Informatica® INFACore
November 2023

Connections for INFACore

Informatica INFACore Connections for INFACore
November 2023

Publication Date: 2024-09-20

Table of Contents

Preface

Read *Connections for INFACore* to learn how to configure connections between INFACore and cloud applications, databases, and storage services. Refer to *Connections* for information about the connections that can be used with INFACore.

Informatica Resources

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

Informatica Documentation

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

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

Informatica Intelligent Cloud Services web site

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

Informatica Intelligent Cloud Services Communities

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

Access the Informatica Intelligent Cloud Services Community at:

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

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

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

Informatica Intelligent Cloud Services Marketplace

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

https://marketplace.informatica.com/

Data Integration connector documentation

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

Informatica Knowledge Base

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

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

Informatica Intelligent Cloud Services Trust Center

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

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

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

To subscribe, go to https://status.informatica.com/ and click **SUBSCRIBE TO UPDATES**. You can then choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or online.

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

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

CHAPTER 1

Connections to source and target endpoints

Connections provide access to data in cloud applications, databases, and file storage services. They specify the location of the data source from where you read from or write data.

INFACore offers multiple connections designed to connect to data sources and integrate data. You create connections in the **Connect to Data Sources** section in the JupyterLab extension for INFACore. You can select the type of data source and then create a connection to access the data source. You enter the connection properties so that INFACore can connect to the source or target to read from or write data.

You can also programmatically connect to a data source using the INFACore Python SDK. When you create a connection, the connection becomes available for use within the organization.

For certain connectors, you have the option to configure additional attributes for both the source and target from the Python SDK. These advanced attributes help you leverage additional functionalities in the data sources. To get the attributes for a data object, call the get_advanced_config() method. To set the value of the parameters, call the set_advanced_config(), and then configure the read or write operation.

To find if additional source and target properties are available for a data source, see *Connections for INFACore* documentation.

For more information on how to call these methods, see *INFACore SDK Reference for Python*.

Amazon Athena

Create an Amazon Athena connection to connect to read data from Amazon Athena tables and views.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Before you begin

You can use an Amazon Athena connection after the organization administrator performs the following tasks:

- Manages authentication by creating an access key and a secret key. The access and secret keys are required when you configure an Amazon Athena connection.
- Creates an AWS Key Management Service (AWS KMS)-managed customer master key if you want to enable server-side encryption or client-side encryption.
- Creates the minimal Amazon Identity and Access Management (IAM) policy, AWS Glue data catalog policy, and Amazon Athena policy for an Amazon Athena connection.

Create a minimal Amazon IAM policy

Create an Amazon IAM policy and define the permissions to store Amazon Athena results on Amazon S3.

Use the following minimum required permissions to store Amazon Athena results on Amazon S3:

- PutObject
- GetObject
- DeleteObject
- ListBucket

You can use the following sample Amazon IAM policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/*",
                "arn:aws:s3:::<bucket_name>"
            ]
        }
    ]
}
```

Create an AWS Glue data catalog policy

You can use AWS IAM to define policies and roles that are needed to access resources used by AWS Glue.

You can use the following sample policy for AWS Glue data catalog:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:*",
            ],
            "Resource": [
                "*"
            ]
        }
```

```
        ]
    }
```

Create an Amazon Athena policy

Specify the minimum required permissions for Amazon Athena Connector to read data from views and external tables in the AWS Glue data catalog and to read and query Amazon S3 files.

You can use the following minimum required permissions:

- GetWorkGroup
- GetTableMetadata
- StartQueryExecution
- GetQueryResultsStream
- ListDatabases
- GetQueryExecution
- GetQueryResults
- GetDatabase
- ListTableMetadata
- GetDataCatalog

You can use the following sample policy for Amazon Athena:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "athena:GetWorkGroup",
                "athena:GetTableMetadata",
                "athena:StartQueryExecution",
                "athena:GetQueryResultsStream",
                "athena:ListDatabases",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:GetDatabase",
                "athena:ListTableMetadata",
                "athena:GetDataCatalog"
            ],
            "Resource": [
                "arn:aws:athena:*:*:workgroup/*",
                "arn:aws:athena:*:*:datacatalog/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "athena:ListDataCatalogs",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Connection properties

The following table describes the Amazon Athena 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.
Authentication Type	The authentication mechanism to connect to Amazon Athena. Select **Permanent IAM Credentials**.
Access Key	Optional. The access key to connect to Amazon Athena.
Secret Key	Optional. The secret key to connect to Amazon Athena.

JDBC URL	The URL of the Amazon Athena connection.
	Enter the JDBC URL in the following format:
	`jdbc:awsathena://AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;`
	You can use pagination to fetch the Amazon Athena query results. Set the property `UseResultsetStreaming=0` to use pagination.
	Enter the property in the following format:
	`jdbc:awsathena://AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;UseResultsetStreaming=0;`
	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.
	By default, streaming is enabled.

Customer Master Key ID	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. 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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Amazon Athena:

Property	Description
Retain Athena Query Result On S3 File	Specifies whether you want to retain the Amazon Athena query result on the Amazon S3 file. Select the check box to retain the Amazon Athena query result on the Amazon S3 file. The Amazon Athena query result in stored in the CSV file format. By default, the **Retain Athena Query Result on S3 File** check box is not selected.
S3OutputLocation	Specifies the location of the Amazon S3 file that stores the result of the Amazon Athena query. You can also specify the Amazon S3 file location in the `S3OutputLocation` parameter in the **JDBC URL** connection property. If you specify the Amazon S3 output location in both the connection and the advanced source properties, the Secure Agent uses the Amazon S3 output location specified in the advanced source properties.
Fetch Size	Determines the number of rows to read in one result set from Amazon Athena. Default is 10000.
Encryption Type	Encrypts the data in the Amazon S3 staging directory. You can select the following encryption types: - None - SSE-S3 - SSE-KMS - CSE-KMS Default is None.
Schema Name	Overrides the schema name of the source object.
Source Table Name	Overrides the table name used in the metadata import with the table name that you specify.
SQL Query	Overrides the default SQL query. Enclose column names in double quotes. The SQL query is case sensitive. Specify an SQL statement supported by the Amazon Athena database. When you specify the columns in the SQL query, ensure that the column name in the query matches the source column name in the mapping.

Amazon Redshift

Create an Amazon Redshift connection to connect to Amazon Redshift. .

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your AWS account.

The following video shows you how to get information from your AWS account:

Connection properties

The following table describes the Amazon Redshift 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.
Username	User name of the Amazon Redshift account.
Password	Password for the Amazon Redshift account.
Access Key ID	Access key to access the Amazon S3 staging bucket. Enter the access key value based on the following authentication methods: - Basic authentication. Enter the actual access key value. - IAM authentication. Do not enter the access key value. - Temporary security credentials using assume role. Enter access key of an IAM user with no permissions to access the Amazon S3 staging bucket. - Assume role for EC2. Do not enter the access key value.

Property	Description
Secret Access Key	Secret access key to access the Amazon S3 staging bucket. The secret key is associated with the access key and uniquely identifies the account. Enter the access key value based on the following authentication methods: - Basic authentication. Enter the actual access secret value. - IAM authentication. Do not enter the access secret value. - Temporary security credentials using assume role. Enter access secret of an IAM user with no permissions to access Amazon S3 staging bucket. - Assume role for EC2. Do not enter the access secret value.
IAM Role ARN	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.
External Id	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.
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. **Note:** The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different account.
Master Symmetric Key	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.
JDBC URL	The URL of the Amazon Redshift connection. Enter the JDBC URL in the following format: `jdbc:redshift://<amazon_redshift_host>:<port_number>/<database_name>`

Property	Description
Cluster Region	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. If you select a cluster region in both **Cluster Region** and **JDBC URL** connection properties, the agent ignores the cluster region that you specify in the **JDBC URL** connection property. To use the cluster region name that you specify in the **JDBC URL** connection property, select **None** as the cluster region in this property. You can only read data from or write data to the cluster regions supported by AWS SDK. Select one of the following cluster regions: - None - Asia Pacific(Mumbai) - Asia Pacific(Seoul) - Asia Pacific(Singapore) - Asia Pacific(Sydney) - Asia Pacific(Tokyo) - Asia Pacific(Hong Kong) - AWS GovCloud (US) - AWS GovCloud (US-East) - Canada(Central) - China(Bejing) - China(Ningxia) - EU(Ireland) - EU(Frankfurt) - EU(Paris) - EU(Stockholm) - South America(Sao Paulo) - Middle East(Bahrain) - US East(N. Virginia) - US East(Ohio) - US West(N. California) - US West(Oregon) Default is **None**.
Customer Master Key ID	The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access. 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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Amazon Redshift:

Property	Description
Read Mode	Specifies the read mode to read data from the Amazon Redshift source. You can select one the following read modes: - Direct. Reads data directly from the Amazon Redshift source without staging the data in Amazon S3. - Staging. Reads data from the Amazon Redshift source by staging the data in the S3 bucket. Default is Staging.
Fetch Size	Determines the number of rows to read in one resultant set from Amazon Redshift. Applies only when you select the **Direct** read mode. Default is 10000. **Note:** If you specify fetch size 0 or if you don't specify a fetch size, the entire data set is read directly at the same time than in batches.
S3 Bucket Name	Amazon S3 bucket name for staging the data. You can also specify the bucket name with the folder path. If you provide an Amazon S3 bucket name that is in a different region than the Amazon Redshift cluster, you must configure the **REGION** attribute in the Unload command options.
Enable Compression	Compresses the staging files into the Amazon S3 staging directory. The task performance improves when the Secure Agent compresses the staging files. Default is selected.
Staging Directory Location	Location of the local staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. Specify the directory path in the following manner: `<staging directory>` For example, `C:\Temp`. Ensure that you have the write permissions on the directory.
Unload Options	Unload command options. Add options to the Unload command to extract data from Amazon Redshift and create staging files on Amazon S3. Provide an Amazon Redshift Role Amazon Resource Name (ARN). You can add the following options: - DELIMITER - ESCAPE - PARALLEL - NULL - AWS_IAM_ROLE - REGION - ADDQUOTES For example: DELIMITER = \036;ESCAPE = OFF;NULL=text;PARALLEL = ON;AWS_IAM_ROLE=arn;aws;iam;;<account ID>;role/<role-name>;REGION = ap-south-1 Specify a directory on the machine that hosts the Secure Agent. **Note:** If you do not add the options to the Unload command manually, the Secure Agent uses the default values.
Treat NULL Value as NULL	Retains the null values when you read data from Amazon Redshift.

Property	Description
Encryption Type	Encrypts the data in the Amazon S3 staging directory. You can select the following encryption types: - None - SSE-S3 - SSE-KMS - CSE-SMK Default is None.
Download S3 Files in Multiple Parts	Downloads large Amazon S3 objects in multiple parts. When the file size of an Amazon S3 object is greater than 8 MB, you can choose to download the object in multiple parts in parallel. Default is 5 MB.
Multipart Download Threshold Size	The maximum threshold size to download an Amazon S3 object in multiple parts. Default is 5 MB.
Schema Name	Overrides the default schema name. **Note:** You cannot configure a custom query when you use the schema name.
Source Table Name	Overrides the default source table name. **Note:** When you select the source type as **Multiple Objects** or **Query**, you cannot use the **Source Table Name** option.
Pre-SQL	The pre-SQL commands to run a query before you read data from Amazon Redshift. You can also use the UNLOAD or COPY command. The command you specify here is processed as a plain text.
Post-SQL	The post-SQL commands to run a query after you write data to Amazon Redshift. You can also use the UNLOAD or COPY command. The command you specify here is processed as a plain text.
Select Distinct	Selects unique values. The Secure Agent includes a `SELECT DISTINCT` statement if you choose this option. Amazon Redshift ignores trailing spaces. Therefore, the Secure Agent might extract fewer rows than expected. **Note:** If you select the source type as query or use the **SQL Query** property and select the **Select Distinct** option, the Secure Agent ignores the **Select Distinct** option.
SQL Query	Overrides the default SQL query. Enclose column names in double quotes. The SQL query is case sensitive. Specify an SQL statement supported by the Amazon Redshift database. When you specify the columns in the SQL query, ensure that the column name in the query matches the source column name in the mapping.
Temporary Credential Duration	The time duration during which an IAM user can use the dynamically generated temporarily credentials to access the AWS resource. Enter the time duration in seconds. Default is 900 seconds. If you require more than 900 seconds, you can set the time duration up to a maximum of 12 hours in the AWS console and then enter the same time duration in this property.
Tracing Level	Use the verbose tracing level to get the amount of detail that appears in the log for the Source transformation.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Amazon Redshift:

Property	Description
S3 Bucket Name	Amazon S3 bucket name for writing the files to Amazon Redshift target. You can also specify the bucket name with the folder path. If you provide an Amazon S3 bucket name that is in a different region than the Amazon Redshift cluster, you must configure the **REGION** attribute in the Copy command options.
Enable Compression	Compresses the staging files before writing the files to Amazon Redshift. The task performance improves when the Secure Agent compresses the staged files. Default is selected.
Staging Directory Location	Location of the local staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. Specify the directory path in the following manner: `<staging directory>` For example, `C:\Temp`. Ensure that you have the write permissions on the directory.
Batch Size	Minimum number of rows in a batch. Enter a number greater than 0. Default is 2000000.
Max Errors per Upload Batch for INSERT	Number of error rows that causes an upload insert batch to fail. Enter a positive integer. Default is 1. If the number of errors is equal to or greater than the property value, the Secure Agent writes the entire batch to the error file.
Truncate Target Table Before Data Load	Deletes all the existing data in the Amazon Redshift target table before loading new data.
Require Null Value For Char and Varchar	Replaces the string value with NULL when you write data to Amazon Redshift columns of Char and Varchar data types. Default is an empty string. **Note:** When you run a mapping to write null values to a table that contains a single column of the Int, Bigint, numeric, real, or double data type, the mapping fails. You must provide a value other than the default value in the **Require Null Value For Char And Varchar** property.
WaitTime In Seconds For S3 File Consistency	Number of seconds to wait for the Secure Agent to make the staged files consistent with the list of files available on Amazon S3. Default is 0.

