the swagger file path.
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. Specify a directory path that is available on each Secure Agent machine.  You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory: <code>&lt;Secure Agent installation directory&gt;\jre\lib\security\cacerts.</code>  For the serverless runtime environment, specify the truststore file path in the serverless agent directory.  For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks
TrustStore Password	The password for the truststore file that contains the SSL certificate. You can also configure the truststore password as a JVM option.
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. Specify a directory path that is available on each Secure Agent machine.  You can also configure the keystore file name and location as a JVM option or import the certificate to any directory.  For the serverless runtime environment, specify the keystore file path in the serverless agent directory.  For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks

Connection property	Description
KeyStore Password	The password for the keystore file required for secure communication. You can also configure the keystore password as a JVM option.
Proxy Type	Type of proxy. You can select one of the following options: <ul style="list-style-type: none"> <li>- No Proxy: Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy: Considers the proxy configured in the agent.</li> <li>- Custom Proxy: Considers the proxy configured in the connection properties.</li> </ul>
Proxy Configuration	The format required to configure proxy. You can configure proxy using the following format: <host>:<port> You cannot configure an authenticated proxy server.
Advanced Fields	<p>Enter the arguments that the agent uses when connecting to a REST endpoint.</p> <p>You can specify the following arguments, each separated by a semicolon (;):</p> <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout</b>. The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API.</li> <li><b>Note:</b> If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime</b>. The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts</b>. Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema</b>. Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <p>For example,</p> <pre>connectiondelaytime:10000;retryattempts:5</pre> <p><b>Note:</b> In a streaming ingestion task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.</p>

## JWT bearer token authentication

When you set up a REST V2 connection, you must configure the connection properties.

The following table describes the REST V2 connection properties when you use JWT bearer token authentication:

Connection property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code>.</p> <p>Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The REST V2 connection type.

Connection property	Description
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>
Authentication	<p>The authentication method that the REST V2 Connector must use to connect to the REST endpoint.</p> <p>Select <b>JWT Bearer Token</b>.</p>
JWT Header	<p>JWT header in JSON format.</p> <p>Sample:</p> <pre>{   "alg": "RS256",   "kid": "xxyyzz" }</pre> <p>You can configure HS256 and RS256 algorithms.</p>
JWT Payload	<p>JWT payload in JSON format.</p> <p>Sample:</p> <pre>{   "iss": "abc",   "sub": "678",   "aud": "https://api.box.com/oauth2/token",   "box_sub_type": "enterprise",   "exp": "120",   "jti": "3ee9364e" }</pre> <p>The expiry time represented as <b>exp</b> is the relative time in seconds. The expiry time is calculated in the UTC format from the token issuer time (<i>iat</i>).</p> <p>When <i>iat</i> is defined in the payload and the expiry time is reached, mappings and Generate Access Token will fail. To generate a new access token, you must provide a valid <i>iat</i> in the payload.</p> <p>If <i>iat</i> is not defined in the payload, the expiry time is calculated from the current timestamp.</p> <p>To pass the expiry time as a string value, enclose the value with double quotes. For example:</p> <pre>"exp": "120",</pre> <p>To pass the expiry time as an integer value, do not enclose the value with double quotes.</p> <p>For example,</p> <pre>"exp": 120,</pre>
Authorization Server	<p>Access token URL configured in your application.</p>

Connection property	Description
Authorization Advanced Properties	<p>Additional parameters to use with the access token URL. Parameters must be defined in the JSON format.</p> <p>For example,</p> <pre>[{"Name": "client_id", "Value": "abc"}, {"Name": "client_secret", "Value": "abc"}]</pre>
TrustStore File Path	<p>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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;\jre \lib\security\cacerts.</pre> <p>For the serverless runtime environment, specify the truststore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
TrustStore Password	<p>The password for the truststore file that contains the SSL certificate.</p> <p>You can also configure the truststore password as a JVM option.</p>
KeyStore File Path	<p>Mandatory. 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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the keystore file name and location as a JVM option or import the certificate to any directory.</p> <p>For the serverless runtime environment, specify the keystore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
KeyStore Password	<p>Mandatory. The password for the keystore file required for secure communication.</p> <p>You can also configure the keystore password as a JVM option.</p>
Private Key Alias	<p>Mandatory. Alias name of the private key used to sign the JWT payload.</p>
Private Key Password	<p>Mandatory. The password for the keystore file required for secure communication. The private key password must be same as the keystore password.</p>

Connection property	Description
Access Token	<p>Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.</p> <p>To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server at the Secure Agent level. The REST V2 connection-level proxy configuration does not apply to the generate access token call.</p>
Swagger File Path	<p>The path of the Swagger file or OpenAPI file.</p> <p>You can specify one of the following file paths:</p> <ul style="list-style-type: none"> <li>- Absolute path along with the file name</li> <li>- Hosted URL</li> </ul> <p>If you provide the absolute path of the swagger file or OpenAPI file, the file must be located on the Secure Agent machine.</p> <p>The hosted URL must return the content of the file without prompting for further authentication and redirection.</p> <p>For example, the path of the swagger file can be:</p> <pre>C:\swagger\sampleSwagger.json</pre> <p>The user must have the read permission for the folder and the file.</p> <p><b>Note:</b> In a streaming ingestion task, use only a hosted URL of the swagger specification file as the swagger file path.</p>
Proxy Type	<p>Type of proxy. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Proxy. Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy. Considers the proxy configured in the agent.</li> <li>- Custom Proxy. Considers the proxy configured in the connection properties.</li> </ul>

Connection property	Description
Proxy Configuration	<p>The format required to configure proxy. You can configure proxy using the following format: &lt;host&gt;:&lt;port&gt;</p> <p>You cannot configure an authenticated proxy server.</p>
Advanced Fields	<p>Enter the arguments that the agent uses when connecting to a REST endpoint. You can specify the following arguments, each separated by a semicolon (;):</p> <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout</b>. The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API.</li> </ul> <p><b>Note:</b> If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</p> <ul style="list-style-type: none"> <li>- <b>connectiondelaytime</b>. The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts</b>. Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema</b>. Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <p>For example, connectiondelaytime:10000;retryattempts:5</p> <p><b>Note:</b> In a streaming ingestion task, only ConnectionTimeout and retryattempts are applicable.</p>

**Important:** The HS256 algorithm support in **JWT Header** is available for preview. Preview functionality is supported for evaluation purposes but is unwarranted and is not production-ready. Informatica recommends that you use in non-production environments only. Informatica intends to include the preview functionality in an upcoming release for production use, but might choose not to in accordance with changing market or technical circumstances. For more information, contact Informatica Global Customer Support. To use the functionality, your organization must have the appropriate licenses.

## API key authentication

When you set up a REST V2 connection, you must configure the connection properties. The API Key authentication allows you to provide a unique key and a corresponding value to authenticate API calls made to the REST endpoint.

The following table describes the REST V2 connection properties when you use API Key authentication:

Connection property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The REST V2 connection type.
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>Specify a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>
Authentication	<p>The authentication method that the REST V2 Connector must use to connect to the REST endpoint.</p> <p>Select <b>API Key</b>.</p>
Key	The unique API key that REST V2 Connector uses to authenticate the API calls made to the REST endpoint.
Value	The value corresponding to the API key that is required to make the API calls.
Add API Key to	<p>Determines if the API key and its corresponding value must be sent as a request header or a query parameter for the REST V2 Connector to make API calls to the REST endpoint.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Request Header</li> <li>- Query Parameter</li> </ul>
Swagger File Path	<p>The path of the Swagger file or OpenAPI file.</p> <p>You can specify one of the following file paths:</p> <ul style="list-style-type: none"> <li>- Absolute path along with the file name</li> <li>- Hosted URL</li> </ul> <p>If you provide the absolute path of the swagger file or OpenAPI file, the file must be located on the Secure Agent machine.</p> <p>The hosted URL must return the content of the file without prompting for further authentication and redirection.</p> <p>For example, the path of the swagger file can be:</p> <pre>C:\swagger\sampleSwagger.json</pre> <p>The user must have the read permission for the folder and the file.</p> <p><b>Note:</b> In a streaming ingestion task, use only a hosted URL of the swagger specification file as the swagger file path.</p>

Connection property	Description
TrustStore File Path	<p>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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;\jre\lib\security\cacerts.</pre> <p>For the serverless runtime environment, specify the truststore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
TrustStore Password	<p>The password for the truststore file that contains the SSL certificate.</p> <p>You can also configure the truststore password as a JVM option.</p>
KeyStore File Path	<p>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. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the keystore file name and location as a JVM option or import the certificate to any directory.</p> <p>For the serverless runtime environment, specify the keystore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
KeyStore Password	<p>The password for the keystore file required for secure communication.</p> <p>You can also configure the keystore password as a JVM option.</p>
Proxy Type	<p>Type of proxy. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Proxy: Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy: Considers the proxy configured in the agent.</li> <li>- Custom Proxy: Considers the proxy configured in the connection properties.</li> </ul>

Connection property	Description
Proxy Configuration	<p>The format required to configure proxy.</p> <p>You can configure proxy using the following format: &lt;host&gt;:&lt;port&gt;</p> <p>You cannot configure an authenticated proxy server.</p>
Advanced Fields	<p>The arguments that the agent uses when connecting to a REST endpoint.</p> <p>You can specify the following arguments, each separated by a semicolon (;):</p> <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout</b>. The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API.</li> <li>- <b>Note</b>: If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime</b>. The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts</b>. Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema</b>. Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <p>For example,</p> <pre>connectiondelaytime:10000;retryattempts:5</pre> <p><b>Note</b>: In a streaming ingestion task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.</p>

## Rules and guidelines for REST V2 connections

Consider the following rules and guidelines for Rest V2 connections:

- When you test the connection, the Secure Agent validates the following parameters:
  - Path of the local Swagger file or the URL of the hosted Swagger file.
  - JSON format of the Swagger file.

However, the Secure Agent does not validate endpoint credentials when you test the connection.

- 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 V2 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.

# 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 <b>Basic</b> . 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.
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: <ul style="list-style-type: none"><li>- None. Bypasses the proxy server configured at the agent or the connection level.</li><li>- Custom. Considers proxy configured at the connection level.</li><li>- Platform. Considers proxy configured at the agent level.</li></ul> Proxy is not applicable when you use the serverless runtime environment.

Connection property	Description
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. <b>Note:</b> 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 <b>OAuth 2.0 authorization code</b> . 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: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in the JSON format. For example: <code>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</code>
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 <b>Send client credentials in body</b> .
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 <b>Generate Access Token</b> 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.
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 <b>Generate Access Token</b> to populate the refresh token value.  If the refresh token expires, you must either provide a valid refresh token or click <b>Generate Access Token</b> to regenerate a new refresh token.

Connection property	Description
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: <ul style="list-style-type: none"> <li>- None. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Custom. Proxy configured at the connection level is considered.</li> <li>- Platform. Proxy configured at the agent level is considered.</li> </ul> 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. <b>Note:</b> 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 <b>OAuth 2.0 client credentials</b> . 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: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
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 <b>Send client credentials in body</b> .
Generate Access Token	Generates access token based on the authentication details provided.

Connection property	Description
Access Token	<p>The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.</p> <p>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.</p>
TrustStore File Path	<p>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.</p> <p>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.</p>
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	<p>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.</p> <p>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.</p>
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	<p>Type of proxy.</p> <p>You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- None. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Custom. Considers proxy configured at the connection level.</li> <li>- Platform. Considers proxy configured at the agent level.</li> </ul> <p>Proxy is not applicable when you use the serverless runtime environment.</p>
Proxy Host	<p>The IP address or host name of the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy Port	<p>The port number of the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy User	<p>The user name for the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy Password	<p>The password for the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Connection Timeout	<p>The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over.</p> <p>Default is 60 seconds.</p> <p><b>Note:</b> If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</p>

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.

# Salesforce Analytics connection properties

When you set up a Salesforce Analytics connection, you must configure the connection properties.

The following table describes the Salesforce Analytics connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	User name of the Salesforce Analytics account.
Password	Password for the Salesforce Analytics account.
Security Token	The token used to login to Salesforce Analytics from an untrusted network.
Service URL	URL of the Salesforce Analytics service that you want to access. For example: <code>https://login.salesforce.com/services/Soap/u/48.0</code> In a test or development environment, you might want to access the Salesforce Analytics Sandbox testing environment.
Temp Folder Name	The directory where the Secure Agent stores the JSON files and data archive files. After the successful execution of a task, the temporary .gz files are deleted.
Default Date Format	The date format to read date columns in the JSON file.

# Salesforce connection properties

When you set up a Salesforce connection, configure the connection properties.

The following table describes the Salesforce connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Salesforce connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Salesforce Connection Type	The type of Salesforce connection. You can select Standard or OAuth connection. <b>Important:</b> Informatica recommends you to use OAuth authentication to securely connect to Salesforce. When you use OAuth authentication, use OAuth 2.0.

The following table lists the connection properties for a standard connection type:

Property	Description
User Name	User name for the Salesforce account.
Password	Password for the Salesforce account.
Security Token	Security token generated from the Salesforce application.
Service URL	URL of the Salesforce service. For example: <code>https://login.salesforce.com/services/Soap/u/57.0</code> When you edit the service URL for an existing standard connection, you must re-enter the password and security token. Maximum length is 100 characters.
Bypass proxy server settings defined for the Secure Agent	Bypass the proxy server settings defined in the Secure Agent Manager for the Secure Agent. When you bypass the proxy server settings, you use a direct connection to Salesforce.

The following table lists the properties for an OAuth connection type:

Property	Description
OAuth Consumer Key	The consumer key that you get from Salesforce, which is required to generate a valid refresh token.
OAuth Consumer Secret	The consumer secret that you get from Salesforce, which is required to generate a valid refresh token.
OAuth Refresh Token	The refresh token generated in Salesforce using the consumer key and consumer secret.
Service URL	URL of the Salesforce service endpoint. For example: <code>https://login.salesforce.com/services/Soap/u/57.0</code> When you edit the service URL for an existing OAuth connection, you must re-enter the consumer key, consumer secret, and refresh token. Maximum length is 100 characters.

You can configure the following Salesforce-specific properties under the Secure Agent configuration properties:

Property	Type	Description
SalesForceConnectionTimeout	DTM	Number of seconds that the Salesforce web service requests to wait before it times out.
AutoAlterColumnType	Custom	For replication tasks, set the AutoAlterColumnType custom configuration property so the database target column adjusts when the data type, precision, or scale of a Salesforce source field changes. Set this property for the Secure Agent that runs the replication task. Enter the following values: <ul style="list-style-type: none"><li>- For Type, select Tomcat.</li><li>- For Sub-type, select INFO.</li><li>- For Name, enter AutoAlterColumnType.</li><li>- For Value, enter yes to turn on this property.</li></ul>

## Salesforce Marketing Cloud connection properties

When you set up a Salesforce Marketing Cloud connection, configure the connection properties.