Property	Description
Copy Options	Copy command options. Add options to the Copy command to write data from Amazon S3 to the Amazon Redshift target when the default delimiter comma (,) or double-quote (") is used in the data. Provide the Amazon Redshift Role Amazon Resource Name (ARN). You can add the following options: - DELIMITER - ACCEPTINVCHARS - QUOTE - COMPUPDATE - AWS_IAM_ROLE - REGION For example: `DELIMITER = \036;ACCEPTINVCHARS = #;QUOTE = \037 COMPUPDATE = ON;AWS_IAM_ROLE=arn:aws:iam::<account ID>:role/<role-name>;REGION = ap-south-1` Specify a directory on the machine that hosts the Secure Agent. **Note:** If you do not add the options to the Copy command manually, the Secure Agent uses the default values.
S3 Server Side Encryption	Indicates that Amazon S3 encrypts data during upload. Provide a customer master key ID in the connection property to enable this property. Default is not selected.
S3 Client Side Encryption	Indicates that the Secure Agent encrypts data using a private key. Provide a master symmetric key ID in the connection property to enable this property. If you enable both server-side and client-side encryptions, the Secure Agent ignores the server-side encryption.
Analyze Target Table	Runs an ANALYZE command on the target table. The query planner on Amazon Redshift updates the statistical metadata to build and choose optimal plans to improve the efficiency of queries.
Vacuum Target Table	Recovers disk space and sorts the row in a specified table or all tables in the database. You can select the following recovery options: - None - Full - Sort Only - Delete Only - Reindex Default is None.
Prefix to retain staging files on S3	Retains staging files on Amazon S3. Provide both a directory prefix and a file prefix separated by a slash (/) or only a file prefix to retain staging files on Amazon S3. For example, `backup_dir/backup_file` or `backup_file`.
Success File Directory	Directory for the Amazon Redshift success file. Specify a directory on the machine that hosts the Secure Agent.
Error File Directory	Directory for the Amazon Redshift error file. Specify a directory on the machine that hosts the Secure Agent.

Property	Description
Treat Source Rows As	Overrides the default target operation. Default is **INSERT**. Select one of the following override options: **NONE** By default, none is enabled. The Secure Agent considers the task operation that you select in the **Operation** target property. **INSERT** Performs insert operation. If enabled, the Secure Agent inserts all rows flagged for insert. If disabled, the Secure Agent rejects the rows flagged for insert. **DELETE** Performs delete operation. If enabled, the Secure Agent deletes all rows flagged for delete. If disabled, the Secure Agent rejects all rows flagged for delete. **UPDATE and UPSERT** Performs update and upsert operations. To perform an update operation, you must map the primary key column and at least one column other than primary key column. You can select the following data object operation attributes: - Update as Update: The Secure Agent updates all rows as updates. - Update else Insert: The Secure Agent updates existing rows and inserts other rows as if marked for insert. Amazon Redshift V2 Connector does not support the Upsert operation in the Upgrade Strategy transformation. To use an Update Strategy transformation to write data to an Amazon Redshift target, you must select **Treat Source Rows As** as **None**. By default, the Secure Agent performs the task operation based on the value that you specify in the **Operation** target property. However, if you specify an option in the **Treat Source Rows As** property, the Secure Agent ignores the value of that you specify in the **Operation** target property or in the Update Strategy transformation.
Override Target Query	Overrides the default update query that the Secure Agent generates for the update operation with the update query that you specify.
TransferManager Thread Pool Size	Number of threads to write data in parallel. Default is 10.
Pre-SQL	The pre-SQL commands to run a query before you read data from Amazon Redshift. You can also use the UNLOAD or COPY command. The command you specify here is processed as a plain text.
Post-SQL	The post-SQL commands to run a query after you write data to Amazon Redshift. You can also use the UNLOAD or COPY command. The command you specify here is processed as a plain text.
Preserve record order on write	Retains the order of the records when you read data from a CDC source and write data to an Amazon Redshift target. Use this property when you create a mapping to capture the changed record from a CDC source. This property enables you to avoid inconsistencies between the CDC source and target.
Minimum Upload Part Size	Minimum size of the Amazon Redshift object to upload an object. Default is 5 MB.

Property	Description
Number of files per batch	Calculates the number of the staging files per batch. If you do not provide the number of files, Amazon Redshift V2 Connector calculates the number of the staging files.
Schema Name	Overrides the default schema name.
Target table name	Overwrites the default target table name.
Recovery Schema Name	Schema that contains recovery information stored in the `infa_recovery_table` table on the target system to resume the extraction of the changed data from the last checkpoint.
Temporary Credential Duration	The time duration during which an IAM user can use the dynamically generated temporarily credentials to access the AWS resource. Enter the time duration in seconds. Default is 900 seconds. If you require more than 900 seconds, you can set the time duration maximum up to 12 hours in the AWS console and then enter the same time duration in this property.
Forward Rejected Rows	This property is not applicable for Amazon Redshift V2 Connector.

Amazon S3

Create an Amazon S3 connection to read from or write data of formats such as Avro, flat, binary, ORC, and Parquet file formats to Amazon S3.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your AWS account.

The following video shows you how to get information from your AWS account:

Connection properties

The following table describes the Amazon S3 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.
Access Key	Access key to access the Amazon S3 bucket. Enter the access key value based on the following authentication methods: - Basic authentication. Enter the actual access key value. - IAM authentication. Don't enter the access key value. - Temporary security credentials using assume role. Enter the secret access key of an IAM user with no permissions to access Amazon S3 bucket. - Assume role for EC2. Don't enter the access key value. - Credential profile file authentication. Don't enter the access key value. - Federated user single sign-on. Don't enter the secret access key value.
Secret Key	Secret access key to access the Amazon S3 bucket. The secret key is associated with the access key and uniquely identifies the account. Enter the secret access key value based on the following authentication methods: - Basic authentication. Enter the actual access secret value. - IAM authentication. Don't enter the access secret value. - Temporary security credentials using assume role. Enter access secret of an IAM user with no permissions to access Amazon S3 bucket. - Assume role for EC2. Don't enter the access key value. - Credential profile file authentication. Don't enter the access secret value. - Federated user single sign-on. Don't enter the access secret value.
IAM Role ARN	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. Enter the value of this property if you want to use the temporary security credentials to access the AWS resources. **Note:** 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. For more information about how to get the ARN of the IAM role, see the AWS documentation.
External Id	Provides a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account.
Use EC2 Role to Assume Role	Enables the EC2 role to assume another IAM role specified in the IAM Role ARN option. **Note:** The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different account. By default, the Use EC2 Role to Assume Role check box is not selected.
Folder Path	Bucket name or complete folder path to the Amazon S3 objects. Don't use a slash at the end of the folder path. For example, `<bucket name>/<my folder name>`.
Master Symmetric Key	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.

Property	Description
Customer Master Key ID	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. You must generate the customer master key for the same region where the Amazon S3 bucket resides. You can specify the following master keys: - Customer generated customer master key. Enables client-side or server-side encryption. - 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.
S3 Account Type	The type of the Amazon S3 account. Select from the following options: - Amazon S3 Storage. Enables you to use the Amazon S3 services. - S3 Compatible Storage. Enables you to use the endpoint for a third-party storage provider such as Scality RING or MinIO. Default is Amazon S3 storage.
REST Endpoint	The S3 storage endpoint required for S3 compatible storage. Enter the S3 storage endpoint in HTTP or HTTPs format. For example, http://s3.isv.scality.com.
Region Name	The AWS region of the bucket that you want to access. Select one of the following regions: - Asia Pacific(Mumbai) - Asis Pacific(Jakarta) - Asia Pacific (Osaka) - Asia Pacific(Seoul) - Asia Pacific(Singapore) - Asia Pacific(Sydney) - Asia Pacific(Tokyo) - Asia Pacific(Hong Kong) - AWS GovCloud (US) - AWS GovCloud (US-East) - Canada(Central) - China(Bejing) - China(Ningxia) - EU(Ireland) - EU(Frankfurt) - EU (London) - EU (Milan) - EU(Paris) - EU(Stockholm) - South America(Sao Paulo) - Middle East(Bahrain) - US East(N. Virginia) - US East(Ohio) - US ISO East - US ISOB East (Ohio) - US ISO West - US West(N. California) - US West(Oregon) Default is US East (N. Virginia).

Property	Description
Federated SSO IdP	SAML 2.0-enabled identity provider for the federated user single sign-on to use with the AWS account. Amazon S3 connector supports only the ADFS 3.0 identity provider. Select **None** if you don't want to use federated user single sign-on.
Other Authentication Type	Select one the following authentication types: - NONE - Credential Profile File Authentication 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. Enter the credential profile file path and the profile name to establish the connection with Amazon S3. You can use permanent IAM credentials or temporary session tokens when you configure the Credential Profile File Authentication. Default is NONE.
Credential Profile File Path	Specifies the credential profile file path. 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: `~/.aws/credentials`
Profile Name	Name of the profile in the credential profile file used to get the credentials. If you don't enter the profile name, the credentials from the default profile in the credential profile file are used.
S3 VPC Endpoint Type	The VPC endpoint type for Amazon S3. You can enable private communication with Amazon S3 by selecting a VPC endpoint. Select one of the following VPC endpoint types: - None - Gateway Endpoint - Interface Endpoint Default is None.
Endpoint DNS Name for Amazon S3	The DNS name for the Amazon S3 interface endpoint. Enter the DNS name in the following format: `bucket.<DNS name of the interface endpoint>`
STS VPC Endpoint Type	Applicable when you select the S3 VPC interface endpoint. The VPC endpoint type for AWS STS. When you select **IAM Role ARN** or **Federated SSO IdP**, configure the STS VPC endpoint.
Endpoint DNS Name for AWS STS service	The DNS name for the AWS STS interface endpoint.
KMS VPC Endpoint Type	Applicable when you select the interface endpoint. The VPC endpoint type for the AWS KMS. When you select **Customer Master Key ID**, configure the KMS VPC endpoint.
Endpoint DNS Name for AWS KMS service	The DNS name for the AWS KMS interface endpoint.

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.
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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Amazon S3:

Property	Description
Source Type	Type of the source from which you want to read data. You can select the following source types: - File - Directory Default is **File**.
Folder Path	Overwrites the bucket name or folder path of the Amazon S3 source file. If applicable, include the folder name that contains the source file in the `<bucket_name>/<folder_name>` format. If you do not provide the bucket name and specify the folder path starting with a slash (/) in the `/<folder_name>` format, the folder path appends with the folder path that you specified in the connection properties. For example, if you specify the `/<dir2>` folder path in this property and `<my_bucket1>/<dir1>` folder path in the connection property, the folder path appends with the folder path that you specified in the connection properties in `<my_bucket1>/<dir1>/<dir2>` format. If you specify the `<my_bucket1>/<dir1>` folder path in the connection property and `<my_bucket2>/<dir2>` folder path in this property, the Secure Agent reads the file in the `<my_bucket2>/<dir2>` folder path that you specify in this property.
File Name	Overwrites the Amazon S3 source file name.
Incremental File Load	Indicates whether you want to incrementally load files when you use a directory as the source for a mapping in advanced mode. When you incrementally load files, the mapping task reads and processes only files in the directory that have changed since the mapping task last ran.
Allow Wildcard Characters	Indicates whether you want to use wildcard characters for the directory source type. If you select this option, you can use the question mark (?) and asterisk (*) wildcard characters in the folder path or file name.

Property	Description
Enable Recursive Read	Indicates whether you want to read flat, Avro, JSON, ORC, or Parquet files recursively from the specified folder and its subfolders and files. Applicable when you select the directory source type.
Encryption Type	Method you want to use to decrypt data. You can select one of the following encryption types: - None - Informatica encryption Default is **None**. **Note:** You cannot select client-side encryption, server-side encryption, and server-side encryption with KMS encryption types.
Staging Directory	Path of the local staging directory. Ensure that the user has write permissions on the directory. In addition, ensure that there is sufficient space to enable staging of the entire file. Default staging directory is the `/temp` directory on the machine that hosts the Secure Agent. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0`. The temporary files are created within the new directory. The staging directory source property does not apply to Avro, ORC, and Parquet files.
Hadoop Performance Tuning Options	This property is not applicable for Amazon S3 V2 Connector.
Compression Format	Decompresses data when you read data from Amazon S3. You can choose to decompress the data in the following formats: - None - Bzip2[2] - Gzip - Lzo Default is **None**. You can decompress data for a mapping in advanced mode if the mapping reads data from a JSON file in Bzip2 format. **Note:** Amazon S3 V2 Connector does not support the Lzo compression format even though the option appears in this property.
Download Part Size	Downloads the part size of an Amazon S3 object in bytes. Default is 5 MB. Use this property when you run a mapping to read a file of flat format type.