The following table describes the Salesforce Marketing Cloud connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Salesforce Marketing Cloud connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run an application ingestion task on a Hosted Agent or serverless runtime environment.
Salesforce Marketing Cloud Url	The URL that the agent uses to connect to the Salesforce Marketing Cloud WSDL. The following URL is an example for OAuth 1.0 URL: <code>https://webservice.s7.exacttarget.com/etframework.wsdl</code> The following URL is an example for OAuth 2.0 URL: <code>https://&lt;SUBDOMAIN&gt;.soap.marketingcloudapis.com/etframework.wsdl</code>  <b>Important:</b> Salesforce is going to deprecate the OAuth 1.0 APIs by September 30 <sup>th</sup> , 2022. Informatica recommends that you upgrade to OAuth 2.0 for new and existing packages.
Username	Applies to basic authentication. The user name of the Salesforce Marketing Cloud account. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.

Property	Description
Password	Applies to basic authentication. The password for the Salesforce Marketing Cloud account. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.
Client ID	The client ID of Salesforce Marketing Cloud required to generate a valid access token.
Client Secret	The client secret of Salesforce Marketing Cloud required to generate a valid access token.
Use Proxy Server	Connects to Salesforce Marketing Cloud through proxy. <b>Note:</b> When you use a serverless runtime environment, you cannot use a proxy server to connect to Informatica Intelligent Cloud Services. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.
Enable Logging	Enables logging for the task. When you enable logging, you can view the session log for the log details. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.
UTC offset	Uses the UTC offset connection property to read data from and write data to Salesforce Marketing Cloud in the UTC offset time zone. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.
Batch Size	Number of rows that the agent writes in a batch to the target. When you insert or update data and specify the contact key, the data associated with the specified contact ID is inserted or updated in a batch to Salesforce Marketing Cloud. When you upsert data to Salesforce Marketing Cloud, do not specify the contact key. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.
Enable Multiple BU	Uses the Salesforce Marketing Cloud connection to access data across all business units. Select this option if there are multiple business units in your Salesforce Marketing Cloud account. <b>Note:</b> This property is not applicable to connections configured for application ingestion tasks.

## Salesforce Mass Ingestion connection properties

When you set up a Salesforce Mass Ingestion connection, you must configure the connection properties.

The Salesforce Mass Ingestion connection uses a connected app to access the Salesforce data. Before you configure the connection, you must configure a connected app in Salesforce to allow the connection to access the Salesforce data.

**Note:** For more information about configuring a connected app, see the Knowledge Base article [000172095](#).

The properties of a Salesforce Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0 Username-Password Flow:** Authenticates the connection by using the Salesforce account login credentials and the consumer key and consumer secret that Salesforce generates for the connected app.
- **OAuth 2.0 JWT Bearer Flow:** Authenticates the connection by using the Salesforce account user name, private key alias, private key password, and the consumer key that Salesforce generates for the connected app. Informatica recommends that you use this authentication method because this method provides secured access to Salesforce without sharing sensitive information, such as consumer secret and Salesforce account password.

## Connection properties for OAuth 2.0 Username-Password Flow authentication

The following table describes the connection properties for a Salesforce Mass Ingestion connection configured with OAuth 2.0 Username-Password Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Salesforce account.
Password	Password for the Salesforce account.
Security Token	Security token associated with the Salesforce account. You can configure the connection without specifying the security token if there are no IP restrictions specified for the connected app. However, you must specify the security token if IP restrictions are enforced for the connected app and if the Secure Agent is not running on the trusted IP range specified for your Salesforce organization. <b>Note:</b> If you do not have the security token, reset the security token in Salesforce. For more information about resetting the security token, see the <a href="#">Salesforce documentation</a> .
Consumer Key	Consumer key that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
Consumer Secret	Consumer secret that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
API Version	Version of the Salesforce API that you want to use to access the source data. Default is 51.0. <b>Note:</b> You cannot use a version older than 51.0.
OAuth token URL	OAuth 2.0 token endpoint of the Salesforce organization. The connected app sends access token requests to this endpoint. Default value is: <code>https://login.salesforce.com/services/oauth2/token</code> This default URL is used for all Salesforce instances. Alternatively, you can enter an instance-specific URL: <code>https://&lt;instance domain URL&gt;/services/oauth2/token</code> An instance-specific URL can establish a more direct and faster connection to the Salesforce host server. If the load on the common default endpoint is heavy and ingestion jobs fail with an authentication error when using it, use this alternative URL instead.

**Note:** For more information about the OAuth 2.0 Username-Password Flow authentication method, see the Salesforce documentation.

## Connection properties for OAuth 2.0 JWT Bearer Flow authentication

The following table describes the connection properties for a Salesforce Mass Ingestion connection configured with OAuth 2.0 JWT Bearer Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Salesforce account.
Consumer Key	Consumer key that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
Keystore Path	Absolute path to the keystore file that contains the X509 certificate required to validate a JSON Web Token (JWT) and establish a secure connection with Salesforce. The keystore file must be in the Java KeyStore (JKS) format.
Keystore Password	Password for the keystore file.
Private Key Alias	Alias name of the private key used to sign the JWT.
Private Key Password	Password for the private key.
API Version	Version of the Salesforce API that you want to use to access the source data. Default is 51.0. <b>Note:</b> You cannot use a version older than 51.0.
OAuth token URL	OAuth 2.0 token endpoint of the Salesforce organization. The connected app sends access token requests to this endpoint. Default value is: <code>https://login.salesforce.com/services/oauth2/token</code> This default URL is used for all Salesforce instances. Alternatively, you can enter an instance-specific URL: <code>https://&lt;instance domain URL&gt;/services/oauth2/token</code> An instance-specific URL can establish a more direct and faster connection to the Salesforce host server. If the load on the common default endpoint is heavy and ingestion jobs fail with an authentication error when using it, use this alternative URL instead.

**Note:** For more information about the OAuth 2.0 JWT Bearer Flow authentication method, see the Salesforce documentation.

# SAP ADSO Writer connection properties

Select the **SAP ADSO Writer** connection type and configure the connection properties. .

The following table describes the SAP ADSO Writer connection properties:

Connection property	Description
Runtime Environment	Runtime environment that contains the Secure Agent that you want to use to access SAP BW/4HANA.
SAP Server Connection Type	<p>The SAP server connection type to use.</p> <p>Select from the following options:</p> <ul style="list-style-type: none"><li>- <b>Application Server Connection.</b> Connect to an SAP Application Server using the SAP user name and password.</li><li>- <b>Application Server SNC Connection.</b> Connect to an SAP Application Server using the secured network connection:<ul style="list-style-type: none"><li>- With X.509 Certificate. You do not need to specify the SAP user name and password explicitly. You must provide the path of the x.509 certificate file.</li><li>- Without X.509 Certificate. You must provide the SAP user name.</li></ul></li><li>- <b>Load Balancing Server Connection.</b> Connect to an SAP Application Server with the least load at run time.</li><li>- <b>Load Balancing Server SNC Connection.</b> Connect to an SAP Application Server using SNC with the least load at run time.</li></ul> <p><b>Note:</b> Before you use an SNC connection, you must verify that SNC is configured both on the SAP Server and the machine where the Secure Agent runs.</p>

The following table describes the properties that must configure when you select **Application Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SAP Username	The SAP user name with the appropriate user authorization.

Connection property	Description
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

The following table describes the properties that must configure when you select **Application Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SNC My Name	Optional. The Informatica client Personal Security Environment (PSE) or certificate name. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name. Default length is 256.
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> Default is 3 - <i>Apply privacy protection (integrity and authentication)</i> .
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	The path to the X509 certificate file. If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.crt</code> extension. You do not need to specify the SAP user name and password. If you do not want to use the X509 certificate, specify the SAP username for which SNC is configured in SAP Server.
Additional Parameters	Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties: <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> During the runtime, the JCo and CPIC traces file are generated in the following location: <code>&lt;Informatica Secure Agent installation directory&gt;\apps</code> <code>\Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</code> During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location: <code>&lt;Informatica Secure Agent installation directory&gt;\apps</code> <code>\Data_Integration_Server\&lt;DIS version&gt;tomcat.out</code>

The following table describes the properties that must configure when you select **Load Balancing Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SNC My Name	Optional. The Informatica client PSE or certificate name generated on the Secure Agent machine. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name generated on the SAP Server. Default length is 256.
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> Default is 3 - <i>Apply privacy protection (integrity and authentication)</i> .
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	The path to the X509 certificate file. If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.cert</code> extension. You do not need to specify the SAP user name and password. If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in the SAP Server.
Additional Parameters	Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties: <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> During the runtime, the JCo and CPIC traces file are generated in the following location: <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location: <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

# SAP BW BEx Query connection properties

To read data from SAP BEx queries, select the **SAP BW BEx Query** connection type and configure the connection properties.

The following table describes the SAP BW BEx Query connection properties:

Connection property	Description
Runtime Environment	Required. Runtime environment that contains the Secure Agent that you want to use to read data from SAP BEx queries.
Authentication	Required. Authentication method for the connection. Select <b>SAP</b> .
Username	Required. SAP user name with the appropriate user authorization.
Password	Required. SAP password.
Connection type	Required. Type of connection that you want to create. To read data from SAP BEx queries, you must select the <b>Application</b> connection type. Use the application connection type to connect to a specific SAP BW server. Default is Application.
Host name	Required. Host name or IP address of the SAP BW server that you want to connect to.
System number	Required. SAP system number.
Client	Required. SAP client number.
Language	Language code that corresponds to the language used in the SAP system.
SAP Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system as an RFC client.</p> <p>You can specify the required RFC-specific parameters and connection information to enable communication between Data Integration and SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments to connect to SAP:</p> <pre>GROUP=interfaces ASHOST=tzxscs20.bmwgroup.net SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=ZXS, OU=SAP system, O=BMW Group SNC_MYNAME=p:CN=CMDB_SWP-2596, OU=SNC partner system, O=BMW Group SNC_LIB=/global/informatica/104/server/bin/libsapcrypto.so X509CERT=/global/informatica/104/SAPSNCertfiles/ROOT_CA_V3.crt TRACE=2</pre> <p><b>Note:</b> If you have specified the mandatory connection parameters in the connection, those values override the additional parameter arguments.</p>

**Note:** You can ignore the other connection properties because they are not relevant for SAP BW BEx Query Connector.

# SAP BW Reader connection properties

To read data from SAP BW objects, select the **SAP BW Connector** connection type and configure the connection properties.

The following table describes the SAP BW connection properties:

Property	Description
Connection Name	Name of the connection.
Description	Description of the connection.
Type	Type of connection.
Runtime Environment	Required. Runtime environment that contains the Secure Agent that you want to use to read data from SAP BW objects.
Username	Required. SAP user name with the appropriate user authorization.
Password	Required. SAP password.
Connection type	Required. Type of connection that you want to create. Select one of the following values: <ul style="list-style-type: none"><li>- Application. Create an application connection when you want to connect to a specific SAP BW server.</li><li>- Load balancing. Create a load balancing connection when you want to use SAP load balancing. Default is Application.</li></ul>
Host name	Required when you create an SAP application connection. Host name or IP address of the SAP BW server that you want to connect to.
System number	Required when you create an SAP application connection. SAP system number.
Message host name	Required when you create an SAP load balancing connection. Host name of the SAP message server.
R3 name/SysID	Required when you create an SAP load balancing connection. SAP system name.
Group	Required when you create an SAP load balancing connection. Group name of the SAP application server.
Client	Required. SAP client number.
Language	Language code that corresponds to the language used in the SAP system.

Property	Description
Trace	<p>Use this option to track the JCo calls that the SAP system makes.</p> <p>Specify one of the following values:</p> <ul style="list-style-type: none"> <li>- 0. Off</li> <li>- 1. Full</li> </ul> <p>Default is 0.</p> <p>SAP stores information about the JCo calls in a trace file.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- <b>Design-time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- <b>Run-time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you want to use.</p> <p>Use the following format:</p> <p>&lt;parameter name1&gt;=&lt;value1&gt;, &lt;parameter name2&gt;=&lt;value2&gt;</p>
Port Range	<p>HTTP port range that the Secure Agent must use to read data from the SAP BW server in streaming mode.</p> <p>Enter the minimum and maximum port numbers with a hyphen as the separator. The minimum and maximum port number can range between 10000 and 65535.</p> <p>Default is 10000-65535.</p>
Use HTTPS	Select this option to enable https streaming.
Keystore location	Absolute path to the JKS keystore file.
Keystore password	Password for the .JKS file.

Property	Description
Private key password	Export password specified for the .P12 file.
SAP Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system as an RFC client.</p> <p>Specify the required RFC-specific parameters and connection information to enable communication between Data Integration and SAP.</p> <p>You can specify the Secure Network Communication (SNC) parameters as additional arguments to securely connect to SAP as shown in the following format:</p> <pre>MSHOST= &lt;Message server hostname&gt; GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about the SNC parameters that you can configure in this field, see the How-To Library article, <a href="#">How to Configure the SAP Secure Network Communication Protocol in Informatica Cloud Data Integration</a>.</p> <p><b>Note:</b> The values of any required connection parameters override SAP additional parameter values that you have entered.</p>

## SAP HANA CDC Connection Properties

When you configure a SAP HANA CDC connection, you must set the connection properties.

The following table describes SAP HANA CDC connection properties:

Property	Description
Connection Name	<p>A name for the SAP HANA CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name.</p> <p>Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	Description of the SAP HANA CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For SAP HANA CDC, the type must be <b>SAP HANA CDC</b> .

Property	Description
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for SAP HANA change data and the PowerExchange Logger for LUW run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p><i>host_name:port_number</i></p> <p>For example:</p> <p>HANADB1:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	SAP HANA instance name that is specified in the <b>Database</b> field of the registration group that contains capture registrations for the SAP HANA source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>

Property	Description
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	<p>Enter the host name or IP address of the system that contains the extraction maps. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p><i>host_name:port_number</i></p> <p>For example:</p> <p>SAPHANA2B:25100</p> <p>The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a SAP HANA table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) SAP HANA CDC connections in PowerCenter.</p>

# SAP HANA connection properties

When you set up an SAP HANA connection, configure the connection properties.

The following table describes the SAP HANA connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Select SAP HANA from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent or serverless runtime environment.
Host	SAP HANA server host name.
Port	SAP HANA server port number.
Database Name	Name of the SAP HANA database.
Current Schema	SAP HANA database schema name. Specify <b>_SYS_BIC</b> when you use SAP HANA database modelling views.
Code Page	The code page of the database server defined in the connection. Select the UTF-8 code page.
Metadata Advanced Connection Properties	The optional properties for the JDBC driver to fetch the metadata. If you specify more than one property, separate each key-value pair with a semicolon. For example, <code>connectTimeout=180000</code>
Run-time Advanced Connection Properties	The optional properties for the ODBC driver to run the mappings. If you specify more than one property, separate each key-value pair with a semicolon. For example, <code>charset=sjis;readtimeout=180</code>
Username	User name of the SAP HANA account.
Password	Password of the SAP HANA account. The password can contain alphanumeric characters and the following special characters: ~ ` ! @ # \$ % ^ & * ( ) _ - + = { [ ]   : ; ' < , > . ? / <b>Note:</b> You can't use a semicolon character in combination with a left brace or right brace character.

# SAP HANA Database Ingestion connection properties

When you set up an SAP HANA connection for a database ingestion task, you must configure connection properties.

The following table describes the SAP HANA connection properties:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is <b>SAP HANA Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run database ingestion tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the SAP HANA instance.
Password	The password to use for connecting to the SAP HANA instance.
Host	The name of the machine that hosts the SAP HANA database server.
Port	The port number for the SAP HANA server to which you want to connect. Default is 30015.
Database Name	The SAP HANA source database name.
Advanced Connection Properties	Advanced properties for the SAP HANA JDBC driver, which is used to connect to the SAP HANA source. If you specify more than one <i>property=value</i> entry, separate them with an ampersand (&). The JDBC connection properties that you can enter in this field are described in the SAP <a href="#">JDBC Connection Properties</a> documentation. For example: encrypt=true.
Log Clear	Required for incremental loads. The time interval, in days, after which the PKLOG table entries and shadow _CDC table entries are purged. The purging occurs only while an incremental load job is running.  Valid values for a database ingestion job are 0 to 366. Any positive value in this range cause automatic housekeeping to run while the incremental job is running. Default is 14.  A value of 0 means that the table entries are not purged. For manual housekeeping, enter 0 and use your in-house process.  Any value outside the range of 0 to 366, including a negative number or non-numeric value, causes database ingestion jobs that use the connection to fail with the following error:  <code>LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.</code>
Trigger Prefix	Adds a prefix to the names of the AFTER DELETE, AFTER INSERT, and AFTER UPDATE triggers that the CDC script generates for each source table to get before images and after images of the DML changes. Enter any prefix value up to 16 characters in length. An underscore (_) follows the prefix in the trigger name, for example, <b>TX_SAP_DEMO_TABLE_DBMI_USER_t_d</b> . You can use the prefix to comply with your site's trigger naming conventions.

**Note:** If you test the connection and the test fails, check that the SAP HANA JDBC driver file, `ngdbc.jar`, has been installed at `Secure Agent installation directory>/ext/connectors/thirdparty/informatica.hanami`.

## SAP IDoc Reader connection properties

To read SAP data through the IDoc interface, select the **iDoc Reader** connection type and configure the connection properties.

The following table describes the SAP IDoc Reader connection properties:

Connection property	Description
Destination Entry	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the RFC server program registered at an SAP gateway. The Program ID for this destination entry must be the same as the Program ID for the logical system you defined in SAP to receive IDocs.
Code Page	Required. The code page compatible with the SAP source. Select one of the following code pages: <ul style="list-style-type: none"><li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li><li>- UTF-8. Select for Unicode data.</li><li>- Shift-JIS. Select for double-byte character data.</li><li>- ISO 8859-15 Latin 9 (Western European).</li><li>- ISO 8859-2 Eastern European.</li><li>- ISO 8859-3 Southeast European.</li><li>- ISO 8859-5 Cyrillic.</li><li>- ISO 8859-9 Latin 5 (Turkish).</li><li>- IBM EBCDIC International Latin-1.</li></ul>

## SAP IDoc Writer connection properties

To write SAP data through the IDoc interface, select the **iDoc Writer** connection type and configure the connection properties.

The following table describes the SAP IDoc Writer connection properties:

Connection property	Description
User Name	Required. SAP user name with authorization on S_DATASET, S_TABU_DIS, S_PROGRAM, and B_BTCH_JOB objects.
Password	Required. SAP password.
Connection String	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.

Connection property	Description
Code Page	Required. The code page compatible with the SAP target. Select one of the following code pages: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>
Language Code	Required. Language code that corresponds to the SAP language.
Client code	Required. SAP client number.

## SAP IQ connection properties

When you set up an SAP IQ connection, you must configure the connection properties.

The following table describes the SAP IQ properties:

Connection property	Description
Connection Name	The name of the connection.
Description	Optional. Description of the SAP IQ connection that you use to identify the connection.
Type	Type of connection. Select SAP IQ as the connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select the Secure Agent from the list as the runtime environment.
Host Name	Name of the machine that hosts the SAP IQ database server.
Port	Network port number used to connect to the SAP IQ database server. Default is 2638.
Database	The SAP IQ database that you want to connect to.
Schema	Schema name in the SAP IQ server to fetch the metadata.
User Name	User name for the SAP IQ database login.
Password	Password for the SAP IQ database login.

Connection property	Description
Checkpoint	If enabled, the SAP IQ database issues a checkpoint after successfully loading the table. If disabled, the database does not issue a checkpoint. Default is enabled.
Notify Interval	Number of rows the SAP IQ external loader loads before it writes a status message to the external loader log. Default is 1000.
Datafile Directory	The SAP IQ directory that stores the data files at runtime. The directory must be accessible from the Secure Agent machine. If the directory is on the Windows system, use a backslash (\) in the path: For example, D:\mydirectory\inputfile.out If the directory is on the UNIX system, use a forward slash (/) in the path: For example, /mydirectory/inputfile.out
External Loader Executable	File name and file path for the external loader executable. When you create an SAP IQ external loader connection, the name of the external loader executable file is set to <b>dbisql</b> by default. If you use an executable file with a different name, you must update the <b>External Loader Executable</b> field. If the external loader executable file directory is not in the system path, you must enter the file path and file name in this field. If you configure the connection on Windows, you must enter <b>dbisql -nogui</b> .
Is Staged	Method of loading data. Select <b>Is Staged</b> to load data to a flat file staging area before loading to the database. Default is enabled.

## SAP Mass Ingestion connection properties

When you set up a SAP Mass Ingestion connection, you must configure the connection properties.

The following table describes the connection properties for a SAP Mass Ingestion connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the SAP instance.

Connection property	Description
Password	Password for the SAP instance.
Language Code	Language code that corresponds to the SAP language.
System Number	System number of the SAP server.
Client Number	Client number of the SAP server.
Port Range	HTTP port range to run the Netty server.
Connection Type	Type of connection to access the ABAP application server. Options are: - <b>Direct Connection</b> : Accesses a single ABAP application server using the server host. - <b>Load Balancing Connection</b> : Accesses a group of ABAP application servers through the message server.
Application Server	Name of the SAP application server host. <b>Note:</b> This field appears only for the <b>Direct Connection</b> type.
Message Server	IP address or name of the SAP message server. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
SAP Logon Group	Name of the group of servers that belong to the SAP system you want to access. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
SAP System ID	ID of the SAP system that you want to access. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
Message Server Port	Port number on which the SAP message server is listening. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
Database	The name of the underlying database.
Database user name	User name of the database instance.
Database password	Password for the database instance.
Host	Host name of the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Code Page	The code page of the database server. Application ingestion tasks use the UTF-8 code page. Default is UTF-8.

Connection property	Description
Encryption Method	<p>For initial load jobs, determines whether the data exchanged between the Secure Agent and the Oracle database server is encrypted:</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>SSL</b>. Establishes a secure connection using SSL for data encryption. If the Oracle database server cannot configure SSL, the connection fails.</li> <li>- <b>No Encryption</b>. Establishes a connection without using SSL. Data is not encrypted.</li> </ul> <p>Default is <b>No Encryption</b>.</p>
Crypto Protocol Version	<p>If you selected SSL as the encryption method, you must specify a cryptographic protocol or a list of cryptographic protocols supported by your server to use with an encrypted connection.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>SSLv2</b></li> <li>- <b>SSLv3</b></li> <li>- <b>TLSv1.2</b></li> </ul> <p>Default is <b>TLSv1.2</b>.</p>
Validate Server Certificate	<p>If you selected SSL as the encryption method, this option controls whether the Secure Agent validates the server certificate that is sent by the Oracle database server.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>True</b>. Validate the server certificate.</li> <li>- <b>False</b>. Do not validate the server certificate.</li> </ul> <p>Default is <b>False</b>.</p> <p>If you also specify the <b>Host Name in Certificate</b> property, the Secure Agent also validates the host name in the certificate.</p>
Trust Store	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the client trusts for SSL authentication.</p>
Trust Store Password	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify a password for accessing the contents of the truststore file.</p>
Host Name in Certificate	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the host name of the machine that hosts the Oracle database to provide for additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
Key Store	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the path and name of the keystore file. The keystore file contains the certificates that the client sends to the Oracle server in response to the server's certificate request.</p>
Key Store Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keystore file.</p>
Key Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keys in the keystore file. Use this property when the keys have a different password than the keystore file.</p>

Connection property	Description
Database Connect String	An Oracle connection string, defined in TNS, that application ingestion tasks use to connect to the Oracle database.
TDE Wallet Directory	<p>The path to the directory that contains the Oracle wallet file used for Oracle Transparent Data Encryption (TDE). Specify this property value only if you capture change data from TDE-encrypted table spaces and one of the following conditions are true:</p> <ul style="list-style-type: none"> <li>- The Oracle wallet is not available to the database.</li> <li>- The Oracle database is running on a server that is remote from Oracle redo logs.</li> <li>- The wallet directory is not in the default location on the database host or the wallet name is not the default name of ewallet.p12.</li> <li>- The wallet directory is not available to the Secure Agent host.</li> </ul>
TDE Wallet Password	A clear text password that is required to access the Oracle TDE wallet and get the master key. This property value is required if you need to read and decrypt data from TDE-encrypted tablespaces in the Oracle source database.
Directory Substitution	<p>A local path prefix to substitute for the server path prefix of the redo logs on the Oracle server. This substitute local path is required when the log reader runs on a system other than the Oracle server and uses a different mapping to access the redo log files.</p> <p>Use this property in the following situations:</p> <ul style="list-style-type: none"> <li>- The redo logs reside on shared disk.</li> <li>- The redo logs have been copied to a system other than the Oracle system.</li> <li>- The archived redo logs are accessed by using a different NFS mount.</li> </ul> <p><b>Note:</b> Do not use this property if you use Oracle Automatic Storage Management (ASM) to manage the redo logs.</p> <p>You can define one or more substitutions. Use the following format:</p> <pre>server_path_prefix,local_path_prefix;server_path_prefix,local_path_prefix;...</pre>
Reader Active Log Mask	<p>A mask that the log reader uses for selecting active redo logs when the Oracle database uses multiplexing of redo logs. The log reader compares the mask against the member names in an active redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Reader Archive Destination 1	<p>The primary log destination from which the log reader reads archived logs, when Oracle is configured to write more than one copy of each archived redo log. Enter a number that corresponds to an <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10.</p> <p>If you set only one of the Reader Archive Destination 1 and Destination 2 properties, the log reader uses that property setting. If you specify neither property, the archive log queries are not filtered by the log destination.</p>
Reader Archive Destination 2	<p>The secondary log destination from which the log reader reads archived logs when the primary destination becomes unavailable or when the logs at the primary destination cannot be read. For example, logs might have been corrupted or deleted. Enter a number that corresponds to the <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10. Usually, this value is a number greater than 1.</p>

Connection property	Description
Reader ASM Connect String	In an Oracle ASM environment, the Oracle connection string, defined in TNS, that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database.
Reader ASM User Name	In an Oracle ASM environment, an Oracle user ID that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database. This user ID must have SYSDBA or SYSASM authority. To use SYSASM authority, set the <b>Reader ASM Connect As SYSASM</b> property to Y.
Reader ASM Password	In an Oracle ASM environment, a clear text password for the user that is specified in the <b>Reader ASM User Name</b> property. The log reader uses this password and the ASM user name to connect to the ASM instance that manages storage of active and archived redo logs for the source database.
Reader ASM Connect As SYSASM	If you use Oracle 11g ASM or later and want the log reader to use a user ID that has SYSASM authority to connect to the ASM instance, select this check box. Also specify a user ID that has SYSASM authority in the <b>Reader ASM User Name</b> property. To use a user ID that has SYSDBA authority, clear this check box. By default, this check box is cleared.
Reader Mode	<p>Indicates the source of and types of Oracle redo logs that the log reader reads. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>ACTIVE</b>. Read active and archived redo logs from the Oracle online system. Optionally, you can use the <b>Reader Active Log Mask</b> property to filter the active redo logs and use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVEONLY</b>. Read only archived redo logs. Optionally, you can use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVECOPY</b>. Read archived redo logs that have been copied to an alternate file system. Use this option in the following situations: <ul style="list-style-type: none"> <li>- You do not have the authority to access the Oracle archived redo logs directly.</li> <li>- The archived redo logs are written to ASM, but you do not have access to ASM.</li> <li>- The archived log retention policy for the database server causes the archived logs to not be retained long enough.</li> </ul> <p>With this option, the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties are ignored.</p> <p>Default is <b>ACTIVE</b>.</p> </li> </ul>
Reader Standby Log Mask	<p>A mask that the log reader uses for selecting redo logs for an Oracle physical standby database when the database uses multiplexing of redo logs. The log reader compares the mask against the member names in a redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Standby Connect String	An Oracle connection string, defined in TNS, that the log reader uses to connect to the Oracle physical standby database for change capture when the database is not open with read only access.

Connection property	Description
Standby User Name	A user ID that the log reader uses to connect to the Oracle physical standby database for change capture. This user ID must have SYSDBA authority.
Standby Password	A password that the log reader uses to connect to the Oracle physical standby database for change capture.
RAC Members	<p>The maximum number of active redo log threads, or <i>members</i>, in an Oracle Real Application Cluster (RAC) that can be tracked. For a Data Guard physical standby database that supports a primary database in a RAC environment, this value is the number of active threads for the primary database.</p> <p>Valid values are 1 to 100. Default is 0, which causes an appropriate number of log threads to be determined automatically. If this value is not appropriate for your environment, set this property to a value greater than 0.</p>
BFILE Access	<p>Select this check box in the following circumstances:</p> <ul style="list-style-type: none"> <li>- You use BFILE access to redo logs in physical directories on the local Oracle server file system. BFILE access uses Oracle directory objects to remotely access the redo logs in the file system. This method is an alternative to other log access methods such as ASM or NFS mounts.</li> <li>- You have an Amazon Relational Database Service (RDS) for Oracle source. In this case, this option enables access to the redo logs of a cloud-based database instance deployed in RDS.</li> </ul> <p>By default, this check box is cleared.</p>

## SAP RFC/BAPI interface connection properties

To access SAP data through the RFC/BAPI interface, select the **SAP RFC/BAPI Interface** connection type and configure the connection properties.

The following table describes the SAP RFC/BAPI Interface connection properties:

Connection property	Description
User Name	Required. SAP user name with authorization on S_DATASET, S_TABU_DIS, S_PROGRAM, and B_BTCH_JOB objects.
Password	Required. SAP password.
Connection String	Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.

Connection property	Description
Code Page	The code page compatible with the SAP target. Select one of the following code pages: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>
Language Code	Required. Language code that corresponds to the SAP language.
Client Code	Required. SAP client number.

## SAP Table connection properties

To process SAP table data, select the **SAP Table Connector** connection type and configure the connection properties.

The following table describes the SAP Table connection properties:

Property	Description
Connection Name	Name of the connection.
Description	Description of the connection.
Type	Type of connection.
Runtime Environment	Required. The name of the runtime environment where you want to run the tasks. Select a Secure Agent or serverless runtime environment.
Username	Required. SAP user name with the appropriate user authorization.
Password	Required. SAP password.
Client	Required. SAP client number.
Language	Language code that corresponds to the SAP language.
Saprfc.ini Path	Required. Local directory to the <code>sapnwrfc.ini</code> file. To write to SAP tables, use the following directory: <Informatica Secure Agent installation directory>/apps/ Data_Integration_Server/ext/deploy_to_main/bin/rdtm

Property	Description
Destination	<p>Required. DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.</p> <p>Destination is case sensitive.</p> <p><b>Note:</b> Use all uppercase letters for the destination.</p>
Port Range	<p>HTTP port range. The SAP Table connection uses the specified port numbers to connect to SAP tables using the HTTP protocol. Ensure that you specify valid numbers to prevent connection errors. Default: 10000-65535.</p> <p>Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>
Test Streaming	<p>Tests the connection. When selected, tests the connection using both RFC and HTTP protocol. When not selected, tests connection using RFC protocol.</p>
Https Connection	<p>When selected, connects to SAP through HTTPS protocol. To successfully connect to SAP through HTTPS, verify that an administrator has configured the machines that host the Secure Agent and the SAP system.</p>
Keystore Location	<p>The absolute path to the JKS keystore file.</p>
Keystore Password	<p>The destination password specified for the .JKS file.</p>
Private Key Password	<p>The export password specified for the .P12 file.</p>

# SAP ODP Extractor connection properties

When you set up an **SAP ODP Extractor** connection, configure the connection properties.