Property	Description
Multiple Download Threshold	Minimum threshold size to download an Amazon S3 object in multiple parts. To download the object in multiple parts in parallel, ensure that the file size of an Amazon S3 object is greater than the value you specify in this property. Default is 10 MB.
Temporary Credential Duration	The time duration during which an IAM user can use the dynamically generated temporarily credentials to access the AWS resource. Enter the time duration in seconds. Default is 900 seconds. If you require more than 900 seconds, you can set the time duration maximum up to 12 hours in the AWS console and then enter the same time duration in this property.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Amazon S3:

Property	Description
Overwrite File(s) If Exists	Overwrites an existing target file. Default is true.
Folder Path	Bucket name or folder path where you want to write the Amazon S3 target file. The path that you enter here overrides the path specified for the target configured to create at runtime. If applicable, include the folder name that contains the target file in the `<bucket_name>/<folder_name>` format. If you do not provide the bucket name and specify the folder path starting with a slash (/) in the `/<folder_name>` format, the folder path appends with the folder path that you specified in the connection properties. For example, if you specify the `/<dir2>` folder path in this property and `<my_bucket1>/<dir1>` folder path in the connection property, the folder path appends with the folder path that you specified in the connection properties in `<my_bucket1>/<dir1>/<dir2>` format. If you specify the `<my_bucket1>/<dir1>` folder path in the connection property and `<my_bucket2>/<dir2>` folder path in this property, the Secure Agent writes the file in the `<my_bucket2>/<dir2>` folder path that you specify in this property.
File Name	Creates a new file name or overwrites an existing target file name.
Encryption Type	Method you want to use to encrypt data. Select one of the following encryption types: - None - Client Side Encryption - Server Side Encryption - Server Side Encryption with KMS - Informatica Encryption Default is **None**.

Property	Description
Staging Directory	Enter the path of the local staging directory. Ensure that the user has write permissions on the directory. In addition, ensure that there is sufficient space to enable staging of the entire file. Default staging directory is the `/temp` directory on the machine that hosts the Secure Agent. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` The temporary files are created within the new directory. The staging directory target property does not apply to Avro, ORC, and Parquet files.
File Merge	This property is not applicable for Amazon S3 V2 Connector.
Hadoop Performance Tuning Options	This property is not applicable for Amazon S3 V2 Connector.
Compression Format	Compresses data when you write data to Amazon S3. You can compress the data in the following formats: - None - Bzip2 - Deflate - Gzip - Lzo - Snappy - Zlib Default is None. **Note:** Amazon S3 V2 Connector does not support the Lzo compression format even though the option appears in this property.
Object Tags	The key value pairs to add single or multiple tags to the objects stored on the Amazon S3 bucket. You can either enter the key value pairs or specify the file path that contains the key value pairs. Use this property when you run a mapping to write a file of flat format type.
TransferManager Thread Pool Size	The number of threads to write data in parallel. Default is 10. Use this property when you run a mapping to write a file of flat format type. Amazon S3 V2 Connector uses the `AWS TransferManager API` to upload a large object in multiple parts to Amazon S3. When the file size is more than 5 MB, you can configure multipart upload to upload object in multiple parts in parallel. If you set the value of **TransferManager Thread Pool Size** to greater than 50, the value reverts to 50.
Merge Partition Files	Determines whether the Secure Agent must merge the number of partition files as a single file or maintain separate files based on the number of partitions specified to write data to the Amazon S3 V2 targets.

Property	Description
Temporary Credential Duration	The time duration during which an IAM user can use the dynamically generated temporarily credentials to access the AWS resource. Enter the time duration in seconds. Default is 900 seconds. If you require more than 900 seconds, you can set the time duration maximum up to 12 hours in the AWS console and then enter the same time duration in this property.
Part Size	Uploads the part size of an Amazon S3 object in bytes. Default is 5 MB. Use this property when you run a mapping to write a file of flat format type.

Cvent

Create a Cvent connection to connect to Cvent.

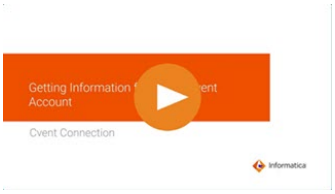
Feature snapshot

Operation	Support
Read	Yes
Write	No

Before you begin

Before you configure the connection properties, you'll need to get information from your Cvent account.

The following video shows you how to get information from your Cvent account:



Connection properties

The following table describes the Cvent 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.
Account Number	Specify the account number.

Property	Description
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

Create a Databricks Delta connection to connect to the Databricks SQL endpoint or Databricks analytics cluster to read or write data.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Databricks account.

The following video shows you how to get information from your Databricks account:

Connection properties

The following table describes the Databricks Delta 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.
Databricks Host	The host name of the endpoint the Databricks account belongs to. Use the following syntax: `jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>;AuthMech=3;UID=token;PWD=<personal-access-token>` **Note:** You can get the URL from the Advanced Options of JDBC or ODBC in the Databricks Delta analytics cluster or all purpose cluster. The value of PWD in Databricks Host, Org Id, and Cluster ID is always `<personal-access-token>`.
Cluster ID	The ID of the Databricks analytics cluster. You can get the cluster ID from the JDBC URL. Use the following syntax: `jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>;AuthMech=3;UID=token;PWD=<personal-access-token>`
Organization Id	The unique organization ID for the workspace in Databricks. Use the following syntax: `jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>;AuthMech=3;UID=token;PWD=<personal-access-token>`
Databricks Token	Personal access token to access Databricks. Ensure that you have permissions to attach to the cluster identified in the **Cluster ID** property.
SQL Endpoint JDBC URL	Databricks SQL endpoint JDBC connection URL. Use the following syntax: `jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint cluster ID>;` This field is required to connect to the Databricks SQL endpoint. Ensure that you set the required environment variables in the Secure Agent. **Note:** The Databricks Host, Organization ID, and Cluster ID properties are not considered if you configure the SQL Endpoint JDBC URL property. For more information on Databricks Delta SQL endpoint, contact Informatica Global Customer Support.
Database	The database in Databricks Delta that you want to connect to. By default, all databases available in the workspace are listed.
JDBC Driver Class Name	The name of the JDBC driver class. Specify the driver class name as `com.simba.spark.jdbc.Driver`.

Property	Description
Cluster Environment	The cloud provider where the Databricks cluster is deployed. Choose from the following options: - AWS - Azure Default is AWS. The connection attributes depend on the cluster environment you select. For more information, see the AWS cluster properties and Azure cluster properties sections.
Min Workers	The minimum number of worker nodes to be used for the Spark job. Minimum value is 1.
Max Workers	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.
DB Runtime Version	The Databricks runtime version. Select 7.3 LTS from the list.
Worker Node Type	The worker node instance type that is used to run the Spark job. For example, the worker node type for AWS can be i3.2xlarge. The worker node type for Azure can be Standard_DS3_v2.
Driver Node Type	The driver node instance type that is used to collect data from the Spark workers. For example, the driver node type for AWS can be i3.2xlarge. The driver node type for Azure can be Standard_DS3_v2. If you don't specify the driver node type, Databricks uses the value you specify in the worker node type field.
Instance Pool ID	The instance pool ID used for the Spark cluster. If you specify the Instance Pool ID, the following connection properties are ignored: - Driver Node Type - EBS Volume Count - EBS Volume Type - EBS Volume Size - Enable Elastic Disk - Worker Node Type - Zone ID
Enable Elastic Disk	Enables the cluster to get additional disk space. Enable this option if the Spark workers are running low on disk space.

Spark Configuration	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"`

Spark Environment Variables	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"`

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Databricks Delta:

Property	Description
Database Name	Overrides the database name provided in connection and the database name provided during metadata import.
Table Name	Overrides the table name used in the metadata import with the table name that you specify.
Pre SQL	The pre-SQL command to run on the Databricks Delta source table before the agent reads the data. For example, if you want to update records in the database before you read the records from the table, specify a pre-SQL statement. The query must include a fully qualified table name. You can specify multiple pre-SQL commands, each separated with a semicolon.
Post SQL	The post-SQL command to run on the Databricks Delta table after the agent completes the read operation. For example, if you want to delete some records after the latest records are loaded, specify a post-SQL statement. The query must include a fully qualified table name. You can specify multiple post-SQL commands, each separated with a semicolon.
Staging Location	Relative directory path to store the staging files. - If the Databricks cluster is deployed on AWS, use the path relative to the Amazon S3 staging bucket. - If the Databricks cluster is deployed on Azure, use the path relative to the Azure Data Lake Store Gen2 staging filesystem name. **Note:** If staging location is not specified for Unity Catalog, the mapping fails.
Job Timeout	Maximum time in seconds that is taken by the Spark job to complete processing. If the job is not completed within the time specified, the Databricks cluster terminates the job and the mapping fails. If the job timeout is not specified, the mapping shows success or failure based on the job completion.
Job Status Poll Interval	Poll interval in seconds at which the Secure Agent checks the status of the job completion. Default is 30 seconds.

Property	Description
DB REST API Timeout	The Maximum time in seconds for which the Secure Agent retries the REST API calls to Databricks when there is an error due to network connection or if the REST endpoint returns `5xx HTTP` error code. Default is 10 minutes.
DB REST API Retry Interval	The time Interval in seconds at which the Secure Agent must retry the REST API call, when there is an error due to network connection or when the REST endpoint returns `5xx HTTP` error code. This value does not apply to the Job status REST API. Use job status poll interval value for the Job status REST API. Default is 30 seconds.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Databricks Delta:

Advanced Property	Description
Target Database Name	Overrides the database name provided in the connection and the database selected in the metadata browser for existing targets.
Target Table Name	Overrides the table name at runtime for existing targets.
Pre SQL	The pre-SQL command to run before the agent writes to Databricks Delta. For example, if you want to assign sequence object to a primary key field of the target table before you write data to the table, specify a pre-SQL statement. You can specify multiple pre-SQL commands, each separated with a semicolon.
Post SQL	The post-SQL command to run after the agent completes the write operation. For example, if you want to alter the table created by using create target option and assign constraints to the table before you write data to the table, specify a post-SQL statement. You can specify multiple post-SQL commands, each separated with a semicolon.
Write Disposition	Overwrites or adds data to the existing data in a table. You can select from the following options: - Append. Appends data to the existing data in the table even if the table is empty. - Truncate. Overwrites the existing data in the table.
Staging Location	Relative directory path to store the staging files. - If the Databricks cluster is deployed on AWS, use the path relative to the Amazon S3 staging bucket. - If the Databricks cluster is deployed on Azure, use the path relative to the Azure Data Lake Store Gen2 staging filesystem name. **Note:** Mandatory if you want to create a new target at runtime when the source query is set for Unity Catalog.
Job Timeout	Maximum time in seconds that is taken by the Spark job to complete processing. If the job is not completed within the time specified, the Databricks cluster terminates the job and the mapping fails. If the job timeout is not specified, the mapping shows success or failure based on the job completion.

Advanced Property	Description
Job Status Poll Interval	Poll interval in seconds at which the Secure Agent checks the status of the job completion. Default is 30 seconds.
DB REST API Timeout	The Maximum time in seconds for which the Secure Agent retries the REST API calls to Databricks when there is an error due to network connection or if the REST endpoint returns `5xx HTTP` error code. Default is 10 minutes.
DB REST API Retry Interval	The time Interval in seconds at which the Secure Agent must retry the REST API call, when there is an error due to network connection or when the REST endpoint returns `5xx HTTP` error code. This value does not apply to the Job status REST API. Use job status poll interval value for the Job status REST API. Default is 30 seconds.
Update Mode	Defines how rows are updated in the target tables. Select from the following options: - Update As Update: Rows matching the selected update columns are updated in the target. - Update Else Insert: Rows matching the selected update columns are updated in the target. Rows that don't match are appended to the target.

Eloqua

Create an Eloqua connection to connect to the Eloqua application.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Oracle Eloqua account.

The following video shows you how to get information from your Oracle Eloqua account:

Connection properties

The following table describes the Eloqua 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.
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 Determining Base URL.
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.
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.

FileIO

You can use the FileIo connection to exports Salesforce attachments to a file system. You can upload files from a local file system to Salesforce. FileIo connection works with any source or target that supports binary or base64 encoded content.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the FileIO connection properties:

Property	Description
Connection Name	Enter a unique name for the connection.
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 `.infaccess` empty file. Create a folder within the parent directory with any name other than inprocess, success, and error. For example, you can create a `read`, `write`, or `test` 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: - Binary: When you select Binary, you must map FileContentAsBinary the field. - base64 encoded string: By default this option is selected. When you select this option, you must map FileContentAsBase64String.
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 **Auto Archive Source Files** option is enabled.
Error Directory	Mention the error directory path. When they are issues/errors in file processing. Such files are moved to error directory.

File Processor

Use the File Processor connection when you perform file processing operations, such as transferring, archiving, unarchiving, encrypting, decrypting, compressing, decompressing, moving, or copying files.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the File Processor 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.
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	The pattern of the files that you want to transfer. For Example, if you want to select file based on a date pattern, you can specify the date format as DD/MM/YYYY in the file pattern field. Note: File Pattern field is not applicable when you select **all** from **Select File** connection property.
Days Calculation	Use days calculation to select files that are created or modified before the specified date or after the specified date. Select files based on Contains Date Pattern, specify the **days calculation** 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. For example, if you select file based on Contains Date Pattern, use the data filters to specify LastModDate as 02/02/2016 in DD/MM/YYYY format, and specify days calculation as -1. Files that are modified till 01/02/2016 are selected.
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

Create a Flat File connection to read from or write to a flat file.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the flat file 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.
Directory	Directory where the flat file is stored and must be accessible by the agent. Enter the full directory or click **Browse** 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. 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. **Note:** On Windows, the **Browse for Directory** 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.
Browse button	Use to locate and select the directory where flat files are stored.

Connection Property	Description
Date Format	Date format for date fields in the flat file. Default date format is: MM/dd/yyyy HH:mm:ss
Code Page	The code page of the system that hosts the flat file. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode data. - UTF-16 encoding of Unicode (Big Endian). - UTF-16 encoding of Unicode (Lower Endian). - Shift-JIS. Select for double-byte character data. - ISO 8859-15 Latin 9 (Western European). - ISO 8859-2 Eastern European. - ISO 8859-3 Southeast European. - ISO 8859-5 Cyrillic. - ISO 8859-9 Latin 5 (Turkish). - IBM EBCDIC International Latin-1. - Japanese EUC (with \ <-> Yen mapping - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - MS Windows Traditional Chinese, superset of Big 5 - Taiwan Big-5 (w/o euro update) - Chinese EUC - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew (w/o euro update) - EBCDIC Hebrew (updated with new sheqel, control characters) - IBM EBCDIC US English IBM037 If the file contains supplementary characters with UTF-16 encoding, the task fails. **Note:** 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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from a flat file:

Property	Description
Tracing Level	Detail level of error and status messages that Data Integration writes in the session log. You can choose terse, normal, verbose initialization, or verbose data. Default is normal.
Thousand Separator	Thousand separator character. Can be none, comma, or period. Cannot be the same as the decimal separator or the delimiter character. Field type must be Number. You might also need to update the field precision and scale. Default is None.
Decimal Separator	Decimal character. Can be a comma or period. Cannot be the same as the thousand separator or delimiter character. Field type must be Number. You might also need to update the field precision and scale. Default is Period.