The following table describes the SAP ODP Extractor connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks to access SAP S/4HANA or SAP ECC. Select a Secure Agent or serverless runtime environment.
SAP Server Connection Type	The SAP server connection type to use. Select from the following options: <ul style="list-style-type: none"><li>- <b>Application Server Connection.</b> Connect to an SAP Application Server using the SAP user name and password.</li><li>- <b>Application Server SNC Connection.</b> Connect to an SAP Application Server using the secured network connection:<ul style="list-style-type: none"><li>- With X.509 Certificate. You do not need to specify the SAP user name and password explicitly. You must provide the path of the x.509 certificate file.</li><li>- Without X.509 Certificate. You must provide the SAP user name.</li></ul></li><li>- <b>Load Balancing Server Connection.</b> Connect to an SAP Application Server with the least load at run time.</li><li>- <b>Load Balancing Server SNC Connection.</b> Connect to an SAP Application Server using SNC with the least load at run time.</li></ul> <b>Note:</b> Before you use an SNC connection, you must verify that SNC is configured both on the SAP Server and the machine where the Secure Agent runs.

The following table describes the properties that must configure when you select **Application Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Subscriber Name	A name which defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) in case of delta read from ODP.

Connection property	Description
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>
Display Delta Fields	<p>Specifies whether the mapping displays the operation modes that caused the changed data on ODP sources.</p> <p>When enabled, the mapping generates the ODQ_CHANGEMODE and ODQ_ENTITYCNTR fields on the <b>Fields</b> tab for ODP sources that are enabled with Operational Delta Queue (ODQ). Default is disabled.</p>

The following table describes the properties that must configure when you select **Load Balancing Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	Host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Subscriber Name	<p>A name which defines the Secure Agent as a unique subscriber in the SAP system.</p> <p>SAP uses this name to define unique operational delta queue (ODQ) in case of delta read from ODP.</p>

Connection property	Description
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location: &lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</p> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location: &lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</p>
Display Delta Fields	<p>Specifies whether the mapping displays the operation modes that caused the changed data on ODP sources.</p> <p>When enabled, the mapping generates the ODQ_CHANGEMODE and ODQ_ENTITYCNTR fields on the <b>Fields</b> tab for ODP sources that are enabled with Operational Delta Queue (ODQ). Default is disabled.</p>

The following table describes the properties that must configure when you select **Application Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SNC My Name	Optional. The Informatica client Personal Security Environment (PSE) or certificate name. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name. Default length is 256.
SNC Quality of Protection (QoP)	<p>Specifies the SAP PSE or certificate name. You can select from the following options:</p> <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> <p>Default is 3 - <i>Apply privacy protection (integrity and authentication)</i>.</p>
SAP Cryptographic Library Path	<p>The path to the cryptographic library. Specify sapcrypto.dll for Windows or libsapcrypto.so for Linux.</p>

Connection property	Description
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	<p>The path to the X509 certificate file.</p> <p>If you select to use the X509 certificate, specify the path to the X509 certificate file with .crt extension. You do not need to specify the SAP user name and password.</p> <p>If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in SAP Server.</p>
Subscriber Name	<p>A name which defines the Informatica Secure Agent as a unique subscriber in the SAP system.</p> <p>SAP uses this name to define unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.</p>
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system.</p> <p>For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>
Display Delta Fields	<p>Specifies whether the mapping displays the operation modes that caused the changed data on ODP sources.</p> <p>When enabled, the mapping generates the ODQ_CHANGEMODE and ODQ_ENTITYCNTR fields on the <b>Fields</b> tab for ODP sources that are enabled with Operational Delta Queue (ODQ).</p> <p>Default is disabled.</p>

The following table describes the properties that must configure when you select **Load Balancing Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	Host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SNC My Name	<p>Optional. The Informatica client PSE or certificate name generated on the Secure Agent machine.</p> <p>Default length is 256.</p>

Connection property	Description
SNC Partner Name	The Informatica client PSE or certificate name generated on the SAP Server. Default length is 256.
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> Default is 3 - <i>Apply privacy protection (integrity and authentication)</i> .
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	The path to the X509 certificate file. If you select to use the X509 certificate, specify the path to the X509 certificate file with <code>.crt</code> extension. You do not need to specify the SAP user name and password. If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in SAP Server.
Subscriber Name	A name which defines the Informatica Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.
Additional Parameters	Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties: <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> During the runtime, the JCo and CPIC traces file are generated in the following location: <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> During the design time, the CPIC traces are generated in the <code>tomcat.out</code> files at the following location: <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>
Display Delta Fields	Specifies whether the mapping displays the operation modes that caused the changed data on ODP sources. When enabled, the mapping generates the <code>ODQ_CHANGEMODE</code> and <code>ODQ_ENTITYCNTR</code> fields on the <b>Fields</b> tab for ODP sources that are enabled with Operational Delta Queue (ODQ). Default is disabled.

# SAS connection properties

When you create a SAS connection, you must configure the connection properties.

The following table describes the SAS connection properties:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={[]}\ ;:''<,>.?/
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>SAS</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent runtime environment.
Host	Host name of the machine that runs the SPI Server.
Port	Port number of the machine that runs the SPI Server.
User Name	User name specified in the SPI Server configuration.
Password	Password for the user.

# Satmetrix connection properties

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

The following table describes the Satmetrix connection properties:

Connection property	Description
Connection Name	Name of the Satmetrix connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Satmetrix connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Satmetrix URL	The URL with which the Secure Agent connects to the Satmetrix APIs. The URL has the following format: <i>http://&lt;company name&gt;.satmetrix.com</i>
Username	Username of the Satmetrix integration user account.
Password	Password of the Satmetrix integration user account.

## ServiceNow connection properties

When you set up a ServiceNow connection, configure the connection properties.

The following table describes the ServiceNow connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The ServiceNow connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	User name of the ServiceNow instance.
Password	Password for the ServiceNow instance.
EndPoint URL	The ServiceNow endpoint URL.
Instance Type	Type of ServiceNow instance. Select JSONv2.

## Sequential File connection properties

When you configure a Sequential File connection, you must set the connection properties.

The following table describes the Sequential File connection properties:

Property	Description
Connection Name	A name for the sequential file connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the sequential file connection. Maximum length is 4000 characters.
Type	Type of connection. For sequential files, the type must be <b>Sequential File</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.

Property	Description
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes requests for sequential file runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example: LSNR1:1467</p>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No</b>. Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For VSAM data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.

Property	Description
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) sequential file connections in PowerCenter.
Write Properties	Write Mode. Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

## ServiceNow Mass Ingestion connection properties

When you set up a ServiceNow Mass Ingestion connection, you must configure the connection properties.

The properties of a ServiceNow Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0:** Authenticates the connection by using the details of the OAuth API endpoint that is created for the connection in ServiceNow. To use this method, you must create OAuth API endpoint in ServiceNow and then specify the client ID and client secret of the API endpoint in the connection properties. For more information about creating an OAuth API endpoint in ServiceNow, see the [ServiceNow documentation](#).
- **Basic:** Authenticates the connection by validating the login credentials of the ServiceNow account.

### Connection properties for OAuth 2.0 authentication

The following table describes the connection properties for a ServiceNow Mass Ingestion connection configured with OAuth 2.0 authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the ServiceNow account.
Password	Password for the ServiceNow account.
Client Secret	Client secret of the API endpoint created for the connection in ServiceNow.
Client ID	Client ID of the API endpoint created for the connection in ServiceNow.

Connection property	Description
Base URI	URL of the ServiceNow instance. You must enter the base URI in the following format: <code>https://{your_servicenow_instance}.service-now.com/</code>
OAuth Token URL	OAuth token endpoint of the ServiceNow instance. The API client associated with the connection sends the access token requests to this endpoint.

### Connection properties for Basic authentication

The following table describes the connection properties for a ServiceNow Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the ServiceNow account.
Password	Password for the ServiceNow account.
Base URI	URL of the ServiceNow instance. You must enter the base URI in the following format: <code>https://{your_servicenow_instance}.service-now.com/</code>

## Snowflake Data Cloud connection properties

When you set up a Snowflake Data Cloud connection, configure the connection properties.

You can use the following authentication methods to connect to Snowflake:

- **Standard.** Uses Snowflake account user name and password credentials to connect to Snowflake.  
**Note:** For application ingestion tasks, you can use only the Standard authentication method.
- **Authorization Code.** Uses the OAuth 2.0 protocol with Authorization Code grant type to connect to Snowflake. Authorization Code allows authorized access to Snowflake without sharing or storing your login credentials.
- **KeyPair.** Uses the private key file and private key file password, along with the existing Snowflake account user name to connect to Snowflake.
- **Client Credentials.** Uses the OAuth 2.0 protocol with the Client Credentials grant type to connect to Snowflake.

You create a Snowflake Data Cloud connection on the Connections page. You can then use the connection when you read from or write data to Snowflake.

## Standard authentication

When you set up a Snowflake Data Cloud connection, configure the connection properties.

The following table describes the Snowflake Data Cloud connection properties for the Standard authentication mode:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Snowflake Data Cloud connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode. You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.
Authentication	The authentication method that the connector must use to log in to Snowflake. Select <b>Standard</b> . Default is <b>Standard</b> .
Username	The user name to connect to the Snowflake account.
Password	The password to connect to the Snowflake account.
Account	The name of the Snowflake account. For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#</code> , your account name is the first segment in the URL before <code>snowflakecomputing.com</code> . Here, <code>123abc.us-east-2.aws</code> is your account name. If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard</code> , your account name is <code>123abc.us-east-2.aws</code> <b>Note:</b> Ensure that the account name doesn't contain underscores. To use an alias name, contact Snowflake Customer Support.
Warehouse	The Snowflake warehouse name.
Role	The Snowflake role assigned to the user.
Additional JDBC URL Parameters	The additional JDBC connection parameters. Enter one or more JDBC connection parameters in the following format: <code>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</code> For example, pass the database and schema values when you connect to Snowflake: <code>db=mydb&amp;schema=public</code> <b>Important:</b> Ensure that there is no space before and after the equal sign (=) when you add the parameters.

## OAuth 2.0 authorization code authentication

The following table describes the Snowflake Data Cloud connection properties for an OAuth 2.0 - AuthorizationCode type connection:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Snowflake Data Cloud connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode. You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.
Authentication	The authentication method that Snowflake Data Cloud Connector must use to log in to Snowflake. Select <b>AuthorizationCode</b> .
Account	The name of the Snowflake account. For example, if the Snowflake URL is https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#, your account name is the first segment in the URL before snowflakecomputing.com. Here, 123abc.us-east-2.aws is your account name. If you use the Snowsight URL, for example, https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard, your account name is 123abc.us-east-2.aws <b>Note:</b> Ensure that the account name doesn't contain underscores. To use an alias name, contact Snowflake Customer Support.
Warehouse	The Snowflake warehouse name.
Additional JDBC URL Parameters	The additional JDBC connection parameters. Enter one or more JDBC connection parameters in the following format: <code>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</code> For example, pass the database and schema values when you connect to Snowflake: <code>db=mydb&amp;schema=public</code> <b>Important:</b> Ensure that there is no space before and after the equal sign (=) when you add the parameters.
Authorization URL	The Snowflake server endpoint that is used to authorize the user request. The authorization URL is https://<account name>.snowflakecomputing.com/oauth/authorize, where <account name> specifies the full name of your account provided by Snowflake. For example, https://<abc>.snowflakecomputing.com/oauth/authorize <b>Note:</b> If the account name contains underscores, use the alias name. You can also use the Authorization Code grant type that supports the authorization server in a Virtual Private Cloud network.

Property	Description
Access Token URL	<p>The Snowflake access token endpoint that is used to exchange the authorization code for an access token.</p> <p>The access token URL is <code>https://&lt;account name&gt;.snowflakecomputing.com/oauth/token-request</code>, where <code>&lt;account name&gt;</code> specifies the full name of your account provided by Snowflake.</p> <p>For example, <code>https://&lt;abc&gt;.snowflakecomputing.com/oauth/token-request</code></p> <p><b>Note:</b> If the account name contains underscores, use the alias name.</p>
Client ID	<p>Client ID of your application generated when you create a security integration of type OAuth in Snowflake.</p> <p>For more information, see the Snowflake documentation.</p>
Client Secret	Client secret generated for the client ID.
Scope	<p>Determines the access control if the API endpoint has defined custom scopes.</p> <p>Enter space-separated scope attributes.</p> <p>For example, specify <code>session:role:CQA_GCP</code> as the scope to override the value of the default user role. The value must be one of the roles assigned in Security Integration.</p>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the parameters in the JSON format.</p> <p>For example, define the following parameters:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre>
Authorization Code Parameters	<p>Additional parameters to use with the authorization token URL.</p> <p>Define the parameters in the JSON format.</p> <p>For example, define the following parameters:</p> <pre>[{"Name": "code_challenge", "Value": "Ikr-vv52th0UeVRi4"}, {"Name": "code_challenge_method", "Value": "S256"}]</pre>
Access Token	<p>The access token value.</p> <p>Enter the populated access token value, or click <b>Generate Token</b> to populate the access token value.</p>
Generate Token	Generates the access token and refresh token based on the OAuth attributes you specified.
Refresh Token	<p>The refresh token value.</p> <p>Enter the populated refresh token value, or click <b>Generate Token</b> to populate the refresh token value. If the access token is not valid or expires, the agent fetches a new access token with the help of the refresh token.</p> <p><b>Note:</b> If the refresh token expires, provide a valid refresh token or regenerate a new refresh token by clicking <b>Generate Token</b>.</p>

## Key pair authentication

The following table describes the Snowflake Data Cloud connection properties for the KeyPair authentication type connection:

Connection 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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Snowflake Data Cloud connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode. You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.
Authentication	The authentication method to log in to Snowflake. Select <b>KeyPair</b> .
Username	The user name to connect to the Snowflake account.
Account	The name of the Snowflake account. For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code> . Here, <code>123abc.us-east-2.aws</code> is your account name. If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code> . <b>Note:</b> Ensure that the account name doesn't contain underscores. To use an alias name, contact Snowflake Customer Support.
Warehouse	The Snowflake warehouse name.
Additional JDBC URL Parameters	The additional JDBC connection parameters. Enter one or more JDBC connection parameters in the following format: <code>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</code> For example, pass the database and schema values when you connect to Snowflake: <code>db=mydb&amp;schema=public</code> <b>Important:</b> Ensure that there is no space before and after the equal sign (=) when you add the parameters.

Connection property	Description
Private Key File	<p>Path to the private key file, including the private key file name, that the Secure Agent uses to access Snowflake.</p> <p>For example, specify the following path and key file name:</p> <ul style="list-style-type: none"> <li>- On Windows: C:\Users\path_to_key_file\rsa_key.p8</li> <li>- On Linux: /export/home/user/path_to_key_file/rsa_key.p8</li> </ul> <p><b>Note:</b> Verify that the keystore is FIPS-certified.</p>
Private Key Password	Password for the private key file.

## OAuth 2.0 client credentials authentication

The following table describes the Snowflake Data Cloud connection properties for an OAuth 2.0 - ClientCredentials type connection:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -,</p> <p>Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Snowflake Data Cloud connection type.
Runtime Environment	<p>The name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p>
Authentication	<p>The authentication method that Snowflake Data Cloud Connector must use to log in to Snowflake.</p> <p>Select <b>ClientCredentials</b>.</p>
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#, your account name is the first segment in the URL before snowflakecomputing.com. Here, 123abc.us-east-2.aws is your account name.</p> <p>If you use the Snowsight URL, for example, https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard, your account name is 123abc.us-east-2.aws</p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.

Property	Description
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>Enter one or more JDBC connection parameters in the following format:</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</pre> <p>For example, pass the database and schema values when you connect to Snowflake:</p> <pre>db=mydb&amp;schema=public</pre> <p><b>Important:</b> Ensure that there is no space before and after the equal sign (=) when you add the parameters.</p>
Access Token URL	<p>The Snowflake access token endpoint that is used to exchange the authorization code for an access token.</p> <p>Specify the access token URL that you get from the OAuth endpoint.</p>
Client ID	<p>Client ID of your application generated when you configure an application that is compatible with OAuth.</p> <p>For more information, see the Snowflake documentation.</p>
Client Secret	Client secret generated for the client ID.
Scope	<p>Determines the access control if the API endpoint has defined custom scopes.</p> <p>Enter space-separated scope attributes.</p> <p>For example, specify <code>session:role:CQA_GCP</code> as the scope to override the value of the default user role. The value must be one of the roles assigned in Security Integration.</p>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the parameters in the JSON format.</p> <p>For example, define the following parameters:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre>
Access Token	<p>The access token value.</p> <p>Enter the populated access token value, or click <b>Generate Access Token</b> to populate the access token value.</p>
Generate Access Token	Generates the access token and refresh token based on the OAuth attributes you specified.

# SuccessFactors LMS connection properties

When you set up a SuccessFactors LMS connection, configure the connection properties.

The following table describes the SuccessFactors LMS connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The SuccessFactors LMS connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Service URL	OData service root URL that exposes the data that you want to read. Enter the URL in the following format: <code>https://&lt;rooturl&gt;/learning/odatav4/&lt;webservicename&gt;/v1/</code> For example, if the root URL is <code>partner0370.scdemo.successfactors.com:443</code> and the Web Service name is <code>curriculum</code> , enter the URL as follows: <code>https://partner0370.scdemo.successfactors.com:443/learning/odatav4/curriculum/v1/</code> For information about the Web Service names, see the <i>SuccessFactors Learning Web Services OData API Reference Guide</i> .
Client ID	The unique ID of the Web Service client that authenticates against the SAP SuccessFactors Learning server.
Client Secret	The secret code that an administrator generates to get OAuth tokens from the SAP SuccessFactors Learning server. The Web Service client then uses the client secret to request for OAuth tokens.
User ID	The unique ID of the user that authenticates against the SAP SuccessFactors Learning server.
Company ID	The tenant ID of the company that authenticates against the SAP SuccessFactors Learning server. The tenant ID is available in the page from where you generate the client ID and client secret.
User Type	The type of user account that runs the Web Service. Select one of the following values: - admin. Select <b>admin</b> if you run the Web Service with an administrator user account. - user. Select <b>user</b> if you run the Web Service with an end-user account.

# SuccessFactors ODATA connection properties

When you set up a SuccessFactors ODATA connection, configure the connection properties.

The following table describes the SuccessFactors ODATA connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The SuccessFactors ODATA connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent or Hosted Agent.
User name	The user name to access the SuccessFactors ODATA account. For example, enter username@companyID.
Password	The password to access the SuccessFactors ODATA account. <b>Important:</b> Even if you use OAuth 2.0 authentication, you must still enter the user name and password of the SuccessFactors ODATA account.
URL	SuccessFactors service root URL. For example, enter <a href="https://apisalesdemo8.successfactors.com/odata/v2">https://apisalesdemo8.successfactors.com/odata/v2</a> .
Security Type	Security protocol that you can use to establish a secure connection with the SuccessFactors server. Select SSL or TLS.
TrustStore File Name	Applies to security type. Name of the truststore file that contains the public certificate for the SuccessFactors server.
TrustStore Password	Applies to security type. Password for the truststore file that contains the public certificate for the SuccessFactors server.
KeyStore File Name	Applies to security type. Name of the keystore file that contains the private key for the SuccessFactors server.
KeyStore Password	Applies to security type. Password for the keystore file that contains the private key for the SuccessFactors server.
Authentication Type	Method to authenticate the user. Select one of the following authentication types: <ul style="list-style-type: none"><li>- HTTP Basic Authentication. Requires administrator access to the OData API and credentials for a valid account.</li><li>- OAuth 2.0. Requires a valid token and a registered OAuth 2.0 client application.</li></ul>
API KEY	Enter the API key that the OAuth Utility returns when you register your OAuth 2.0 client application. For more information about API key, see SuccessFactors documentation.

Property	Description
PRIVATE KEY	Enter the private key that the OAuth Utility returns when you generate the X.509 certificate. For more information about private key, see SuccessFactors documentation.
COMPANY ID	If you select OAuth 2.0 authentication, enter your company ID that SuccessFactors returns when you create an account in SuccessFactors.

## SuccessFactors SOAP connection properties

When you set up a SuccessFactors SOAP connection, you must configure the connection properties.

The following table describes the SuccessFactors SOAP connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select SuccessFactors SOAP from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
URL	SuccessFactors service root URL. For example, enter <a href="https://apisalesdemo8.successfactors.com/sfapi/v1/soap?wsdl">https://apisalesdemo8.successfactors.com/sfapi/v1/soap?wsdl</a> .
Company ID	Enter your company ID.
User name	Enter the username.
Password	Enter the password.

# Tableau V3 connection properties

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

The following table describes the Tableau V3 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Tableau Product	<p>The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the <code>.hyper</code> file:</p> <p><b>Tableau Desktop</b></p> <p>Creates a <code>.hyper</code> or TWBX files in the Secure Agent machine. You can then manually import the <code>.hyper</code> or TWBX files to Tableau Desktop and use the files to perform append or overwrite operation.</p> <p><b>Tableau Server</b></p> <p>Publishes the generated <code>.hyper</code> file to Tableau Server.</p> <p><b>Tableau Online</b></p> <p>Publishes the generated <code>.hyper</code> file to Tableau Online.</p>
Connection URL	<p>The URL of Tableau Server or Tableau Online to which you want to publish the <code>.hyper</code> file. The URL has the following format: <code>http://&lt;Host name of Tableau Server or Tableau Online&gt;:&lt;port&gt;</code></p> <p><b>Note:</b> This property is applicable when you select the value of the <b>Tableau product</b> as Tableau Server or Tableau Online.</p>
User Name	<p>User name of the Tableau Server or Tableau Online account.</p> <p><b>Note:</b> This property is applicable when you select the value of the <b>Tableau product</b> as Tableau Server or Tableau Online.</p>
Password	<p>Password for the Tableau Server or Tableau Online account.</p> <p><b>Note:</b> This property is applicable when you select the value of the <b>Tableau product</b> as Tableau Server or Tableau Online.</p>

Connection property	Description
Site ID	<p>The ID of the site on Tableau Server or Tableau Online where you want to publish the .hyper file. Contact the Tableau administrator to provide the site ID.</p> <p><b>Note:</b> This property is applicable when you select the value of the <b>Tableau product</b> as Tableau Server or Tableau Online.</p>
Schema File Path	<p>The path to a sample .hyper file from where the Secure Agent imports the Tableau metadata. Enter one of the following options for the schema file path:</p> <ul style="list-style-type: none"> <li>- Directory path for the .hyper files.</li> <li>- Empty directory path.</li> </ul> <p>You can only specify an empty directory if you want to publish the .hyper file to Tableau Server or Tableau Online.</p> <p>When you do not specify a schema file path, the Secure Agent displays the projects and data sources that are present on Tableau Server or Tableau Online when you select the target object in the <b>Object</b> target properties. The Secure Agent uses the following default file path for the target .hyper file:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ &lt;latest version&gt;/main/bin/rdtm</pre>

## Teradata connection properties

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

The following table describes the Teradata connection properties:

Connection property	Description
Connection Name	Name of the connection.
Description	Description of the connection.
Type	The type of connection. Select Teradata.
Runtime Environment	<p>The name of the run-time environment where you want to run the tasks.</p> <p>You cannot use the Hosted Agent for Teradata Connector.</p>
TDPID	The name or IP address of the Teradata database machine.
Tenacity	<p>Amount of time, in hours, that Teradata PT API continues trying to log on when the maximum number of operations runs on the Teradata database.</p> <p>Specify a positive integer. Default is 4.</p>
Database Name	<p>The Teradata database name.</p> <p>If you do not enter a database name, Teradata PT API uses the default login database name.</p>

Connection property	Description
Code Page	<p>Code page associated with the Teradata database.</p> <p>Select one the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode and non-Unicode data.</li> </ul> <p>When you run a task that extracts data from a Teradata source, the code page of the Teradata PT API connection must be the same as the code page of the Teradata source.</p>
Max Sessions	<p>Maximum number of sessions that Teradata PT API establishes with the Teradata database. Specify a positive, non-zero integer. Default is 4.</p>
Min Sessions	<p>Minimum number of Teradata PT API sessions required for the Teradata PT API job to continue.</p> <p>Specify a positive integer between 1 and the Max Sessions value. Default is 1.</p>
Sleep	<p>Amount of time, in minutes, that Teradata PT API pauses before it retries to log on when the maximum number of operations runs on the Teradata database.</p> <p>Specify a positive, non-zero integer. Default is 6.</p>
Data Encryption	<p>Enables full security encryption of SQL requests, responses, and data.</p> <p>Default is disabled.</p>
Block Size	<p>Maximum block size, in bytes.</p> <p>Teradata PT API uses this property to read the data block size from source through the Export operator.</p> <p>Maximum is 16775168 bytes for Teradata Database version 16.20 and higher.</p> <p>If the Teradata Database version is lower than 16.20, then Teradata scales down the block size from 16775168 bytes to the maximum allowed value. The block size 16775168 is not allowed in the Spool mode. For more information, see Teradata logs and verify the Teradata documentation of the same version.</p>
Authentication Type	<p>Method to authenticate the user. Select one of the following authentication types:</p> <ul style="list-style-type: none"> <li>- Native. Authenticates your user name and password against the Teradata database specified in the connection.</li> <li>- LDAP. Authenticates user credentials against the external LDAP directory service.</li> <li>- KRB5. Authenticates to the Teradata database through Kerberos.</li> </ul> <p>Default is Native.</p>
Kerberos Artifacts Directory	<p>Directory that contains the Kerberos configuration files named <code>krb5.conf</code> and <code>IICSTPT.keytab</code>.</p> <p>Applicable when you select KRB5 as the authentication type.</p>
Metadata Advanced Connection Properties	<p>The values to set the optional properties of the JDBC driver to fetch the metadata.</p> <p>For example, <code>tmode=ANSI</code>.</p>
Enable Metadata Qualification	<p>Select this option to enable the Teradata connection to read reserved words used as table or column names from the Teradata database.</p> <p>By default, the Enable Metadata Qualification checkbox is not selected and the Secure Agent does not read reserved words from Teradata.</p>

Connection property	Description
User Name	Database user name with the appropriate read and write database permissions to access the database. If you select KRB5 as the authentication type, you must specify the Kerberos user name.
Password	Password for the database user name. If you select KRB5 as the authentication type, you do not need to specify the Kerberos user password.

## UKGPro connection properties

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

The following table describes the UKGPro connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	The user name of the UKGPro service account. Specify one of the following user names: <ul style="list-style-type: none"> <li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the user name of the service account in UKGPro.</li> <li>- To read Time Management data, specify the ODataService user name associated with UKG support.</li> </ul>
Password	The password of the UKGPro service account. Specify one of the following passwords: <ul style="list-style-type: none"> <li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the password of the service account in UKGPro.</li> <li>- To read Time Management data, specify the ODataService password associated with UKG support.</li> </ul>
Service Host Name	The organization domain of UKGPro to read data from the HR, Payroll, Talent, Benefits, or the Integration Events module. To get the service host name, navigate to <b>UKGPro &gt; Menu &gt; System Configuration &gt; Security &gt; Web Services</b> . Specify the service host name in the following format: <code>service\$.ultipro.com,</code> where \$ is a numeric value. To read the Time Management data, specify the clock server URL provided by UKG support.
User API Key	The User API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module. To get the user API key, navigate to <b>UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio Dashboard &gt; Service Accounts graphic tile</b> To read the Time Management data, specify None as the value of the user API key.

Property	Description
Customer API Key	<p>The Customer API key to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the customer API key, navigate to <b>Dashboard &gt; Service Accounts graphic tile &gt; UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio</b>.</p>
Application Module	<p>Determines the type of objects that you can access through the connection.</p> <p>You can select from the following modules to access data from UKGPro:</p> <p><b>HR, Payroll, Talent, and Benefits</b></p> <p>Access HR, Payroll, Talent, and Benefits objects.</p> <p><b>Integration Events</b></p> <p>Access the Integration Events object to read subscribed Integration Events, such as the date and time of the completed events.</p> <p><b>Other</b></p> <p>Access Time Management objects.</p>

## UKGPro V2 connection properties

When you set up a UKGPro V2 connection, you must configure the connection properties.

The following table describes the UKGPro V2 connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	<p>The user name of the UKGPro service account.</p> <p>Specify one of the following user names:</p> <ul style="list-style-type: none"> <li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the user name of the service account in UKGPro.</li> <li>- To read Time Management data, specify the ODataService user name associated with UKG support.</li> </ul>
Password	<p>The password of the UKGPro service account.</p> <p>Specify one of the following passwords:</p> <ul style="list-style-type: none"> <li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the password of the service account in UKGPro.</li> <li>- To read Time Management data, specify the ODataService password associated with UKG support.</li> </ul>

Property	Description
Service Host Name	<p>The organization domain of UKGPro to read data from the HR, Payroll, Talent, Benefits, or the Integration Events module.</p> <p>To get the service host name, navigate to <b>UKGPro &gt; Menu &gt; System Configuration &gt; Security &gt; Web Services</b>.</p> <p>Specify the service host name in the following format:  <code>service\$.ultipro.com</code>,  where \$ is a numeric value.</p> <p>To read the Time Management data, specify the clock server URL provided by UKG support.</p>
User API Key	<p>The User API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the user API key, navigate to <b>UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio Dashboard &gt; Service Accounts graphic tile</b></p> <p>To read the Time Management data, specify None as the value of the user API key.</p>
Customer API Key	<p>The Customer API key to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the customer API key, navigate to <b>Dashboard &gt; Service Accounts graphic tile &gt; UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio</b>.</p>
Application Module	<p>Determines the type of objects that you can access through the connection.</p> <p>You can select from the following modules to access data from UKGPro:</p> <p><b>HR, Payroll, Talent, and Benefits</b></p> <p>Access HR, Payroll, Talent, and Benefits objects.</p> <p><b>Integration Events</b></p> <p>Access the Integration Events object to read subscribed Integration Events, such as the date and time of the completed events.</p> <p><b>Other</b></p> <p>Access Time Management objects.</p>

# UltiPro connection properties

When you set up an UltiPro connection, you must configure the connection properties.