Property	Description
Source File Directory	For flat file sources, name of the source directory. For FTP sources, name and path of the local source file directory used to stage the source data. By default, the mapping task reads source files from the source connection directory. You can also use an input parameter to specify the file directory. If you use the service process variable directory $PMSourceFileDir, the task writes target files to the configured path for the system variable. To find the configured path of a system variable, see the pmrdtm.cfg file located at the following directory: `<Secure Agent installation directory>\apps\Data_Integration_Server\<Data Integration Server version>\ICS\main\bin\rdtm` You can also find the configured path for the $PMSourceFileDir variable in the Data Integration Server system configuration details in Administrator.
Source File Name	For flat file sources, file name, or file name and path of the source file. You can also use an input parameter to specify the file name. For FTP sources, name of the local source file used to stage the source data.
Remote File Name	For FTP sources, file name, or file name and path of the remote file. You can also use an input parameter to specify the remote file name.
File Reader Truncate String Null	For flat file sources, truncates string field values from the first null character. Enable when the source file contains null characters. Do not enable when you use the FileRdrTreatNullCharAs custom property. Using both properties creates conflicting settings for how Data Integration handles null characters in a flat file source, and the task fails. Default is disabled.

Note: Tracing level is not applicable for INFACore.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to a flat file:

Property	Description
Forward Rejected Rows	Causes the mapping task to forward rejected rows to the reject file. If you do not forward rejected rows, the mapping task drops rejected rows and writes them to the session log. If you enable row error handling, the mapping task writes the rejected rows and the dropped rows to the row error logs. It does not generate a reject file. If you want to write the dropped rows to the session log in addition to the row error logs, you can enable verbose data tracing.
Thousand Separator	Thousand separator character. Can be none, comma, or period. Cannot be the same as the decimal separator or the delimiter character. Field type must be Number. You might also need to update the field precision and scale. Default is None.

Property	Description
Decimal Separator	Decimal character. Can be a comma or period. Cannot be the same as the thousand separator or delimiter character. Field type must be Number. You might also need to update the field precision and scale. Default is Period.
Append if Exists	Appends the output data to the target files and reject files for each partition. You cannot use this option for FTP/SFTP target files. If you do not select this option, the mapping task truncates each target file before writing the output data to the target file. If the file does not exist, the mapping task creates it.
Create Target Directory	Creates the target directory if it doesn't exist as specified in the Output file directory field.
Header Options	Creates a header row in the file target. You can choose the following options: - No Header. Do not create a header row in the flat file target. - Output Field Names. Create a header row in the file target with the output field names. - Use header command output. Use the command in the Header Command field to generate a header row. For example, you can use a command to add the date to a header row for the file target. Default is No Header.
Header Command	Command used to generate the header row in the file target. For example, you can use a command to add the date to a header row for the file target.
Footer Command	Command used to generate the footer row in the file target.
Output Type	Type of target for the task. Select **File** to write the target data to a file target. Select **Command** to output data to a command. You cannot select **Command** for FTP/SFTP target connections.
Output File Name	File name or file name and path of the output file. By default, the mapping task names output files after the target object.
Output File Directory	Name of the output directory for a flat file target. By default, the mapping task writes output files to the target connection directory. You can also use an input parameter to specify the target file directory. If you use the service process variable directory $PMTargetFileDir, the task writes target files to the configured path for the system variable. To find the configured path of a system variable, see the pmrdtm.cfg file located at the following directory: `<Secure Agent installation directory>\apps\Data_Integration_Server\<Data Integration Server version>\ICS\main\bin\rdtm` You can also find the configured path for the $PMTargetFileDir variable in the Data Integration Server system configuration details in Administrator.

Property	Description
Reject File Directory	Directory path to write the reject file. By default, the mapping task writes all reject files to the following service process variable directory: `$PMBadFileDir/<federated task ID>` If you specify both the directory and file name in the **Reject File Name** field, clear this field. The mapping task concatenates this field with the **Reject File Name** field when it runs the task.
Reject File Name	File name, or file name and path of the reject file. By default, the mapping task names the reject file after the target object name: <target name>.bad. The mapping task concatenates this field with the **Reject File Directory** field when it runs the task. For example, if you have `C:\reject_file\` in the **Reject File Directory** field, and enter `filename.bad` in the **Reject File Name** field, the mapping task writes rejected rows to `C:\reject_file\filename.bad`.

Note: Forward Rejected Rows property is not applicable for INFACore.

Google BigQuery

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

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Google account.

The following video shows you how to get information from your Google account:

Connection properties

The following table describes the Google BigQuery 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.
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: - `gs://<bucket name>` - `gs://<bucket name>/<folder_name>`
Connection mode	The mode that you want to use to read data from or write data to Google BigQuery. Select one of the following connection modes: - Simple. Flattens each field within the Record data type field as a separate field. - Hybrid. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery connection displays the top-level Record data type field as a single field of the String data type. - Complex. Displays all the columns in the Google BigQuery table as a single field of the String data type. Default is Simple.
Connection mode	The mode that you want to use to read data from or write data to Google BigQuery. Select one of the following connection modes: - Simple. Flattens each field within the Record data type field as a separate field. - Hybrid. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery connection displays the top-level Record data type field as a single field of the String data type. - Complex. Displays all the columns in the Google BigQuery table as a single field of the String data type. Default is Simple.
Schema Definition File Path	Storage path in Google Cloud Storage where the 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.

Property	Description
Use Legacy SQL For Custom Query	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. **Note:** Not applicable when you configure the Google BigQuery connection in hybrid or complex mode.
Dataset Name for Custom Query	When you define a custom query, you must specify a Google BigQuery dataset.
Optional Properties	Specifies whether you can configure source and target functionality through custom properties. You can select one of the following options: - None. If you do not want to configure any custom properties, select None. - Required. If you want to specify custom properties to configure the source and target functionalities. Default is None.
Provide Optional Properties	Comma-separated key-value pairs of custom properties in the Google BigQuery connection to configure certain source and target functionalities. Appears only when you select **Required** in the Optional Properties.
Schema Definition File Path	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. 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.
Use Legacy SQL For Custom Query	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. **Note:** Not applicable when you configure the Google BigQuery connection in hybrid or complex mode.
Dataset Name for Custom Query	When you define a custom query, you must specify a Google BigQuery dataset.
Region Id	The region name where the Google BigQuery dataset that you want to access resides. **Note:** You must ensure that you specify a bucket name or the bucket name and folder name in the **Storage Path** property that resides in the specified region. For more information about the regions supported by Google BigQuery, see Dataset locations.
Staging Dataset	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.
Optional Properties	Specifies whether you can configure source and target functionality through custom properties. You can select one of the following options: - None. If you do not want to configure any custom properties, select None. - Required. If you want to specify custom properties to configure the source and target functionalities. Default is None.

Property	Description
Provide Optional Properties	Comma-separated key-value pairs of custom properties in the Google BigQuery connection to configure certain source and target functionalities. Appears when you select **Required** in the Optional Properties. For more information about the list of custom properties that you can specify, see the Informatica Knowledge Base article: https://kb.informatica.com/faq/7/Pages/26/632722.aspx
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, you can configure the retry strategy when the Google BigQuery connection fails to connect to the Google BigQuery source.

The following table describes the retry properties for the Google BigQuery connection:

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 **Enable Retry** 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 **Enable Retry** 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 **Enable Retry** property.
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 **Enable Retry** 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 **Enable Retry** property.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Google BigQuery:

Property	Description
Source Dataset ID	Optional. Overrides the Google BigQuery dataset name that you specified in the Source transformation.
Source Table Name	Optional. Overrides the Google BigQuery table name that you specified in the Source transformation.
Source Staging Dataset	Optional. Overrides the Google BigQuery staging dataset name that you specified in the connection and the Source Dataset ID source advanced property.
Number of Rows to Read	Specifies the number of rows to read from the Google BigQuery source table.
Allow Large Result	Determines whether Google BigQuery V2 Connector must produce arbitrarily large result tables to query large source tables. If you select this option, you must specify a destination table to store the query results.
Query Results Table Name	Required if you select the **Allow Large Results** option. Specifies the destination table name to store the query results. If the table is not present in the dataset, Google BigQuery V2 Connector creates the destination table with the name that you specify.
Job Poll Interval in Seconds	The number of seconds after which Google BigQuery V2 Connector polls the status of the read job operation. Default is 10.
Read Mode	Specifies the read mode to read data from the Google BigQuery source. You can select one the following read modes: - Direct. In direct mode, Google BigQuery V2 Connector reads data directly from the Google BigQuery source table. **Note:** When you use hybrid and complex connection mode, you cannot use direct mode to read data from the Google BigQuery source. - Staging[1]. In staging mode, Google BigQuery V2 Connector exports data from the Google BigQuery source into Google Cloud Storage. After the export is complete, Google BigQuery V2 Connector downloads the data from Google Cloud Storage into the local stage file and then reads data from the local stage file. Default is Direct mode.
Use EXPORT DATA Statement to stage	Indicates whether to support ORDER BY clause in a custom query or SQL Override Query. This property applies to staging mode.
Number of Threads for Downloading Staging Files	Specifies the number of files that Google BigQuery V2 Connector downloads at a time to enable parallel download. This property applies to staging mode.

Property	Description
Local Stage File Directory	Specifies the directory on your local machine where Google BigQuery V2 Connector stores the Google BigQuery source data temporarily before it reads the data. This property applies to staging mode.
Staging File Name	Name of the staging file where data from the Google BigQuery source table is exported to Google Cloud Storage. This property applies to staging mode.
Data Format of the staging file	Specifies the data format of the staging file. You can select one of the following data formats: - Avro - JSON (Newline Delimited). Supports flat and record data with nested and repeated fields. - CSV. Supports flat data. **Note:** In a .csv file, columns of the Timestamp data type are represented as floating point numbers that cause the milliseconds value to differ. - Parquet This property applies to staging mode.
Enable Staging File Compression	Indicates whether to compress the size of the staging file in Google Cloud Storage before Google BigQuery V2 Connector reads data from the staging file. You can enable staging file compression to reduce cost and transfer time. This property applies to staging mode.
Persist Extract Staging File After Download	Indicates whether Google BigQuery V2 Connector must persist the staging file after it reads data from the staging file. By default, Google BigQuery V2 Connector deletes the staging file.
Persist Destination Table	Indicates whether Google BigQuery V2 Connector must persist the query results table after it reads data from the query results table. By default, Google BigQuery V2 Connector deletes the query results table.
pre SQL	SQL statement that you want to run before reading data from the source. For example, if you want to select records in the database before you read the records from the table, specify the following pre SQL statement: `SELECT * FROM [api-project-80697026669:EMPLOYEE.DEPARTMENT] LIMIT 1000;`

pre SQL Configuration	Specify a pre SQL configuration.
	For example,
	`DestinationTable:PRESQL_SRC,DestinationDataset:EMPLOYEE,`
	`FlattenResults:False,WriteDisposition:WRITE_TRUNCATE,UseLegacySql:False`

post SQL	SQL statement that you want to run after reading data from the source.
	For example, if you want to update records in a table after you read the records from a source table, specify the following post SQL statement:
	`UPDATE [api-project-80697026669.EMPLOYEE.PERSONS_TGT_DEL]`
	`SET phoneNumber.number=1000011, phoneNumber.areaCode=100 where fullname='John Doe'`

Property	Description
post SQL Configuration	Specify a post SQL configuration. For example, `DestinationTable:POSTSQL_SRC,DestinationDataset:EMPLOYEE, FlattenResults:True,WriteDisposition:WRITE_TRUNCATE,UseLegacySql:False`
SQL Override Query	Overrides the default SQL query used to read data from the Google BigQuery source. **Note:** When you specify SQL override query, you must specify a dataset name in the Source Dataset ID advanced source property. Ensure that the list of selected columns, data types, and the order of the columns that appear in the query matches the columns, data types, and order in which they appear in the source object. Ensure that you only map all the columns in the SQL override query to the target. Select the source advanced property **Use EXPORT DATA Statement to stage** to use the ORDER BY clause in a SQL Override Query in staging mode. When staging optimization is enabled in a mapping, the columns mapped in the SQL Override Query must match the columns in the source object.