The following table describes the UltiPro connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Password	The password of the UltiPro service account. Specify one of the following passwords: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the password of the service account in UltiPro.</li><li>- To read Time Management data, specify the ODataService password associated with UKG support.</li></ul>
Username	The user name of the UltiPro service account. Specify one of the following user names: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the user name of the service account in UltiPro.</li><li>- To read Time Management data, specify the ODataService user name associated with UKG support.</li></ul>
Service Host Name	<p>The organization domain of UltiPro to read data from the HR, Payroll, Talent, Benefits, or the Integration Events module.</p> <p>To get the service host name, navigate to <b>UltiPro &gt; Menu &gt; System Configuration &gt; Security &gt; Web Services</b>.</p> <p>Specify the service host name in the following format:</p> <p><code>service\$.ultipro.com,</code></p> <p>where \$ is a numeric value.</p> <p>To read the Time Management data, specify the clock server URL provided by UKG support.</p>
Customer API Key	<p>The Customer API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the customer API key, navigate to <b>Dashboard &gt; Service Accounts graphic tile &gt; UltiPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio</b>.</p>
User API Key	<p>The User API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the user API key, navigate to <b>UltiPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio Dashboard &gt; Service Accounts graphic tile</b></p> <p>To read the Time Management data, specify None as the value of the user API key.</p>
Application Module	<p>Determines the type of objects that you can access through the connection.</p> <p>You can select from the following modules to access data from Ultipro:</p> <p><b>HR, Payroll, Talent, and Benefits</b></p> <p>Access HR, Payroll, Talent, and Benefits objects.</p> <p><b>Integration Events</b></p> <p>Access the Integration Events object to read subscribed Integration Events, such as the date and time of the completed events.</p> <p><b>Other</b></p> <p>Access Time Management objects.</p>

# VSAM CDC connection properties

When you configure a VSAM CDC connection, you must set the connection properties.

The following table describes VSAM CDC connection properties:

Property	Description
Connection Name	A name for the VSAM CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the VSAM CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For VSAM CDC, the type must be <b>VSAM CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for VSAM change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example: <code>CDC1A:1467</code>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains the capture registrations for the VSAM source data sets. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.

Property	Description
Encryption	<p>Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> <p>The default is <b>None</b>.</p>
Pacing Size	<p>Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance.</p> <p>The default and minimum value is 0.</p>
Pacing Units	<p>Type of units to use with the <b>Pacing Size</b> property.</p> <p>Select either <b>Rows</b> or <b>Kilobytes</b>.</p>
Map Location	<p>Host name or IP address of the system where the extraction maps reside. Also include the port number.</p> <p>This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.</p> <p>Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p style="text-align: center;"><i>host_name:port_number</i></p> <p>For example:</p> <p>CDC01:25100</p> <p><b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.</p>
Map Location User	<p>A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.</p>
Map Location Password	<p>Password associated with the user name that is specified in <b>Map Location User</b> property.</p>
Event Table	<p>If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The VSAM event table must reside on the CDC source system.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) VSAM CDC connections in PowerCenter.</p>

# VSAM connection properties

When you configure a VSAM connection, you must set the connection properties.

The following table describes the VSAM connection properties:

Property	Description
Connection Name	A name for the VSAM connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the VSAM connection. Maximum length is 4000 characters.
Type	Type of connection. For VSAM, the type must be <b>VSAM</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for VSAM runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example: <code>LSNR1:1467</code>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.
Offload Threads	The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs. Valid values are 1 through 64. Default is 0, which disables multithreading. Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.

Property	Description
Array Size	<p>For VSAM data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) VSAM connections in PowerCenter.</p>
Write Properties	<p>Write Mode. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

## Web Service Consumer connection properties

When you configure a Web Service Consumer connection, you must configure the connection properties.

The following table describes the Web Service Consumer connection properties:

Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select Web Service Consumer from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.

Property	Description
Authentication	<p>You can configure the connection to use the following types of authentication:</p> <p><b>Username Token</b></p> <p>Use the user name token and the password to authenticate the web services.</p> <p><b>Other Authentication</b></p> <p>Use the WSDL URL and endpoint URL to authenticate the web services.</p> <p><b>NTLM Authentication</b></p> <p>Use NTLM V2 authentication to authenticate the web services.</p>
WSDL URL	The URL provided by the web service.
Endpoint URL	Endpoint URL for the web service. The WSDL file specifies this URL in the location element.
Username	Applicable if you use Username Token or NTLM authentication. User name to authenticate the web service.
Password	Applicable if you use Username Token or NTLM authentication. Password to authenticate the web service.
DOMAIN NAME	Applicable if you use NTLM authentication. Name of the domain that authenticates the accounts.
Encrypt Password	Applicable if you use Username Token authentication. Enables the PasswordDigest property which combines the password with a nonce and a time stamp. The mapping task applies a SHA hash on the password, encodes it in base64 encoding, and uses the encoded password in the SOAP header.
Must Understand	Applicable if you use Username Token authentication. Specifies whether to process a header entry or not.
HTTP Username	User name to access the web service.
HTTP Password	Password to access the web service.

## Workday Mass Ingestion connection properties

When you set up a Workday Mass Ingestion connection, you must configure the connection properties.

The properties of a Workday Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **Basic:** Authenticates the connection by validating the login credentials of the Workday account.
- **OAuth 2.0 Refresh Token Flow:** Authenticates the connection by using an application that is registered in Workday. To use this method, you must register an application in Workday and then specify the client ID and client secret of the application in the connection properties. For more information about registering an application in Workday, see the [Workday documentation](#).

## Connection properties for Basic authentication

The following table describes the connection properties for a Workday Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	Identifier of the Workday tenant that you want to access.
Version	Optional. Web Service Description Language (WSDL) version for the endpoints that the connection must use to retrieve Workday data. The list of operations supported for a web service depends on the WSDL version that you specify in this field. <b>Note:</b> Informatica recommends that you use WSDL v37.0 because Workday Mass Ingestion connections might not read data from the services that are not part of WSDL v37.0. For more information on the WSDL versions, see the <a href="#">Workday Web Services (WWS) documentation</a> .
User Name	User name of the Workday account.
Password	Password for the Workday account.

**Note:** If you configure a connection with the Basic authentication method and then test the connection, the test is always successful even if the connection property values that you specified are incorrect. Therefore, ensure that you specify correct values for the connection properties before you save the connection.

## Connection properties for OAuth 2.0 Refresh Token Flow authentication

The following table describes the connection properties for a Workday Mass Ingestion connection configured with OAuth 2.0 Refresh Token Flow authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	Identifier of the Workday tenant that you want to access.
Version	Optional. Web Service Description Language (WSDL) version for the endpoints that the connection must use to retrieve Workday data. The list of operations supported for a web service depends on the WSDL version that you specify in this field. <b>Note:</b> Informatica recommends that you use WSDL v37.0 because Workday Mass Ingestion connections might not read data from the services that are not part of WSDL v37.0. For more information on the WSDL versions, see the <a href="#">Workday Web Services (WWS) documentation</a> .

Connection property	Description
User Name	Optional. User name of the Workday account.
Client ID	Client ID of the application registered in Workday.
Client Secret	Private key of the application registered in Workday.
Refresh Token	Refresh token string that Workday generates for the registered application.
Token Endpoint	OAuth token endpoint of the Workday instance. The registered application sends the access token requests to this endpoint.

## Workday V2 connection properties

When you set up a Workday V2 connection, you must configure the connection properties.

The following table describes the Workday V2 connection properties:

Connection property	Description
Type	Connection to access Workday resources. Select Workday V2.
Runtime Environment	The name of the run-time environment where you want to run the tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication	Authentication by Workday service for users who want to access Workday modules. Select Workday from the drop down list.
Username	User name for the Workday tenant to log in to the Workday service. You can enter the user name, or the user name and tenant in the following format: <username>@<tenant name>. For example, jjoe@informatica_pt1. If you do not provide the tenant name, the Secure Agent appends the tenant name value to the user name that you specify in the connection property.
Password	Password associated with the user name.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	The Workday tenant ID that you want to access. For example, informatica_pt1
Module Name	The Workday service that you want to access. For example, Human_Resources, Financial_Management, and Staffing. For example, to view the available modules for version 26.1 of the web services, see the following link: <a href="https://community.workday.com/sites/default/files/file-hosting/productionapi/index.html">https://community.workday.com/sites/default/files/file-hosting/productionapi/index.html</a>

Connection property	Description
Version	<p>The Web Service Description Language (WSDL) version for a service that you want to fetch from Workday. The list of operations supported for a service depends on the WSDL version that you select.</p> <p>For the supported versions, see the following link:  <a href="https://community.workday.com/sites/default/files/file-hosting/productionapi/versions/index.html">https://community.workday.com/sites/default/files/file-hosting/productionapi/versions/index.html</a></p>
Customized	<p>The Standard or Custom WSDL to fetch Workday object fields.</p> <p>To fetch Workday custom object fields, select Customized. Default is Standard WSDL.</p>

## Xactly connection properties

When you set up an Xactly connection, configure the connection properties.

The following table describes the Xactly connection properties:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Xactly connection type.
Runtime Environment	<p>Name of the runtime environment where you want to run the tasks.</p> <p>You can specify a Secure Agent, Hosted Agent, or serverless runtime environment for a mapping.</p>
UserID	The UserID for accessing the Xactly portal.
PassKey	The password for accessing the Xactly portal.
Xactly App Name	The application name to sign in to Xactly.
WSDL URL	The WSDL URL.
Endpoint URL	The endpoint URL where you want to send the request.
Enable Logging	<p>Enables logging for the task.</p> <p>Select to log SOAP request and response in the session log file.</p>

## XML Source connection properties

When you create an XML Source connection, you must configure the connection properties.

The following table describes the XML Source connection properties:

Connection property	Description
Connection Name	Name of the XML Source connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select XML Source from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Sample XML File Name	Enter the XML file path.
Sample XSD Schema Name	Enter the XSD file path.

## XML Target connection properties

When you create an XML Target connection, you must configure the connection properties.

The following table describes the XML Target connection properties:

Connection property	Description
Connection Name	Enter a name for the connection.
Description	Provide a description for the connection.
Type	Select XML Target from the list.
Secure Agent	Select the secure agent from the list.
Sample XML/XSD Schema Name	Enter XSD file path or XML file path.
XML Working Directory	Enter the file path for XML working directory.
Final XML File Name	Enter final XML file path with the file name.

**Note:** The XML target Connector will create other files in XML working directory for its internal processing, which you can delete after generating the final XML to save the space.

# Yellowbrick Data Warehouse connection properties

When you set up a Yellowbrick Data Warehouse connection, you must configure the connection properties.

The following table describes the Yellowbrick Data Warehouse connection properties:

Connection property	Description
Connection Name	Name of the connection.
Description	Optional. Description that you use to identity the connection.
Type	Select Yellowbrick as the connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Database	Name of the Yellowbrick Data Warehouse that you want to connect to.
Host Name	Hostname or IP address of the Yellowbrick server.
Password	Password for the Yellowbrick Data Warehouse.
Port No	Port number of the Yellowbrick Data Warehouse.
Schema Name	Name of the schema. Required if you select Specified for Schema Policy.
Schema Policy	Policy for naming the schemas for tables. Select one of the following options: <ul style="list-style-type: none"><li>- None</li><li>- Specified</li><li>- FromImport: Not applicable</li></ul>
User Name	User name for the Yellowbrick Data Warehouse.
Secure Connection	Select this option to use TLS to secure the communication with Yellowbrick. Default is false.
Secure CA Cert	Use the name of the custom PEM-encoded certificate file or the name and password of the JKS keystore file to customize trust with secure communications. The name and password of the JKS keystore file must be in the following format: FILENAME:PASSWORD If a file name is not specified, use the following fallback root CA certificate file: Windows: %APPDATA%\postgresql\root.crt If the file exists, it will be treated the same as a specified Secure CA Certificate file. For more information, see the Yellowbrick Documentation Library.
Secure Disable Trust	Select this option to disable the SSL and TLS trust when you use a secured connection. Default is false.

# Zendesk Mass Ingestion connection properties

When you set up a Zendesk Mass Ingestion connection, you must configure the connection properties.

The properties of a Zendesk Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **Basic:** Authenticates the connection by using the login credentials and subdomain associated with the Zendesk account. The Basic authentication method does not use any encrypted access token to connect to the data source, which results in quick and easy access to Zendesk data.

**Note:** You can use the Basic authentication method only if your Zendesk account is not configured with two-factor authentication. If the account is configured with two-factor authentication, you must use the OAuth 2.0 authentication method for the connection.

- **OAuth 2.0:** Authenticates the connection by using an application that is registered in Zendesk along with the login credentials and subdomain associated with the Zendesk account. To use this method, you must register an application in Zendesk and then specify the client ID and client secret of the application in the connection properties. For more information about registering an application in Zendesk, see the [Zendesk documentation](#).

## Connection properties for Basic authentication

The following table describes the connection properties for a Zendesk Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the Zendesk account. The user name is an email address.
Password	Password for the Zendesk account.
Subdomain	URL of the Zendesk help center that you want to access.

**Note:** For more information about the Basic authentication method, see the Zendesk documentation.

## Connection properties for OAuth 2.0 authentication

The following table describes the connection properties for a Zendesk Mass Ingestion connection configured with OAuth 2.0 authentication:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the Zendesk account. The user name is an email address.

Connection property	Description
Password	Password for the Zendesk account.
Subdomain	URL of the Zendesk help center that you want the connection to access.
Client ID	Client ID of the application registered in Zendesk.
Client Secret	Client secret of the application registered in Zendesk.
Grant Type	OAuth 2.0 grant type to be used by the connection. By default, Zendesk Mass Ingestion connections are configured to use the password grant type to exchange user names and passwords for access tokens.

**Note:** For more information about the OAuth 2.0 authentication method, see the Zendesk documentation.

## Zendesk V2 connection properties

When you set up a Zendesk V2 connection, configure the connection properties.

The following table describes the Zendesk V2 connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Zendesk V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	Username of the Zendesk account.
Password	Password of the Zendesk account.
URL	URL of the Zendesk account. Specify the complete URL. For example, <a href="https://informaticabusinesssolution13.zendesk.com/api/v2">https://informaticabusinesssolution13.zendesk.com/api/v2</a> .
Enable Logging	Select the checkbox to enable logging.
Use Proxy	Connects to Zendesk through proxy server. Select the checkbox to use proxy server.
Custom Field	Specify custom fields for Zendesk objects.