Use Legacy SQL for SQL Override	Indicates that the SQL Override query is specified in legacy SQL.
	Use the following format to specify a legacy SQL query for the **SQL Override Query** property:
	`SELECT <Col1, Col2, Col3> FROM [projectID:datasetID.tableName]`
	Clear this option to define a standard SQL override query.
	Use the following format to specify a standard SQL query for the **SQL Override Query** property:
	`SELECT * FROM `projectID.datasetID.tableName``

Retry Options	Comma-separated list to specify the following retry options: - Retry Count. The number of retry attempts to read data from Google BigQuery. - Retry Interval. The time in seconds to wait between each retry attempt. - Retry Exceptions. The list of exceptions separated by pipe (|) character for which the retries are made. Use the following format to specify the retry options: For example, `RetryCount:5,RetryInterval:1,RetryExceptions:java.net.ConnectException| java.io.IOException` **Note:** The retry options are 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.
Number of Spark Partitions	Specifies the maximum number of partitions that the Spark engine splits the data into. Default is 1.
Billing Project ID	The project ID for the Google Cloud project that is linked to an active Google Cloud Billing account where the Secure Agent runs the query. If you do not specify a value for the **Billing Project ID** property, the Secure Agent runs the query in the Google Cloud project that contains the Google BigQuery objects based on the **Project ID** value specified in the Google BigQuery V2 connection.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Google BigQuery:

Property	Description
Target Dataset ID	Optional. Overrides the Google BigQuery dataset name that you specified in the connection.
UpdateMode	Determines the mode that the Secure Agent uses to update rows in the Google BigQuery target. You can select one of the following modes: - Update As Update. The Secure Agent updates all rows flagged for update if the entries exist. - Update Else Insert. The Secure Agent first updates all rows flagged for update if the entries exist in the target. If the entries do not exist, the Secure Agent inserts the entries. Default is Update as Update. Not applicable when you perform a data driven operation.
Enable Data Driven	Implements data driven operation to honor flagged rows for an insert, update, delete, or reject operation based on the data driven condition. Select this option when you select **Data Driven** as the target operation.
Enable Merge	Implements the Merge query to perform an update, upsert, delete or data driven operation on a Google BigQuery target table. If you select the **Enable Data Driven** property, you must select this option. Default is not selected.
UsUpdate Override[1] e Default Column Values	Applicable when the selected data format for the staging file is CSV when the mapping contains unconnected ports. Includes the default column values for the unconnected port from the staging file to create the target. This is applicable when you have defined the default constraint value in the Google BigQuery source column. When you do not enable this option, the agent creates a target only with the connected ports. The agent populates null or empty strings for unconnected ports.

Update Override	Optional. Overrides the update SQL statement that the Secure Agent generates to update the Google BigQuery target.
	Use the following format to define an update override query:
	`UPDATE `<project_name>.<dataset_name>.<table_name>` as <alias_name>`
	`SET <alias_name>.<col_name1>=:<temp_table>.<col_name1>, <alias_name>.<col_name2>=:<temp_table>.<col_name2> FROM <dataset_name>.:<temp_table> WHERE <conditional expression>`
	For example,
	`UPDATE `project1.custdataset.cust_table1` as ab SET ab.fld_str=:custtemp.fld_str, ab.fld_int=:custtemp.fld_int FROM custdataset.:custtemp WHERE ab.fld_string_req = :custtemp.fld_string_req`
	Not applicable when you perform a data driven operation.

Target Table Name	Optional. Overrides the Google BigQuery target table name that you specified in the Target transformation. **Note:** If you specify an update override query, Google BigQuery V2 Connector ignores this property.
Target Staging Dataset	Optional. Overrides the Google BigQuery staging dataset name that you specified in the connection and the Target Dataset ID target advanced property.

Property	Description
Create Disposition	Specifies whether Google BigQuery V2 Connector must create the target table if it does not exist. You can select one of the following values: - Create if needed. If the table does not exist, Google BigQuery V2 Connector creates the table. - Create never. If the table does not exist, Google BigQuery V2 Connector does not create the table and displays an error message. Create disposition is applicable only when you perform an insert operation on a Google BigQuery target.
Write Disposition	Specifies how Google BigQuery V2 Connector must write data in bulk mode if the target table already exists. You can select one of the following values: - Write append. If the target table exists, Google BigQuery V2 Connector appends the data to the existing data in the table. - Write truncate. If the target table exists, Google BigQuery V2 Connector overwrites the existing data in the table. - Write empty. If the target table exists and contains data, Google BigQuery V2 Connector displays an error and does not write the data to the target. Google BigQuery V2 Connector writes the data to the target only if the target table does not contain any data. Write disposition is applicable for bulk mode. Write disposition is applicable only when you perform an insert operation on a Google BigQuery target.
Write Mode	Specifies the mode to write data to the Google BigQuery target. You can select one of the following modes: - Bulk. Google BigQuery V2 Connector first writes the data to a staging file in Google Cloud Storage. When the staging file contains all the data, Google BigQuery V2 Connector loads the data from the staging file to the BigQuery target. Google BigQuery V2 Connector then deletes the staging file unless you configure the task to persist the staging file. - Streaming[1]. Google BigQuery V2 Connector directly writes data to the BigQuery target. Google BigQuery V2 Connector writes the data into the target row by row. - CDC[1]. Applies only when you capture changed data from a CDC source. In CDC mode, Google BigQuery V2 Connector captures changed data from any CDC source and writes the changed data to a Google BigQuery target table. Default is Bulk mode. Streaming mode is not applicable when you perform a data driven operation.
Streaming Template Table Suffix	Specify the suffix to add to the individual target tables that Google BigQuery V2 Connector creates based on the template target table. This property applies to streaming mode. If you select the Enable Merge option, Google BigQuery V2 Connector ignores this property. Streaming mode is not applicable when you perform a data driven operation.
Rows per Streaming Request	Specifies the number of rows that Google BigQuery V2 Connector streams to the BigQuery target for each request. Default is 500 rows. The maximum row size that Google BigQuery V2 Connector can stream to the Google BigQuery target for each request is 10 MB. This property applies to streaming mode. Streaming mode is not applicable when you perform a data driven operation.
Staging file name	Name of the staging file that Google BigQuery V2 Connector creates in the Google Cloud Storage before it loads the data to the Google BigQuery target. This property applies to bulk mode.

Property	Description
Data Format of the staging file	Specifies the data format of the staging file. You can select one of the following data formats: - Avro - JSON (Newline Delimited). Supports flat and record data with nested and repeated fields. - Parquet - CSV. Supports flat data. **Note:** In a .csv file, columns of the Timestamp data type are represented as floating point numbers that cause the milliseconds value to differ. This property applies to bulk and CDC mode. Avro and parquet format is not applicable when you perform a data driven operation.
Persist Staging File After Loading	Indicates whether Google BigQuery V2 Connector must persist the staging file in the Google Cloud Storage after it writes the data to the Google BigQuery target. You can persist the staging file if you want to archive the data for future reference. By default, Google BigQuery V2 Connector deletes the staging file in Google Cloud Storage. This property applies to bulk mode.
Enable Staging File Compression	Select this option to compress the size of the staging file before Google BigQuery writes the data to the Google Cloud Storage and decompress the staging file before it loads the data to the Google BigQuery target. You can enable staging file compression to reduce cost and transfer time.
Job Poll Interval in Seconds	The number of seconds after which Google BigQuery V2 Connector polls the status of the write job operation. Default is 10.
Number of Threads for Uploading Staging file	The number of files that Google BigQuery V2 Connector must create to upload the staging file in bulk mode.
Local Stage File Directory	Specifies the directory on your local machine where Google BigQuery V2 Connector stores the files temporarily before writing the data to the staging file in Google Cloud Storage. This property applies to bulk mode.
Allow Quoted Newlines	Indicates whether Google BigQuery V2 Connector must allow the quoted data sections with newline character in a .csv file.
Field Delimiter	Indicates whether Google BigQuery V2 Connector must allow field separators for the fields in a .csv file.
Quote Character	Specifies the quote character to skip when you write data to Google BigQuery. When you write data to Google BigQuery and the source table contains the specified quote character, the task fails. Change the quote character value to a value that does not exist in the source table. Default is double quotes.
Allow Jagged Rows	Indicates whether Google BigQuery V2 Connector must accept the rows without trailing columns in a .csv file.
Pre SQL	SQL statement that you want to run before writing data to the target. For example, if you want to select records from the database before you write the records into the table, specify the following pre-SQL statement: `SELECT * FROM 'api-project-80697026669.EMPLOYEE.RegionNation' LIMIT 1000`

Property	Description
Pre SQL Configuration	Specify a pre-SQL configuration. For example, `DestinationTable:PRESQL_TGT2,DestinationDataset:EMPLOYEE, FlattenResults:False,WriteDisposition:WRITE_TRUNCATE,UseLegacySql:False`
Post SQL	SQL statement that you want to run after writing the data into the target. For example, if you want to update records in a table after you write the records into the target table, specify the following post-SQL statement: `UPDATE [api-project-80697026669.EMPLOYEE.PERSONS_TGT_DEL] SET phoneNumber.number =1000011, phoneNumber.areaCode=100 where fullname='John Doe'`
Suppress post SQL on Error	Indicates whether the Secure Agent must abort the post-SQL query execution in case the task fails to write data to the Google BigQuery target table due to errors. Default is not selected.

Post SQL Configuration	Specify a post-SQL configuration.
	For example,
	`DestinationTable:POSTSQL_SRC,DestinationDataset:EMPLOYEE,`
	`FlattenResults:True,UseLegacySQL:False`

Truncate target table	Truncates the Google BigQuery target table before loading data to the target. Default is not selected.
Allow Duplicate Inserts	Applicable when the selected data format for the staging file is CSV when the mapping contains both connected and unconnected ports. Includes the values from the connected ports and considers the default column values from the unconnected ports from the staging file while loading to the target. If the ports are unconnected, the agent considers the default value only if you have defined the default constraint value in the Google BigQuery target table. When you do not enable the **Use Default Column Values** option, the agent populates the target with values from the connected ports. This property doesn't apply when you create a new target at runtime. Also, when the selected write disposition selected is **Write Truncate**, the agent removes the field from the target table that is not part of the schema and removes the default constraint for the target column.
Disable Duplicate Update Rows	Determines if multiple incoming rows attempt to update the same target row, the Secure Agent must process only one of the incoming rows and ignore the rest of the incoming rows. Select this option to configure the mapping to process only one of the incoming rows and ignore the rest of the incoming rows. Default is not selected.
Forward Rejected Rows	Applicable only when you configure DD_REJECT constant in the data driven condition to reject all the rows. Otherwise, this property is not applicable for Google BigQuery V2 Connector.
Billing Project ID	The project ID for the Google Cloud project that is linked to an active Google Cloud Billing account where the Secure Agent runs the query. If you do not specify a value for the **Billing Project ID** property, the Secure Agent runs the query in the Google Cloud project that contains the Google BigQuery objects based on the **Project ID** value specified in the Google BigQuery V2 connection.

Google Cloud Storage

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

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Google account.

The following video shows you how to get information from your Google account:

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.
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	Specifies whether a file is encrypted. Select this option when you import an encrypted file from Google Cloud Storage. Default is unselected.

Property	Description
Bucket Name	The Google Cloud Storage bucket name that you want to connect to. When you select a data source, the Package Explorer lists files and folder available in the specified Google Cloud Storage bucket. If you do not specify a bucket name, you can select a bucket from the Package Explorer to select a source.
Optimize Object Metadata Import	Optimizes the import of metadata for the selected object without parsing other objects, folders, or sub-folders available in the bucket. 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. Default is not selected.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Google Cloud Storage:

Property	Description
Google Cloud Storage Path	Optional. Overrides the bucket name or folder path of the Google Cloud Storage file that you selected in the Google Cloud Storage source object. Use the following format: `gs://<bucket name>` or `gs://<bucket name>/<folder name>` **Note:** You cannot specify wildcard characters in the Google Cloud Storage path.
Source File Name	Optional. Overrides the Google Cloud Storage source file name that you specified in the Source transformation. **Note:** Does not apply when you configure **Is Directory** option to read multiple files from a directory.
Is Directory	Select this property to read all the files available in the folder specified in the **Google Cloud Storage Path** property. **Note:** If you do not provide the **Google Cloud Storage Path** value during run time, the Secure Agent considers the value of the **Google Cloud Storage Path** that you specify when you select a Google Cloud Storage source file in the Source transformation.
Incremental File Load	Indicates whether you want to incrementally load files when you use a directory as the source for mappings in advanced mode. When you incrementally load files, the mapping task reads and processes only files in the directory that have changed since the mapping task last ran.
Allow Wildcard Characters	Indicates whether you want to use wildcard characters for the directory sources. If you select this option, you can use the question mark (?) and asterisk (*) wildcard characters in the folder path or file name.

Property	Description
Encryption Type	Method to decrypt data. You can select one of the following encryption types: - Informatica Encryption - None Default is **None**.
Compression Format	Method to read compressed data from Google Cloud Storage. You can read the compressed data in the following formats: - None - Gzip Select **None** to read from the compressed Avro or Parquet file. Select **Gzip** to read from the compressed Flat file. Default is **None**.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Google Cloud Storage:

Property	Description
Google Cloud Storage Path	Overrides the Google Cloud Storage path where the target file exists. Use the following format: `gs://<bucket name>` or `gs://<bucket name>/<folder name>`
Target File Name	Optional. Overrides the Google Cloud Storage target object name specified in the Target transformation.
Encryption Type	Method to encrypt data. You can select one of the following encryption types: - Informatica Encryption - None Default is **None**.
Compression Format	Compresses data when you write to Google Cloud Storage. You can compress the data in the following formats: - None - Gzip - Deflate - Snappy Default is **None**. In advanced mode, you can compress data only when you run a mapping that writes data to a Google Cloud Storage file in Parquet, JSON, or Delimited file formats.

Hadoop Files

You can use Hadoop Files V2 Connector to securely read data from and write data to complex files on local system or to HDFS (Hadoop Distributed File System). You can read or write structured, semi-structured, and unstructured data.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Hadoop Files 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.
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.

NameNode URI	The URI to access HDFS.
	Use the following format to specify the name node URI in Cloudera, Amazon EMR, and Hortonworks distributions:
	`hdfs://<namenode>:<port>/`
	Where
	- `<namenode>` is the host name or IP address of the name node.
	- `<port>` is the port that the name node listens for remote procedure calls (RPC).
	If the Hadoop cluster is configured for high availability, you must copy the `fs.defaultFS` value in the `core-site.xml` file and append `/` to specify the name node URI.
	For example, the following snippet shows the `fs.defaultFS` value in a sample `core-site.xml` file:
	`<property>`
	`<name>fs.defaultFS</name>`
	`<value>hdfs://nameservice1</value>`
	`<source>core-site.xml</source>`
	`</property>`
	In the above snippet, the `fs.defaultFS` value is
	`hdfs://nameservice1`
	and the corresponding name node URI is
	`hdfs://nameservice1/`
	Note: 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.

Connection property	Description
Local Path	A local file system path to read and write data. Read the following conditions to specify the local path: - You must enter **NA** in local path if you specify the name node URI. If the local path does not contain **NA**, the name node URI does not work. - 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. - If you leave the local path blank, the agent configures the root directory (/) in the connection. The connection uses the local path to run all tasks. - If the file or directory is in the local system, enter the fully qualified path of the file or directory. For example, `/user/testdir` specifies the location of a directory in the local system. Default value for Local Path is NA.
Configuration Files Path	The directory that contains the Hadoop configuration files. **Note:** Copy the core-site.xml, hdfs-site.xml, and hive-site.xmlfrom the Hadoop cluster and add them to a folder in Linux Box.
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 jobs in a Hadoop cluster that uses Kerberos authentication or connect to sources and targets that use Kerberos authentication. To enable different users to run jobs or connect to big data sources and targets, you must configure user impersonation.

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

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from the endpoint:

Advanced Property	Description
File path	Mandatory. Location of the file or directory from which you want to read data. Maximum length is 255 characters. If the path is a directory, all the files in the directory must have the same file format. If the file or directory is in HDFS, enter the path without the node URI. For example, /user/lib/testdir specifies the location of a directory in HDFS. The path must not contain more than 512 characters. If the file or directory is in the local system, enter the fully qualified path. For example, /user/testdir specifies the location of a directory in the local system.
File Pattern	Mandatory. Name and format of the file from which you want to read data. Specify the value in the following format: `<filename>.<format>` For example, `customer.avro`

Advanced Property	Description
Allow Wildcard Characters	Indicates whether you want to use wildcard characters for the source directory name or the source file name. If you select this option, you can use asterisk (*) wildcard character for the source directory name or the source file name in the **File path** field.
Allow Recursive Read	Indicates whether you want to use wildcard characters to read complex files of the Parquet, Avro, or JSON formats recursively from the specified folder and its subfolders and files. You can use the wildcard character as part of the file or directory. For example, you can use a wildcard character to recursively read data from the following folders: - **/myfolder*/**. Returns all files within any folder or subfolder that has a pattern myfolder in the path name. - **/myfolder*/*.csv**. Returns all .csv files within any folder or subfolder that has a pattern myfolder in the path name. - **/myfolder*/ and file name is abc***. Returns all files that have a pattern abc within any folder or subfolder that has a pattern myfolder in the path name.
File Format	Specifies a file format of a complex file source. Select one of the following options: - Binary - Custom Input - Sequence File Format Default is Binary.
Input Format	The class name for files of the input file format. If you select input file format in the **File Format** field, you must specify the fully qualified class name implementing the `InputFormat` interface. To read files that use the Avro format, use the following input format: `com.informatica.avro.AvroToXML`
Input Format Parameters	Parameters for the input format class. Enter name-value pairs separated with a semicolon. Enclose the parameter name and value within double quotes. For example, use the following syntax: `"param1"="value1";"param2"="value2"`
Compression Format	Compression format of the source files. Select one of the following options: - None - Auto - DEFLATE - gzip - bzip2 - Lzo - Snappy - Custom
Custom Compression Codec	Required if you use custom compression format. Specify the fully qualified class name implementing the `CompressionCodec` interface.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to the endpoint:

Advanced Property	Description
File Directory	Optional. The directory location of one or more output files. Maximum length is 255 characters. If you do not specify a directory location, the output files are created at the location specified in the connection. If the directory is in HDFS, enter the path without the node URI. For example, /user/lib/testdir specifies the location of a directory in HDFS. The path must not contain more than 512 characters. If the file or directory is in the local system, enter the fully qualified path. For example, /user/testdir specifies the location of a directory in the local system.
File Name	Optional. Renames the output file. The file name is not applicable when you read or write multiple Hadoop Files V2s.
Overwrite Target	Indicates whether the Secure Agent must first delete the target data before writing data. If you select the **Overwrite Target** option, the Secure Agent deletes the target data before writing data. If you do not select this option, the Secure Agent creates a new file in the target and writes the data to the file.
File Format	Specifies a file format of a complex file source. Select one of the following options: - Binary - Custom Input - Sequence File Format Default is Binary.
Output Format	The class name for files of the output format. If you select Output Format in the **File Format** field, you must specify the fully qualified class name implementing the `OutputFormat` interface.
Output Key Class	The class name for the output key. If you select Output Format in the **File Format** field, you must specify the fully qualified class name for the output key. You can specify one of the following output key classes: - BytesWritable - Text - LongWritable - IntWritable **Note:** Hadoop Files V2 generates the key in ascending order.
Output Value Class	The class name for the output value. If you select Output Format in the **File Format** field, you must specify the fully qualified class name for the output value. You can use any custom writable class that Hadoop supports. Determine the output value class based on the type of data that you want to write. **Note:** When you use custom output formats, the value part of the data that is streamed to the complex file data object write operation must be in a serialized form.
Compression Format	Compression format of the source files. Select one of the following options: - None - Auto - DEFLATE - gzip - bzip2 - LZO - Snappy - Custom

Advanced Property	Description
Custom Compression Codec	Required if you use custom compression format. Specify the fully qualified class name implementing the `CompressionCodec` interface.
Sequence File Compression Type	Optional. The compression format for sequence files. Select one of the following options: - None - Record - Block

Hive

You can create a Hive connection to read from and write to Hive tables.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Hive 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.
Authentication Type	You can select one of the following authentication types: - Kerberos. Select **Kerberos** for a Kerberos cluster. - LDAP. Select **LDAP** for an LDAP-enabled cluster. - None. Select **None** for a Hadoop cluster that is not secure or not LDAP-enabled.

Connection property	Description
JDBC URL *	The JDBC URL to connect to Hive. Specify the following format based on your requirement: - To view and import tables from a single database, use the following format: `jdbc:hive2://<host>:<port>/<database name>` - To view and import tables from multiple databases, do not enter the database name. Use the following JDBC URL format: `jdbc:hive2://<host>:<port>/` **Note:** After the port number, enter a slash. - To access Hive on a Hadoop cluster enabled for TLS, specify the details in the JDBC URL in the following format: `jdbc:hive2://<host>:<port>/<database name>;ssl=true;sslTrustStore=<TrustStore_path>;trustStorePassword=<TrustStore_password>`, where the truststore path is the directory path of the truststore file that contains the TLS certificate on the agent machine.
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 jobs on a Hadoop cluster. You can configure user impersonation to enable different users to run jobs 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.
Configuration Files Path *	The directory that contains the Hadoop configuration files for the client. Copy the following site.xml files from the Hadoop cluster and add them to a folder in the Linux box: core-site.xml, hdfs-site.xml, and hive-site.xml Specify the path in this field before you use the connection to access Hive on a Hadoop cluster:
DFS URI *	The URI to access the Distributed File System (DFS), such as Amazon S3, Microsoft Azure Data Lake Storage, and HDFS. Based on the DFS you want to access, specify the required storage and bucket name. For example, for HDFS, refer to the value of the **fs.defaultFS** property in the **core-site.xml** file of the Hadoop cluster and enter the same value in the **DFS URI** field.
DFS Staging Directory	The staging directory in the Hadoop cluster where the Secure Agent stages the data. You must have full permissions for the DFS staging directory. Specify a transparent encrypted folder as the staging directory.
Hive Staging Database	The Hive database where external or temporary tables are created. You must have full permissions for the Hive staging database.

Connection property	Description

Additional Properties	The additional properties required to access the DFS.
	Configure the property as follows:
	<DFS property name>=<value>;<DFS property name>=<value>
	For example:
	To access the Amazon S3 file system, specify the access key, secret key, and the Amazon S3 property name, each separated by a semicolon:
	`fs.s3a.<bucket_name>.access.key=<access key value>;`
	`fs.s3a.<bucket_name>.secret.key=<secret key value>;`
	`fs.s3a.impl=org.apache.hadoop.fs.s3a.S3AFileSystem;`
	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:
	`fs.azure.account.auth.type=<Authentication type>;`
	`fs.azure.account.oauth.provider.type=<Authentication_provider>;`
	`fs.azure.account.oauth2.client.id=<Client_ID>;`
	`fs.azure.account.oauth2.client.secret=<Client-secret>;`
	`fs.azure.account.oauth2.client.endpoint=<ADLS Gen2 endpoint>`

* These fields are mandatory parameters.	

JD Edwards EnterpriseOne

You can use a JD Edwards EnterpriseOne connection to connect to the JD Edwards EnterpriseOne Enterprise server.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the JD Edwards EnterpriseOne 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.
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	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: - DataDirect JDBC driver class name for Oracle: `com.informatica.jdbc.oracle.OracleDriver` - DataDirect JDBC driver class name for IBM DB2: `com.informatica.jdbc.db2.DB2Driver` - DataDirect JDBC driver class name for Microsoft SQL Server: `com.informatica.jdbc.sqlserver.SQLServerDriver` For more information about which driver class to use with specific databases, see the vendor documentation.
Connection String	The connection string to connect to the database. Required to write data in bulk with the interface table write option. The JDBC connection string uses the following syntax: - For Oracle: `jdbc:informatica:oracle://<host name>:<port>,ServiceName=<db service name>` - For DB2: `jdbc:informatica:db2://<host name>:<port>;databaseName=<db name>` - For Microsoft SQL: `jdbc:informatica:sqlserver://<host name>:<port>;databaseName=<db name>`
JDE Product Code	The product code for the tables and views in JD Edwards EnterpriseOne. **Note:** You must specify only the product code without the description. If you specify a schema that is not valid, a java exception appears.

JDBC

Create a JDBC connection to connect to databases that support the JDBC Type 4 driver.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

Configure the connection properties to connect to databases compliant with the JDBC Type 4 driver.

Before you configure the connection properties, you'll need to get information from the database that you want to connect to.

The following table describes the JDBC 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.
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. 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: `jdbc:<subprotocol>:<subname>` For more information about the connection string to use with specific drivers, see the corresponding third-party vendor documentation.
Additional Security Properties	Masks sensitive and confidential data of the connection string that you don't want to display in the session log. Specify the part of the connection string that you want to mask. When you create a connection, the string you enter in this field appends to the string that you specified in the **Connection String** field.
Database Type	The database type to which you want to connect to that supports the Type 4 JDBC driver Select the **Others** option to connect to an Oracle database. PostgreSQL and Azure SQL Database options are not applicable.

Property	Description
Enable Auto Commit	Specifies whether the driver supports connections to automatically commit data to the database when you run an SQL statement. When disabled, the driver does not support connections to automatically commit data even if the auto-commit mode is enabled in the JDBC driver. Default is disabled.
Support Mixed-Case Identifiers	Indicates whether the database supports case-sensitive identifiers. When enabled, the Secure Agent encloses all identifiers within the character selected for the SQL Identifier Character property. Default is disabled.
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select **None** if the database uses regular identifiers. When the Secure Agent generates SQL queries, it does not place delimited characters around any identifiers. Select a character if the database uses delimited identifiers. When the Secure Agent generates SQL queries, it encloses delimited identifiers within this character.

Read properties

The following table describes the advanced source properties that you can configure in the Python code for the read operation:

Advanced Source Property	Description
Pre SQL	The SQL query that the Secure Agent runs before reading data from the source.
Post SQL	The SQL query that the Secure Agent runs after reading data from the source.
Fetch Size	The number of rows that the Secure Agent fetches from the database in a single call.
Table Name	Overrides the table name used in the metadata import with the table name that you specify.
Schema Name	Overrides the schema name of the source object. If you specify the schema name both in the connection and the source properties, the Secure Agent uses the schema name specified in the source properties.
SQL Override	The SQL statement to override the default query and the object name that is used to read data from the JDBC V2 source.

Write properties

The following table describes the advanced target properties that you can configure in the Python code for the write operation:

Advanced Target Property	Description
Pre SQL	The SQL statement to run before writing data to the target.
Post SQL	The SQL statement to run after writing data to the target.
Truncate Target	Truncates the target table before inserting records to the target.
Reject Truncated/ Overflow Rows	Writes truncated and overflow data to the reject file. If you select Reject Truncated/Overflow Rows, the Data Integration Service sends all truncated rows and any overflow rows to the reject file.
Table Name	Overrides the table name used in the metadata import with the table name that you specify.
Schema Name	Overrides the schema name of the target object. If you specify the schema name both in the connection and the target properties, the Secure Agent considers the schema name specified in the target properties.
Update Mode	Determines the mode how the Secure Agent writes data to the target. Select one of the following modes: - Update As Update. Updates all rows flagged for update if the entries exist. - Update Else Insert. Updates all rows flagged for update if the entries exist in the target. If the entries do not exist, the agent then inserts the entries.

JIRA

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

Before you configure the connection properties, you'll need to get information from your Jira account.

The following video shows you how to get information from your Jira account:

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.
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 KB 576517.
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.