## Rules and guidelines for custom fields

Consider the following rules and guidelines when you configure a custom field:

- Specify the custom fields in Zendesk using the following format, where FieldKey is value of the **Field key** in Zendesk:

```
Object1="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldKey2,DataType,Size,Filterable,PrimaryKey"
Object2="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldKey2,DataType,Size,Filterable,PrimaryKey"
```

For example, you can specify the following custom fields for Organizations and Users objects:

```
Organizations="support_description,String,255,true,false"
Users="problems,String,255,true,false";age,Double,0,true,false";"required,Boolean,0,true,false";"select,String,255,true,false";"support_description,String,255,true,false";"reg_ex,String,255,true,false"
```

- When you specify a custom field for Tickets object, you must specify the custom fields in the following format:

```
Tickets="CF_FieldID1,DataType,Size,Filterable,PrimaryKey";"CF_FieldID2,DataType,Size,Filterable,PrimaryKey"
```

For example:

```
Tickets="CF_360003199614,String,255,true,false";"CF_360003373654,String,255,true,false"
```

- Specify the custom fields for different objects in a new line.
- When you specify multiple custom fields for an object, you must separate each custom field with a semicolon (;).
- If you specify a size for a custom field, the agent considers the size of only the string data type. You must set the size for custom fields of other data types as zero.
- The field key in a custom field must not contain special characters.
- To find the field key for Tickets object in the Zendesk website, go to **Settings > Manage Ticket Fields**.

## Zuora AQuA connection properties

When you set up a Zuora AQuA connection, configure the connection properties.

The following table describes the Zuora AQuA connection properties:

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 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Zoura AQuA connection type.

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent runtime environment.
Endpoint URL	The URL of the Zuora server. For example, you can specify the URL as <code>https://www.zuora.com/apps/api/</code> .
Username	User name for the Zuora account.
Password	Password for the Zuora account.
Entity ID	The entity ID to connect to a specific entity in a tenant that contains multiple entities.
Entity Name	The entity name to connect to a specific entity in a tenant that contains multiple entities.
WSDL Version	Zuora WSDL version number.
Retrieve Deleted Rows	Optional. Retrieves the deleted rows in an incremental mode. Default is false.
UTC Offset	The difference in hours from the Coordinated Universal Time (UTC) for a particular place and date.  You can use the UTC offset value when you use the <code>lastruntime</code> data filter field to read data from Zuora based on the specified time zone.

## Zuora Multi-Entity connection properties

When you create a Zuora Multi-Entity connection, you must configure the connection properties.

The following table describes the Zuora Multi-Entity connection properties:

Property	Description
Runtime Environment	Runtime environment that contains the Secure Agent used to access Zuora.
Username	User name for the Zoura portal login.
Password	Password for the Zuora portal login.
WSDL Url	Path of the Zuora WSDL Url.
EndPoint Url	Path of the Zuora Endpoint Url.
UTC Offset	The difference in hours from the Coordinated Universal Time (UTC) for a particular place and date.  You can use the UTC offset value when you use the <code>\$LastRuntime</code> data filter field to read data from Zuora Multi-Entity based on the specified time zone.  By default, the UTC value is 0.

Property	Description
No of Records for Batch	Number of the records that the Secure Agent reads in batches.
No of records for Batch Write	Number of the records that the Secure Agent writes to the end point in batches. By default, the value of the field is 100.
Enable Debug logger	Determines whether to print the SOAP request and response in the session log.
Entity Id	When you have multiple entities in a single tenant, specify the entity ID to connect to a particular entity.
Entity Name	When you have multiple entities in a single tenant, specify the entity name to connect to a particular entity.

## Zuora REST V2 connection properties

When you create a Zuora REST V2 connection, you must configure the connection properties.

The following table describes the Zuora REST V2 connection properties:

Property	Description
Runtime Environment	Runtime environment that contains Secure Agent used to access Zuora.
Authentication	Select <b>ZuoraRESTV2</b> .
Base Url	Endpoint URL of REST API to which you want to make calls. Do not specify the query parameters with the Base URL. For example, <a href="https://rest.apisandbox.zuora.com/">https://rest.apisandbox.zuora.com/</a>
Authentication Type	The type of user authentication to connect to the Zuora portal login. Select authentication method that the connector must use to login to the Zuora portal login. You can select the following authentication types: <ul style="list-style-type: none"> <li>- Basic Auth</li> <li>- OAuth 2.0</li> </ul> Default is OAuth 2.0.
Username	User name for the Zuora portal login. You must enter the username if you select <b>Basic Auth</b> as the <b>Authentication Type</b> .
Password	Password for the Zuora portal login. You must enter the password if you select <b>Basic Auth</b> as the <b>Authentication Type</b> .
Client ID	The client ID to complete the OAuth 2.0 authentication to connect to Zuora. You must enter the client ID if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Client Secret	The client secret key to complete the OAuth 2.0 authentication to connect to Zuora. You must enter the client secret key if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Grant Type	The type of authentication used to obtain the token. Use <b>client_credentials</b> .

Property	Description
Entity ID	<p>When you have multiple entities in a single tenant, specify the entity ID to connect to a particular entity.</p> <p>You can also specify the entity ID in the Request Message Editor. If you specify the entity ID in connection properties and Request Message Editor, entity ID specified in the connection properties takes precedence</p> <p><b>Note:</b> <b>Entity ID</b> is mandatory when you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> and specify custom fields in the <b>Custom Field Config</b> property.</p>
Zuora API Version	<p>Swagger file that you want to use for the Zuora REST V2 connection.</p> <p>You can select the <b>Zuora Swagger API V1_2017_09_06</b> or <b>Zuora Swagger API V1_2018_08_23</b> swagger file.</p>
Custom Field Config	<p>Specify the name of the Zuora objects for which you want to configure custom fields as comma-separated values.</p> <p>You can specify the following Zuora objects that support custom fields:</p> <ul style="list-style-type: none"> <li>- Account</li> <li>- Accounting Code</li> <li>- Accounting Period</li> <li>- Amendment</li> <li>- Contact</li> <li>- CreditBalanceAdjustment</li> <li>- CreditMemoItem</li> <li>- CreditMemo</li> <li>- DebitMemoItem</li> <li>- DebitMemo</li> <li>- Feature</li> <li>- InvoiceAdjustment</li> <li>- InvoiceItemAdjustment</li> <li>- InvoiceItem</li> <li>- Invoice</li> <li>- JournalEntryItem</li> <li>- JournalEntry</li> <li>- OrderAction</li> <li>- Order</li> <li>- Payment</li> <li>- ProductFeature</li> <li>- Product</li> <li>- ProductRatePlanCharge</li> <li>- ProductRatePlan</li> <li>- RatePlanCharge</li> <li>- RatePlan</li> <li>- Refund</li> <li>- RevenueEventItem</li> <li>- RevenueEvent</li> <li>- RevenueScheduleItem</li> <li>- RevenueSchedule</li> <li>- Subscription</li> <li>- SubscriptionProductFeature</li> <li>- TaxationItem</li> <li>- Usage</li> </ul> <p><b>Note:</b> Applies only when you select the value of the <b>Zuora API Version</b> as <b>Zuora Swagger API V1_2018_08_23</b>.</p> <p>For more information about Zuora objects that support custom fields, visit <a href="https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Manage_Custom_Fields/Objects_that_Support_Custom_Fields_in_Zuora">https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Manage_Custom_Fields/Objects_that_Support_Custom_Fields_in_Zuora</a>.</p>

## CHAPTER 4

# Swagger file generation for REST V2 connections

For the REST V2 connector, you must specify the path to a Swagger file that defines the REST service when you configure the connection. You can generate a Swagger file using Informatica Intelligent Cloud Services.

Informatica Intelligent Cloud Services supports Swagger specification version 2.0. When you generate a Swagger file in Informatica Intelligent Cloud Services, you send an API call to the service using a sample request. If you do not have permissions to send an API call to the service, you can generate a Swagger file using a sample request and a sample response without submitting an API call.

You cannot modify a Swagger file once it is created. If you want to make changes in a Swagger file, create a new Swagger file.

**Note:** The swagger file generation functionality is available for the convenience of the REST V2 customers. Informatica does not warranty the compatibility of the swagger file for all customer scenarios.

## Generating a Swagger file

You can generate a swagger file for REST V2 connections from the **Swagger Files** page in Administrator.

1. Click **New**.
2. Enter a name and description for the swagger file.
3. Specify the swagger details. The following table describes parameters to create a swagger file:

Parameter	Description
Runtime Environment	Mandatory. Name of the runtime environment used to generate the swagger file.
URL	Mandatory. URL consists of the host name and port number. For example: <code>http://localhost:8000</code>

Parameter	Description
Verb	Select the REST method being used by the web service. The supported methods are: <ul style="list-style-type: none"> <li>- GET</li> <li>- POST</li> <li>- PUT</li> <li>- DELETE</li> <li>- OPTIONS</li> <li>- HEAD</li> <li>- PATCH</li> </ul>
Authentication Type	If required, select the authentication method to login to the web service application. Default is none.
API Base Path	The path on which the API is served. The base path is the one specified after the hostname and port. For example, if the REST web service URL is <code>http://localhost:8000/greetings/hello?Status=GoodMorning</code> , the base path will be <code>/greetings</code> .
API Path	<p>The path specified after the base path is API path. For example, if the REST web service URL is <code>http://localhost:8000/greetings/hello?Status=GoodMorning</code>, the API path will be <code>/hello?Status=GoodMorning</code>.</p> <p>To define a path parameter, enclose the path, which is being treated as variable with curly brackets {}.</p> <p>For example, if the REST web service URL is <code>https://localhost:8080/sample/Stringoperation/concat/str1/str2?id=123</code> and <code>concat</code> is a variable in this path, define the API path as below:</p> <pre>Stringoperation/{concat}/str1/str2?id=123</pre> <p>You can define any number of path parameters.</p> <p><b>Note:</b> The API path can include the query parameters. If you define the query parameters with the API path, do not specify the query parameters in the <b>Query Params</b> field.</p>
Username	The user name to login to the web service application. Required for Basic and Digest authentication types.
Password	The password associated with the user name. Required for Basic and Digest authentication types.
Token	The access token to connect to the web service application. Required only for OAuth authentication type.
Token Secret	The password associated with the OAuth token. Required for OAuth authentication type.
Consumer Key	The client key associated with the web service application. Required for OAuth authentication type.
Consumer Secret	The client password to connect to the web service application. Required only for OAuth authentication type.
Accept	Select the MIME type.
Headers	Define header parameters in JSON format. For example: <code>{"Accept-Charset":"utf-8"}</code> Maximum length is 1020 characters.

Parameter	Description
Query Params	<p>Provide query parameters in JSON format. For example: {"name":"subject","description":"The subject to be greeted."}</p> <p>Defining query parameters in the Query Params field adds the query parameters as input parameters in the Swagger specification file.</p> <p>If you define the query parameters in <b>Query Params</b>, do not specify the query parameters in the <b>API Path</b> field.</p> <p>Maximum length is 1020 characters.</p>
Operation ID	Mandatory. A unique text identifier for the API path.
Content Type	Select the MIME type.
Raw Body	<p>Enter the request body content. If you select <code>application/x-www-form-urlencoded</code> in the content type, specify the raw body parameters in the key-value pair. Each key-value pair starts with a new line. Example:</p> <pre>a : b c : d e : f</pre> <p>Not applicable to the GET method.</p>
JSON Response File	<p>Optional. Upload the JSON response file if you want to generate the swagger definition from the response file. No call is made to the REST endpoint if you select the JSON response file.</p> <p>If you do not provide the JSON response file, a call is made to the REST endpoint to fetch the response for generating swagger definition.</p>

**Note:** For information about the swagger definition objects and fields supported by REST V2 Connector, see the REST V2 Connector documentation.

- Click **Save** to generate the swagger file. An entry for the swagger file appears in the **Swagger Files** page.  
In case of failure while connecting to the web service, the fault response obtained from the web service is logged in the **Swagger Files** page.
- Click the download icon to save the Swagger file in a local directory.  
To use the swagger file in the REST V2 connection, copy the file to the Secure Agent system where you will create a REST V2 connection.

# INDEX

## A

- Adabas
  - connection properties [17](#)
- Adabas CDC
  - connection properties [15](#)
- add-on connectors
  - building [9](#)
  - installing [9](#)
  - purpose [9](#)
- Adobe Experience Platform
  - connection properties [19](#)
- Advanced FTP V2 connections
  - properties [20](#)
- Advanced FTPS V2 connections
  - properties [22](#)
- Advanced SFTP V2 connections
  - properties [24](#)
- Amazon Athena
  - connection properties [25](#)
- Amazon Aurora
  - connection properties [28](#)
- Amazon DynamoDB V2
  - connection properties [29](#)
- Amazon Kinesis connection
  - overview [29](#)
- Amazon Redshift
  - connection properties [32](#)
- Amazon Redshift V2
  - connection properties [34](#)
- Amazon S3
  - connection properties [38](#)
- Amazon S3 V2
  - connection properties [39](#)
- Anaplan V2
  - connection properties [44](#)
- Ariba V2
  - connection properties [46](#)
- AS2
  - properties [47](#)
- authentication
  - API key [251](#)
  - OAuth 2.0 authorization code [204](#), [244](#), [256](#), [301](#), [303](#)
  - OAuth 2.0 client credentials [206](#), [242](#), [259](#), [304](#)
- Azure Data Lake Storage Gen2
  - connection properties [164](#)

## B

- Birst Cloud Connect
  - connection properties [51](#)
- Business 360
  - connection properties [52](#)
- Business 360 FEP
  - connection properties [53](#)

## C

- CallidusCloud Commissions
  - connection properties [54](#)
- CallidusCloud File Processor
  - connection properties [55](#)
- Cassandra V2 connections
  - properties [59](#)
- Chatter
  - connection properties [57](#)
- Concur V2
  - connection properties [57](#)
- connection
  - Amazon Kinesis Firehose
    - connection properties [30](#)
  - Amazon Kinesis Streams
    - connection properties [31](#)
  - properties [53](#)
- connection dependencies [13](#)
- connection properties
  - company name [179](#)
  - Domo [95](#)
  - language [179](#)
  - SuccessFactors ODATA Connector [307](#)
  - WSDL URI [179](#)
- connections
  - SAP ADSO Writer [268](#)
  - Adabas CDC connection properties [15](#)
  - Adabas connection properties [17](#)
  - add-on connectors [9](#)
  - Adobe Experience Platform [19](#)
  - Amazon Athena [25](#)
  - Amazon Aurora [28](#)
  - Amazon DynamoDB V2 [29](#)
  - Amazon Redshift [32](#)
  - Amazon Redshift V2 [34](#)
  - Amazon S3 [38](#)
  - Amazon S3 V2 [39](#)
  - AMQP
    - connection properties [26](#)
  - Anaplan V2 [44](#)
  - application ID [174](#)
  - Ariba V2 [46](#)
  - AS2 [47](#)
  - Azure Data Lake Storage Gen2 [164](#)
  - Azure Event Hub
    - connection properties [166](#)
  - Birst Cloud Connect [51](#)
  - Business 360 [52](#)
  - Business 360 FEP [53](#)
  - CallidusCloud Commissions [54](#)
  - CallidusCloud File Processor [55](#)
  - Chatter [57](#)
  - Concur V2 [57](#)
  - configuring properties [12](#)
  - connection properties [174](#)

connections (*continued*)