Kafka

Create an Kafka connection to read from or write to Kafka.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Kafka 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: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
Kafka Broker List	Comma-separated list of the Kafka brokers. To list a Kafka broker, use the following format: <*HostName*>:<*PortNumber*> **Note:** 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.
Retry Timeout	Optional. Number of seconds after which the Secure Agent attempts to reconnect to the Kafka broker to read or write data. Default is 180 seconds.
Kafka Broker Version	Kafka message broker version. The only valid value is Apache 0.10.1.1 and above.
Additional Connection Properties	Optional. Comma-separated list of additional configuration properties of the Kafka producer or consumer.
Schema Registry URL	Location and port of the Confluent schema registry service to access Avro sources and targets in Kafka. To list a schema registry URL, use the following format: <https>://<*HostName or IP*>:<*PortNumber*> or <http>://<*HostName or IP*>:<*PortNumber*> Example for the schema registry URL: https://kafkarnd.informatica.com:8082 or http://10.65.146.181:8084 Applies only when you import a Kafka topic in Avro format that uses the Confluent schema registry to store the metadata.
SSL Mode	Required. Determines the encryption type to use for the connection. You can choose a mode from the following SSL modes: - Disabled. Establishes an unencrypted connection to the Kafka broker. - One-way. Establishes an encrypted connection to the Kafka broker using truststore file and truststore password. - Two-way. Establishes an encrypted connection to the Kafka broker using truststore file, truststore password, keystore file, and keystore password.
SSL TrustStore File Path	Required when you use the one-way or two-way SSL mode. Absolute path and file name of the SSL truststore file that contains the SSL certificate to connect to the Kafka broker.

Property	Description
SSL TrustStore Password	Required when you use the one-way or two-way SSL mode. Password for the SSL truststore.
SSL KeyStore File Path	Required when you use the two-way SSL mode. Absolute path and file name of the SSL keystore file that contains private keys and certificates to connect to the Kafka broker.
SSL KeyStore Password	Required when you use the two-way SSL mode. Password for the SSL keystore.
Additional Security Properties	Optional. Comma-separated list of additional configuration properties to connect to the Kafka broker in a secure way. If you specify two different values for the same property in **Additional Connection Properties** and **Additional Security Properties**, the value in **Additional Security Properties** overrides the value in **Additional Connection Properties**.

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
Additional Security Properties Schema Registry	Optional. Comma-separated list of additional security properties to connect to the Confluent schema registry in a secure way. For example, when you configure basic authentication to establish a secure communication with Confluent schema registry, specify the following value: `basic.auth.credentials.source=USER_INFO,basic.auth.user.info=<username>:<password>` If you specify two different values for the same property in **Additional Connection Properties** and **Additional Security Properties Schema Registry**, the value in **Additional Security Properties Schema Registry** overrides the value in **Additional Connection Properties**.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Kafka:

Property	Description
Topic Pattern	A regular expression pattern for the topic name that you want to read from. Use the regular expression syntax guidelines to specify the pattern.
Start position offset	The position of the Kafka consumer from where the Kafka Connector starts reading Kafka messages from a Kafka topic. You can select one of the following options: - Custom. Read messages from a specific time. - Earliest. Read all the messages available on the Kafka topic from the beginning. - Latest[1]. Read messages received by the Kafka topic after the mapping has been deployed.
Connector Mode	Specifies the mode to read data from the Kafka source. You can select one of the following modes: - Batch. The Secure Agent reads the messages available in a Kafka topic based on the position offset you specify. After the Secure Agent reads the data, the mapping terminates. When you configure a mapping for recovery, the Secure Agent reads data from the last checkpoint and stops reading data till the offset when the mapping recovery started. - Streaming. The Secure Agent reads the messages available in a Kafka topic in real-time. The Secure Agent continues to read messages from the Kafka topic and does not terminate the mapping. You must manually terminate the mapping task.
Custom Start Position Timestamp	The time in GMT from when the Kafka Connector starts reading Kafka messages from a Kafka topic. Specify the time in the following format: `yyyy-mm-dd hh:mm:ss[.fff]` The milliseconds are optional. This property is applicable only when you select **Custom** as the Start position offset.
Consumer Configuration Properties	The configuration properties for the Kafka consumer. Overrides the **Additional Connection Properties** or **Additional Security Properties** specified in the Kafka connection. For more information about Kafka consumer configuration properties, see Kafka documentation.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Kafka:

Property	Description
Metadata Fetch Timeout in milliseconds	The time after which the metadata is not fetched. Default value is 10000.
Batch Flush Time in milliseconds	The interval after which the data is published to the target. Default value is 1000.

Property	Description
Batch Flush Size in bytes	The batch size of the events after which the Secure Agent writes data to the target. Default value is 16384.
Producer Configuration Properties	The configuration properties for the producer. Overrides the **Additional Connection Properties** or **Additional Security Properties** specified in the Kafka connection. For more information about Kafka producer configuration properties, see Kafka documentation.

LDAP

Create an LDAP connection to read from or write to LDAP.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the LDAP 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.

Host Name	Required. LDAP directory server host name.
	You can use the LDAP or LDAPS protocol to connect to LDAP Server.
	- To use the LDAP protocol, use one of the following formats:
	  - `ldap://<hostname>`
	  - `<hostname>`
	- To use the LDAPS protocol, use the `ldaps://<hostname>` format.
	Note: 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. **Note:** You cannot establish an anonymous connection with Active Directory.

Property	Description
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: `dc=informatica-connector,dc=com` If you do not specify the base DN, the Secure Agent fails to fetch the metadata.

Marketo

Create a Marketo connection to read from or write to Marketo.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Adobe Marketo account.

The following video shows you how to get information from your Adobe Marketo account:

Connection properties

The following table describes the Marketo 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.
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.
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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Marketo:

Property	Description
Lead - Filter Field	The field name to use for filtering leads that you want to read from Marketo. Enter only one field. ID and email are common filter values. Ensure that the data in the field that you specify does not contain null values.
Lead - Filter Values CSV File	The location of the CSV file where the filter values are present when you specify a **Filter Field** value.
Lead - Filter Values	The filter values based on which you can filter the lead data when you specify a **Filter Field** value. To get data from the lead object based on multiple filter values, specify the filter IDs for the lead object each separated by a comma.

Property	Description
Lead - List Id	The list ID for retrieving leads from a specific list. **Note:** The list ID appears on the URL when you select the list in Marketo.
Lead - Partition Name	The Lead - Partition Name property is deprecated.
Lead - Program Id	The program ID for retrieving a lead. When you specify a program ID, you get the following default fields of the lead: progressionStatus, stream, nurtureCadence, isExhausted, acquiredBy, reachedSuccess, reachedSuccessDate, and membershipDate To get multiple leads, specify multiple program IDs, each separated by a comma.
Lead - Activity Type Id	The activity type ID to get lead details based on the lead activities when you select Lead as source. To get lead details based on multiple lead activity types, enter each activity type ID separated by a comma.
Lead Activity - Activity Type Id	The activity type ID to get lead activities when you select LeadActivity as source. To get multiple lead activities, enter each activity type ID separated by a comma.
Lead Activity - List Id	The list ID for filtering the lead activity. To filter multiple lead activities, specify the list IDs separated by a comma.
Lead Activity - Lead Id	The lead ID for filtering the lead activity of a lead. To filter lead activities for multiple leads, specify the lead IDs separated by a comma.
List - List Id	The list ID for the list details that you want to get from Marketo. **Note:** The list ID appears on the URL when you select the list in Marketo. To get multiple list details, specify multiple list IDs, separated by a comma.
List - List Name	The list name to get the list from Marketo. To get multiple lists, specify multiple list names separated by a comma.
List - Program Name	The program name to get the list associated with the program. To get multiple lists, specify the associated program names separated by a comma.
Program - Program Id	The program ID to get the program from Marketo.
Program - Program Name	The program name to get the program from Marketo.

Property	Description
Program - Tag Type	The associated tag type for a program based on which you want to get the program when you specify a Tag Value for program.
Program - Tag Value	The tag value associated with a program based on which you want to get the program when you specify a Tag Type for program.
Channel - Channel Name	The channel name to get the channel from Marketo.
Email - Email Id	The ID for the email in Marketo from which you want to get email records.
Tag - Tag Name	The tag name to get the tag from Marketo.
Folder - Max Depth	The maximum number of levels to traverse in the folder hierarchy. Default is 2.
Folder - Workspace	The name of the workspace that you want to filter.
Campaign - Campaign Id	The campaign ID to get the campaign from Marketo. To get multiple campaigns, enter each campaign ID separated by a comma.
Campaign - Campaign Name	The campaign that you want to get from Marketo based on the campaign name. To get multiple campaigns, enter each campaign name separated by a comma.
Custom Obj / Oppty (Role) / Company / Sales Per - Type Filter*	The field type to use to filter custom, opportunity, opportunity role, sales person, or company objects from Marketo.
Custom Obj / Oppty (Role) / Company / Sales Per - Values Filter*	The location of the CSV file that contains the filter values to get specific custom, opportunity, opportunity role, sales person, or company object data from Marketo. Ensure that each filter value is on a separate line in the CSV file.
Custom Obj / Oppty (Role) / Company / Sales Per - Fields Filter*	The names of the custom, opportunity, opportunity role, sales person, or company object fields that you want to get. If you don't specify a filter field value, the agent uses the fields from the field mapping in the task.

Property	Description

Custom Obj / Oppty (Role) / Company / Sales Per - String Values Filter*	The filter values to get specific data from Marketo custom objects.
	When you specify the filter values, enter the column name of the custom object on which you want to apply a filter, followed by the filter string values on consecutive lines similar to the format in a CSV file:
	`Column Name`
	`filter value1`
	`filter value2`
	`filter value3`

General - Since Date Time	Gets lead and lead activity beginning with the specified date or date/time value. Use one of the following formats: - 2016-04-01T17:00:00-0800 - 2016-10-06 Ensure that you select No as the value in the Incremental Extract field.
General - Incremental Extract	Gets incremental lead activities or lead changes. Choose one of the following values: - Yes. Gets incremental lead changes or lead activity changes from the time since the last extract. Enter the variable, $LastRunTime in Since Date Time to get incremental lead activities and lead changes. - No. Doesn't get incremental lead changes or lead activity changes since the last extract. Default is No.
General - Start Date	Gets lead and lead activities beginning with the specified date value. Use one of the following formats: - YYYY-MM-DD - YYYY-MM-DDT00:00:00Z
General - End Date	Gets lead and lead activities ending with the specified date or date/time value. Use one of the following formats: - YYYY-MM-DD - YYYY-MM-DDT00:00:00Z
General - Concurrent Threads	The number of concurrent processing threads that the task spawns for a Marketo source to optimize the performance results to get lead details. Specify from 1 to 10 concurrent threads for a Marketo source to optimize the performance of the task. Default is 1.
General - Results Batch Size	The number of records that can be read in a batch. The maximum number of records is 300. Default is 300.

Property	Description
Bulk Extract - Lead/Lead Activity	Gets lead or lead activities in bulk from Marketo based on the start and end date you specify. Default is No.
*You can configure type, values, fields, and string values filters for custom objects, opportunity, opportunity role, sales person, or company. These properties are optional.	

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Marketo:

Advanced Target Property	Description
Lead - Type of API to be used	The type of Marketo API used to insert leads in the Marketo database. You can select from the following options: - Standard API. Uses the Standard API when you want to create leads in Marketo. - Bulk API. You cannot use Bulk API to insert leads in the Marketo database. Default is Standard API.
Lead - Create Duplicate	Creates a duplicate of the lead when that lead already exists in the Marketo database. The REST API either inserts or upserts data based on the operation you specify. You can choose one of the following values: - Yes. Duplicates an existing lead. - No. Does not duplicate an existing lead. Default is No.
Lead - List ID for Leads	The ID of a list for leads where you want to create the lead.
Lead - Lookup Field	Performs a lookup of the field you specify to determine whether the lead you want to add to the Marketo database is a duplicate lead.
Lead - Partition Name	The partition name where you want to insert, update, or upsert leads in Marketo. If specified, the Secure Agent verifies if the user has access to the partition. If you do not specify a partition, the API operation uses the primary partition of the list workspace.
Custom Obj / Oppty (Role) / Company / Sales Per - Dedupe Fields	The dedupeFields or idField of the custom, opportunity, opportunity role, sales person, or company object in Marketo for which you want to perform an update or delete operation. When you do not specify dedupeFields or idField for an update or delete operation, Marketo considers the dedupeFields of the corresponding custom, opportunity, opportunity role, sales person, or company object as the default. **Note:** You can specify this field value only to update or delete data in custom, opportunity, opportunity role, sales person, or company objects in Marketo. This field is optional.

Advanced Target Property	Description
Success File Directory	Directory for the success rows files. Specify a directory path that is available on each Secure Agent machine in the runtime environment. By default, Data Integration writes the success rows file to the following directory: `<Secure Agent installation directory>/apps/Data_Integration_Server/data/success`
Error File Directory	Directory for the error rows files. Specify a directory path that is available on each Secure Agent machine in the runtime environment. By default, Data Integration writes the error rows file to the following directory: `<Secure Agent installation directory>/apps/Data_Integration_Server/data/error`

Microsoft Azure Blob Storage

Create a Microsoft Azure Blob Storage connection to read from or write to Microsoft Azure Blob Storage.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Azure account.

The following video shows you how to get information from your Azure account:

Connection properties

The following table describes the Microsoft Azure Blob 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.
Account Name	Microsoft Azure Blob Storage account name.

Property	Description
Authentication Type	Authentication type to access the Microsoft Azure Blob Storage account. Select one of the following options: - Shared Key Authentication. Uses the account key to connect to Microsoft Azure Blob Storage. - 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.
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: - core.windows.net. Connects to Azure endpoints. - core.usgovcloudapi.net. Connects to Azure Government endpoints. - core.chinacloudapi.cn. Not applicable. Default is core.windows.net.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Microsoft Azure Blob Storage:

Property	Description
Number of concurrent connections to Blob Store	The number of concurrent connections to Blob Store to upload files. Default is 4.
Source Type	Select the type of source from which you want to read data. You can select the following source types: - File - Directory Default is File.
Blob Name Override	Overrides the default file name.