- Coupa V2 [61](#)
- creating [12](#)
- Cvent [62](#)
- Databricks Delta [63](#)
- Datacom CDC connection properties [68](#)
- Datacom connection properties [70](#)
- Db2 Data Map connection properties [72](#)
- Db2 for i CDC connection properties [74](#)
- Db2 for i connection properties [76](#)
- Db2 for i Database Ingestion [78](#)
- Db2 for LUW CDC connection properties [79](#)
- Db2 for LUW Database Ingestion connection [82](#)
- Db2 for z/OS Bulk Load connection properties [83](#)
- Db2 for z/OS CDC connection properties [84](#)
- Db2 for z/OS connection properties [86](#)
- Db2 for z/OS Image Copy connection properties [88](#)
- Db2 for z/OS Unload File connection properties [90](#)
- Db2 for zOS Database Ingestion [92](#)
- DB2 Loader [93](#)
- Db2 Warehouse on Cloud connection properties [94](#)
- Dropbox [96](#)
- Eloqua Bulk API [98](#)
- Eloqua REST [99](#)
- FHIR connection properties [100](#)
- File List [105](#)
- File Processor [106](#)
- FileIO [104](#)
- flat file [107](#)
- FTP/SFTP [109](#)
- Google Ads [111](#)
- Google Analytics [112](#)
- Google Analytics Mass Ingestion [113](#)
- Google BigQuery [113](#), [119](#)
- Google Bigtable [127](#)
- Google Cloud Spanner [127](#)
- Google Cloud Storage [128](#)
- Google Cloud Storage V2 [129](#)
- Google Drive [130](#)
- Google PubSub [131](#), [132](#)
- Google Sheets [133](#), [134](#)
- Greenplum [134](#)
- guidelines for [11](#)
- Hive [137](#)
- HubSpot [139](#)
- IBM MQ [139](#)
- IDMS CDC connection properties [140](#)
- IDMS connection properties [142](#)
- IMS CDC connection properties [144](#)
- IMS connection properties [146](#)
- JD Edwards EnterpriseOne [150](#)
- JDBC [148](#)
- JDBC V2 [149](#)
- JIRA [152](#)
- JIRA Cloud [152](#)
- JMS
  - connection properties [153](#)
- JSON Target [154](#)
- Kafka
  - connection properties [155](#)
- LDAP [158](#)
- Litmos [159](#)
- Marketo V3 [159](#)
- Microsoft Access [160](#)
- Microsoft Azure Blob Storage V2 [161](#)
- Microsoft Azure Blob Storage V3 [161](#)
- Microsoft Azure Cosmos DB SQL API [162](#)
- Microsoft Azure Data Lake Storage Gen1 V2 [163](#)

connections (*continued*)

- Microsoft Azure Data Lake Storage Gen1 V3 [163](#)
- Microsoft Azure SQL Data Warehouse - Database Ingestion [167](#)
- Microsoft Azure SQL Data Warehouse V2 [168](#)
- Microsoft Azure Synapse Analytics - Database Ingestion [171](#)
- Microsoft Azure Synapse SQL [169](#)
- Microsoft CDM Folders V2 [173](#)
- Microsoft Dynamics 365 Mass Ingestion [176](#)
- Microsoft Excel [180](#)
- Microsoft SharePoint [180](#)
- Microsoft Sharepoint Online [181](#)
- Microsoft SQL Server [184](#)
- Microsoft SQL Server CDC connection properties [182](#)
- MLLP connection properties [187](#)
- MQTT
  - connection properties [191](#)
- MRI Software [192](#)
- MySQL [195](#)
- MySQL CDC connection properties [193](#)
- Netezza [199](#)
- NetSuite Mass Ingestion [199](#)
- NICE Satmetrix [201](#)
- OData [201](#)
- OData V2 Protocol Reader [203](#)
- OData V2 Protocol Writer [202](#)
- ODBC [207](#)
- OpenAir [209](#)
- Oracle [215](#)
- Oracle Business Intelligence Publisher V1 [210](#)
- Oracle CDC connection properties [211](#)
- Oracle CRM Cloud V1 [218](#)
- Oracle CRM On Demand [218](#)
- Oracle Database Ingestion [219](#)
- Oracle E-Business Suite [224](#)
- Oracle E-Business Suite Interface [225](#)
- Oracle Financials Cloud [227](#)
- Oracle Financials Cloud V1 [228](#)
- Oracle Fusion Cloud Mass Ingestion [230](#)
- Oracle HCM Cloud [230](#)
- Oracle HCM Cloud V1 [232](#)
- overview [11](#)
- PostgreSQL [236](#)
- PostgreSQL CDC connection properties [234](#)
- purpose [9](#)
- QuickBooks V2 [238](#)
- REST V2 [239](#), [247](#)
- REST V3 [255](#)
- rules for [11](#)
- rules for FTP/SFTP [111](#)
- Salesforce [262](#)
- Salesforce Analytics [262](#)
- Salesforce Marketing Cloud [264](#)
- Salesforce Mass Ingestion [265](#)
- SAP BW Reader [273](#)
- SAP HANA [278](#)
- SAP HANA CDC connection properties [275](#)
- SAP HANA Database Ingestion [279](#)
- SAP IDoc Reader [280](#)
- SAP IDoc Writer [280](#)
- SAP IQ [281](#)
- SAP Mass Ingestion [282](#)
- SAP ODP Extractor [290](#)
- SAP RFC/BAPI Interface [287](#)
- SAP Table [288](#)
- Satmetrix [295](#)
- Sequential connection properties [296](#)
- service URL [174](#)
- ServiceNow [296](#)

connections (*continued*)

- ServiceNow Mass Ingestion [298](#)
- Snowflake Data Cloud [299](#), [300](#)
- Tableau V3 [309](#)
- Teradata connection [310](#)
- testing [12](#)
- UKGPro [312](#)
- UKGPro V2 [313](#)
- UltiPro [315](#)
- VSAM CDC connection properties [316](#)
- VSAM connection properties [318](#)
- Web Service Consumer [319](#)
- Workday Mass Ingestion [320](#)
- Workday V2 [322](#)
- Xactly [323](#)
- XML Source [324](#)
- XML Target [324](#)
- Yellowbrick [325](#)
- Zendesk Mass Ingestion [326](#)
- Zuora AQuA [328](#)
- Zuora Multi-Entity [329](#)
- Zuora REST V2 [330](#)

connections Hadoop Files V2 [135](#)

Cosmos DB URI [162](#)

Couchbase connections  
properties [60](#)

Coupa V2  
connection properties [61](#)

Cvent  
connection properties [62](#)

## D

database [162](#)

Databricks Delta  
connection properties [63](#)

Datacom  
connection properties [70](#)

Datacom CDC  
connection properties [68](#)

Db2 Data Map  
connection properties [72](#)

Db2 for i  
connection properties [76](#)

Db2 for i CDC  
connection properties [74](#)

Db2 for i Database Ingestion connections  
connection properties [78](#)

Db2 for LUW CDC  
connection properties [79](#)

Db2 for LUW Database Ingestion connection  
connection properties [82](#)

Db2 for z/OS  
connection properties [86](#)

Db2 for z/OS Bulk Load  
connection properties [83](#)

Db2 for z/OS CDC  
connection properties [84](#)

Db2 for z/OS Image Copy  
connection properties [88](#)

Db2 for z/OS Unload File  
connection properties [90](#)

Db2 for zOS Database Ingestion connections  
connection properties [92](#)

DB2 Loader  
connection properties [93](#)

Db2 Warehouse on Cloud

connection properties [94](#)

dependencies

connections [13](#)

Domo Connection

properties [95](#)

Dropbox

connection properties [96](#)

## E

Elasticsearch connections  
properties [97](#)

Eloqua Bulk API  
connection properties [98](#)

Eloqua REST  
connection properties [99](#)

## F

FHIR

connection properties [100](#)

File List

connection properties [105](#)

File Processor

connection properties [106](#)

FileIO

connection properties [104](#)

flat file

connection properties [107](#)

FTP/SFTP

connection properties [109](#)

FTP/SFTP connections

local directory [109](#)

overview [109](#)

remote directory [109](#)

rules and guidelines [111](#)

## G

generating Swagger files [332](#)

Google Ads

connection properties [111](#)

Google Analytics

connection properties [112](#)

Google Analytics Mass Ingestion connections

connection properties [113](#)

Google BigQuery

connection properties [113](#), [119](#)

Google Bigtable

connection properties [127](#)

Google Cloud Spanner

connection properties [127](#)

Google Cloud Storage

connection properties [128](#)

Google Cloud Storage V2

connection properties [129](#)

Google Drive

connection properties [130](#)

Google PubSub

connection properties [131](#), [132](#)

Google Sheets

connection properties [133](#), [134](#)

Greenplum

connection properties [134](#)

## H

Hadoop Files V2  
connection properties [135](#)  
Hive  
connection properties [137](#)  
HubSpot  
connection properties [139](#)

## I

IBM MQ  
connection properties [139](#)  
IDMS  
connection properties [142](#)  
IDMS CDC  
connection properties [140](#)  
IMS  
connection properties [146](#)  
IMS CDC  
connection properties [144](#)

## J

JD Edwards EnterpriseOne  
connection properties [150](#)  
JDBC  
connection properties [148](#), [278](#)  
JDBC V2  
connection properties [149](#)  
JIRA  
connection properties [152](#)  
JIRA Cloud connection [152](#)  
JSON Target connection  
properties [154](#)

## K

key exchange algorithms  
SFTP connections [110](#)

## L

LDAP  
connection properties [158](#)  
Litmos  
connection properties [159](#)

## M

Marketo V3  
connection properties [159](#)  
Microsoft Access  
connection properties [160](#)  
Microsoft Azure Blob Storage V2  
connection properties [161](#)  
Microsoft Azure Blob Storage V3  
connection properties [161](#)  
Microsoft Azure Cosmos DB SQL API  
connection properties [162](#)  
Microsoft Azure Data Lake Storage Gen1 V2  
connection properties [163](#)

Microsoft Azure Data Lake Storage Gen1 V3  
connection properties [163](#)  
Microsoft Azure SQL Data Warehouse - Database Ingestion  
connections  
connection properties [167](#)  
Microsoft Azure SQL Data Warehouse V2  
connection properties [168](#)  
Microsoft Azure Synapse Analytics Database Ingestion connections  
connection properties [171](#)  
Microsoft Azure Synapse SQL  
connection properties [169](#)  
Microsoft CDM Folders V2  
connection properties [173](#)  
Microsoft Dynamics 365 for Sales Connector  
connection properties [175](#)  
Microsoft Dynamics 365 Mass Ingestion connections  
connection properties [176](#)  
Microsoft Dynamics AX V3  
connection properties [179](#)  
Microsoft Dynamics AX V3 connections  
properties [179](#)  
Microsoft Excel  
connection properties [180](#)  
Microsoft SharePoint  
connection properties [180](#)  
Microsoft Sharepoint Online  
connection properties [181](#)  
Microsoft SQL Server  
connection properties [184](#)  
Microsoft SQL Server CDC  
connection properties [182](#)  
MLLP  
connection properties [187](#)  
MongoDB V2 connections  
properties [188](#)  
MongoDB V2 Connector  
administration [190](#)  
MRI Software  
connection properties [192](#)  
MySQL  
connection properties [195](#)  
MySQL CDC  
connection properties [193](#)

## N

Netezza  
connection properties [199](#)  
NetSuite Mass Ingestion connections  
connection properties [199](#)  
NICE Satmetrix  
connection properties [201](#)

## O

OData  
connection properties [201](#)  
OData V2 Applications  
connection properties [202](#)  
OData V2 Protocol Reader  
connection properties [203](#)  
ODBC  
connection properties [207](#)  
OpenAir  
connection properties [209](#)

- Oracle
  - connection properties [215](#)
- Oracle Business Intelligence Publisher V1
  - connection properties [210](#)
- Oracle CDC
  - connection properties [211](#)
- Oracle Cloud Object Storage connections
  - properties [214](#)
- Oracle CRM Cloud V1
  - connection properties [218](#)
- Oracle CRM On Demand
  - connection properties [218](#)
- Oracle Database Ingestion connections
  - connection properties [219](#)
- Oracle E-Business Suite
  - connection properties [224](#)
- Oracle E-Business Suite Interface
  - connection properties [225](#)
- Oracle Financials Cloud
  - connection properties [227](#)
- Oracle Financials Cloud V1
  - connection properties [228](#)
- Oracle Fusion Cloud Mass Ingestion connections
  - connection properties [230](#)
- Oracle HCM Cloud
  - connection properties [230](#)
- Oracle HCM Cloud V1
  - connection properties [232](#)

## P

- PostgreSQL
  - connection properties [236](#)
- PostgreSQL CDC
  - connection properties [234](#)

## Q

- QuickBooks V2
  - connection properties [238](#)

## R

- Redis connections
  - properties [238](#)
- REST V2
  - authentication
    - standard [239](#), [247](#)
  - connection properties [239](#), [247](#)
- REST v2 connection
  - Swagger file generation [332](#)
- REST V3
  - authentication
    - standard [255](#)
  - connection properties [255](#)

## S

- Salesforce
  - connection properties [262](#)
- Salesforce Analytics
  - connection properties [262](#)
- Salesforce Marketing Cloud
  - connection properties [264](#)

- Salesforce Mass Ingestion connections
  - connection properties [265](#)
- SAP ADSO Writer
  - connection properties [268](#)
- SAP BW BEx query connection
  - properties [272](#)
- SAP BW Reader
  - connection properties [273](#)
- SAP HANA CDC
  - connection properties [275](#)
- SAP HANA Database Ingestion connections
  - connection properties [279](#)
- SAP IDoc Reader
  - connection properties [280](#)
- SAP IDoc Writer
  - connection properties [280](#)
- SAP IQ
  - connection properties [281](#)
- SAP Mass Ingestion connections
  - connection properties [282](#)
- SAP RFC/BAPI Interface
  - connection properties [287](#)
- SAP Table
  - connection properties [288](#)
- Satmetrix
  - connection properties [295](#)
- Sequential File
  - connection properties [296](#)
- ServiceNow
  - connection properties [296](#)
- ServiceNow Mass Ingestion connections
  - connection properties [298](#)
- SFTP connections
  - key exchange algorithms [110](#)
- Snowflake Data Cloud
  - authentication
    - standard [300](#)
  - connection properties [299](#), [300](#)
- SuccessFactors Connector
  - connection properties [308](#)
- SuccessFactors LMS connections
  - properties [306](#)
- SuccessFactors ODATA Connector
  - connection properties [307](#)
- Swagger files
  - generating [332](#)

## T

- Tableau V3
  - connection properties [309](#)
- Teradata connection
  - connection properties [310](#)

## U

- UKGPro
  - connection properties [312](#)
- UKGPro V2
  - connection properties [313](#)
- UltiPro
  - connection properties [315](#)

## V

viewing connection dependencies [13](#)

VSAM

connection properties [318](#)

VSAM CDC

connection properties [316](#)

## W

Web Service Consumer

connection properties [319](#)

Workday Mass Ingestion connections

connection properties [320](#)

Workday V2

connection properties [322](#)

## X

Xactly

connection properties [323](#)

XML Source

connection properties [324](#)

XML Target

connection properties [324](#)

## Y

Yellowbrick

connection properties [325](#)

## Z

Zendesk Mass Ingestion connections

connection properties [326](#)

Zendesk V2 connections

properties [327](#)

Zuora AQUA

connection properties [328](#)

Zuora Multi-Entity

connection properties [329](#)

Zuora REST V2

connection properties [330](#)