Property	Description
Blob Container Override	Overrides the default container name. When you read data from a directory and override the Blob container, ensure that files in the Blob container that you override with are not empty. When you generate the SAS token at the container-level, the default container name and the container name that you specify for the container override must be the same.
Compression Format	Decompresses data when you read data from Microsoft Azure Blob Storage. You can decompress the data in the following formats: - None. Select None to decompress deflate and snappy file formats. - Gzip - Bzip2 - Lzo Default is None.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Microsoft Azure Blob Storage:

Property	Description
Number of concurrent connections to Blob Store	The number of concurrent connections to Blob Store to upload files. Default is 4.
Source Type	Select the type of source from which you want to read data. You can select the following source types: - File - Directory Default is File.
Blob Name Override	Overrides the default file name.
Blob Container Override	Overrides the default container name. When you read data from a directory and override the Blob container, ensure that files in the Blob container that you override with are not empty. When you generate the SAS token at the container-level, the default container name and the container name that you specify for the container override must be the same.
Compression Format	Decompresses data when you read data from Microsoft Azure Blob Storage. You can decompress the data in the following formats: - None. Select None to decompress deflate and snappy file formats. - Gzip - Bzip2 - Lzo Default is None.

Microsoft Azure Cosmos DB

Create a Microsoft Azure Cosmos DB connection to read from or write to Microsoft Azure Cosmos DB SQL API.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Azure account.

The following video shows you how to get information from your Azure account:

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.
Cosmos DB URI	The URI of Microsoft Azure Cosmos DB account.
Key	The primary or secondary key that provides you 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 SQL Data Warehouse

Create a Microsoft Azure SQL Data Warehouse V2 connection to read from or write to Microsoft Azure SQL Data Warehouse.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Azure Synapse account.

The following video shows you how to get information from your Azure Synapse account:

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.

Azure DW JDBC URL	The Microsoft Azure Synapse SQL JDBC connection string.
	Enter the connection string in the following format for Microsoft SQL Server authentication:
	`jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>`
	Enter the connection string in the following format for Azure Active Directory (AAD) authentication:
	`jdbc:sqlserver://<Server>.database.windows.net:1433; database=<Database>;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;`
	Default is Microsoft SQL Server authentication.

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.

Property	Description
Azure DW Schema Name	Name of the schema in Microsoft Azure Synapse SQL.
Azure Storage Type	Type of Azure storage to stage the files. Select one of the following storage types: - Azure Blob. Uses Microsoft Azure Blob Storage to stage the files. - ADLS Gen2. Uses Microsoft Azure Data Lake Storage Gen2 to stage the files. Default is Azure Blob.
Authentication Type	Authentication type to connect to Azure storage to stage the files. Select one of the following options: - Shared Key Authentication. Uses the account name and account key to connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2. - 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. - 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.
Azure Blob Account Name	Applies to Shared Key Authentication for Microsoft Azure Blob Storage. Name of the Microsoft Azure Blob Storage account to stage the files.
Azure Blob Account Key	Applies to Shared Key Authentication for Microsoft Azure Blob Storage. The Microsoft Azure Blob Storage access key to stage the files.
Container Name	Applies to Microsoft Azure Blob Storage. The name of the container in the Azure Blob Storage account.
ADLS Gen2 Storage Account Name	Applies to Shared Key Authentication and Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2. Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
ADLS Gen2 Account Key	Applies to Shared Key Authentication for Microsoft Azure Data Lake Storage Gen2. The Microsoft Azure Data Lake Storage Gen2 access key to stage the files.
Client ID	Applies to Service Principal Authentication and Managed Identity Authentication for Microsoft Azure Data Lake Storage Gen2. The client ID of your application. To use service principal authentication, enter the application ID or client ID for your application registered in the Azure Active Directory. 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.
Client Secret	Applies to Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2. The client secret for your application.
Tenant ID	Applies to Service Principal Authentication for Microsoft Azure Data Lake Storage Gen2. The directory ID or tenant ID for your application.

Property	Description
File System Name	Applies to Microsoft Azure Data Lake Storage Gen2. The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.
Blob End-point	Type of Microsoft Azure endpoints. Select one of the following endpoints: - core.windows.net. Connects to Azure endpoints. - core.usgovcloudapi.net. Connects to US Government Microsoft Azure Synapse SQL endpoints. - core.chinacloudapi.cn. Connects to Microsoft Azure Synapse SQL endpoints in the China region. Default is core.windows.net.
VNet Rule	Enable to connect to a Microsoft Azure Synapse SQL endpoint residing in a virtual network (VNet).

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Microsoft Azure SQL Data Warehouse:

Property	Description
Azure Blob Container Name	Required if you select Azure Blob storage in the connection properties. The name of the container in Microsoft Azure Blob Storage. The container name must not contain special characters.
ADLS FileSystem Name	Required if you select ADLS Gen2 storage in the connection properties. The name of the file system in Microsoft Azure Data Lake Storage Gen2. The file system name must not contain special characters. You can also specify the path of the directory under the file system. Use only a forward slash to specify the directory path.
Schema Name Override	Overrides the schema specified in the connection.
Table Name Override	Overrides the table name of the imported source table.
Staging File Format	Type of file format to use when you stage the files. Select one of the following formats: - Delimited Text - Parquet
Field Delimiter	Character used to separate fields in the file. Default is `0x1e`. You can specify 'TAB' or 0-256 single-char printable and non-printable ASCII characters. Non-printable characters must be specified in hexadecimal. **Note:** Multi-char ASCII characters except TAB are not applicable. You cannot use the following non-printable characters: `00x0`, `0x0`, `0x0A` , `0x1B`, `0x0D`, and `0x1F`

Property	Description
Number of Concurrent Connections to Blob Store	Number of concurrent connections to extract data from the Microsoft Azure Blob Storage. When reading a large-size blob, you can spawn multiple threads to process data. Configure **Blob Part Size** to partition a large-size blob into smaller parts. Default is 4. Maximum is 10.
Blob Part Size	Partitions a blob into smaller parts each of specified part size. When reading a large-size blob, consider partitioning the blob into smaller parts and configure concurrent connections to spawn required number of threads to process data in parallel. Default is 8 MB.
Pre-SQL	Pre-SQL command that must be run before reading data from the source.
Post-SQL	Post-SQL command that must be run after reading data from the source.
SQL Override	When you read data from an object, you can configure SQL overrides and define constraints.
On Pre-Post SQL Error	Determines the behavior when a task that includes pre-SQL or post-SQL commands encounters errors. Select one of the following options: - Continue. The task continues regardless of errors. - Stop. The task stops when errors occur while executing pre-SQL or post-SQL commands.
Quote Character	Specifies the quote character to skip when you read data from Microsoft Azure Synapse SQL. The quote character that you specify must not exist in the source table. If it exists, enter a different quote character value. Default is `0x1f`.
Interim Directory	Optional. Path to the staging directory in the Secure Agent machine. Specify the staging directory where you want to stage the files when you read data. Ensure that the directory has sufficient space and you have write permissions to the directory. Default staging directory is `/tmp`. You cannot specify an interim directory when you use the Hosted Agent.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization, or verbose data. Default is normal.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Microsoft Azure SQL Data Warehouse:

Advanced Property	Description
Azure Blob Container Name	Required if you select Azure Blob storage in the connection properties. The name of the container in Microsoft Azure Blob Storage. The container name cannot contain special characters.
ADLS FileSystem Name	Required if you select ADLS Gen2 storage in the connection properties. The name of the file system in Microsoft Azure Data Lake Storage Gen2. The file system name cannot contain special characters. You can also specify the path of the directory under the file system. Use only a forward slash to specify the directory path.
Copy Method	The method to load data from the staging location to Microsoft Azure Synapse SQL. Select one of the following options: - Polybase - Copy Command Default is Polybase.
Copy Command Options	Options for the copy command in key=value format. Specify each option on a new line. For more information on copy command options, see the topic Copy Commands in the Cloud Data Integration documentation.
Schema Name Override	Overrides the schema specified in the connection.
Table Name Override	Overrides the table name of the imported Microsoft Azure Synapse SQL Data Warehouse target table.
Field Delimiter	Character used to separate fields in the file. Default is `0x1e`. You can specify 'TAB' or 0-256 single-char printable and non-printable ASCII characters. Non-printable characters must be specified in hexadecimal. **Note:** Multi-char ASCII characters except TAB are not applicable. You cannot use the following non-printable characters: `00x0`, `0x0`, `0x0A` , `0x1B`, `0x0D`, and `0x1F`
Number of Concurrent Connections to Blob Storage	Number of concurrent connections to extract data from the Microsoft Azure Blob Storage. When reading a large-size blob, you can spawn multiple threads to process data. Default is 4. Maximum is 10.
Truncate Table	Truncates the target before inserting data to the target.
Pre-SQL	Pre-SQL command that must be run before reading data from the source.
Post-SQL	Post-SQL command that must be run after writing data to the target.
On Pre-Post SQL Error	Determines the behavior when a task that includes pre-SQL or post-SQL commands encounters errors. You can select any of the following options: - Continue. The task continues regardless of errors. - Stop. The task stops when errors occur while executing pre-SQL or post-SQL commands.

Advanced Property	Description
Treat Source Rows As	Select one of the following options: - NONE - INSERT - DELETE - UPDATE - UPSERT - DATA DRIVEN. Select to honor the flagged rows from the update strategy or any other custom transformation, or a CDC source. Default is None.
Batch Size	Minimum number of rows in a batch. Enter a number greater than 0. Default is 2000000.
Reject Threshold	Number of errors within a batch that causes a batch to fail. Enter a positive integer. If the number of errors is equal to or greater than the property value, the Secure Agent rejects the entire batch to the error file and marks the session failed. **Note:** When you do not set the reject threshold, the mapping fails when an error is encountered.
Quote Character	Specifies the quote character to skip when you write data to Microsoft Azure Synapse SQL. The quote character that you specify must not exist in the source table. If it exists, enter a different quote character value.
Compression Format	Compresses the staging files in the `.Gzip` format. Default is None.
Update Override	Overrides the default update SQL statement that the Secure Agent generates.
Interim Directory	Optional. Path to the staging directory in the Secure Agent machine. Specify the staging directory where you want to stage the files when you write data to Microsoft Azure Synapse SQL. Ensure that the directory has sufficient space and you have write permissions to the directory. Default staging directory is `/tmp`. You cannot specify an interim directory when you use the Hosted Agent.

Microsoft CDM Folders

Create a Microsoft CDM Folders connection to read from or write to Microsoft CDM Folders.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Microsoft account.

The following video shows you how to get information from your Microsoft account:

Connection properties

The following table describes the Microsoft CDM Folders 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.
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

Create a Microsoft Dynamics 365 for Operations connection to read from or write to Microsoft Dynamics 365 for Operations.

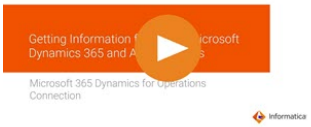
Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Microsoft Dynamics 365 and Azure Active Directory(AAD) account.

The following video shows you how to get information from your Microsoft Dynamics 365 and AAD account:



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.
Authentication Type	The authentication method that the connector must use to login to the web application. Select one of the following authentication types: - OAuth 2.0. Requires the service URL, username, password, and application ID. - OAuth 2.0 Client Secret Grant. Requires the service URL, application ID, tenant ID, and client secret. - OAuth 2.0 Client Certificate Grant. Requires the keystore file, keystore password, key alias and key password. Not applicable.

Service URL	Enter the URL of the Microsoft Dynamics 365 for Operations service in the following format:
	`https:<server name>:<port number>`
	or
	`http:<server name>:<port number>`
	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.

Property	Description
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

Create a Microsoft Dynamics 365 for Sales connection to read from or write to Microsoft Dynamics 365 for Sales.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Microsoft Dynamics 365 and Azure Active Directory(AAD) account.

The following video shows you how to get information from your Microsoft Dynamics 365 and AAD account:

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.
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: - 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. - 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. - OAuth 2.0 Client Secret Grant. Requires the application ID and client secret. Applies to Microsoft Dynamics 365 for Sales online.
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.
Keystore Password	The password for the keystore file required for secure communication.
Key Alias	The alias name for the individual key.
Key Password	The password for the individual keys in the keystore file required for secure communication.
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.

Property	Description
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, `https://sts1.<company>.com/adfs/oauth2/token`

Microsoft Excel

Create a Microsoft Excel connection to read from Microsoft Excel.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Connection properties

The following table describes the Microsoft Excel 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.
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. **Note:** You must add the `.xlsx` extension to the file name.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Microsoft Excel:

Property	Description
Row Limit	The maximum number of rows the agent processes. Default is 0. The default value indicates that there is no row limit, and the agent processes all records.

Microsoft Fabric OneLake

Create a Microsoft Fabric OneLake connection to connect to Microsoft Fabric OneLake.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Configure the connection properties to connect to Microsoft Fabric OneLake.

Before you configure the connection properties, you'll need to get information from your Microsoft Fabric OneLake account.

The following table describes the Microsoft Fabric OneLake 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.
Workspace Name	Name of the workspace in Microsoft Fabric OneLake.
Lakehouse Path	Path or name of the lakehouse present in the workspace. You can specify the path in one of the following ways: - *root directory (/)* to access all the tables and files in the workspace. - *lakehouse name* to access all tables and files present in the lakehouse. - *lakehouse name/Files* to access files present in the lakehouse. - *lakehouse name/Tables* to access tables present in the lakehouse.
Authentication Type	Authentication type to access Microsoft Fabric OneLake. Service Principal Authentication uses the client ID, client secret, and tenant ID to connect to Microsoft Fabric OneLake.
Client ID	The application ID or client ID of your application registered in the Azure Active Directory.

Property	Description
Client Secret	The client secret of your application registered in the Azure Active Directory.
Tenant ID	The ID of the Azure Active Directory instance in which you created the application.
OneLake Endpoint	The type of Microsoft Fabric OneLake endpoint that you want to connect to. Default is **fabric.microsoft.com**.

Note: Microsoft Fabric OneLake Connector is available for preview.

Preview functionality is supported for evaluation purposes but is unwarranted and is not supported in production environments or any environment that you plan to push to production. 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.

MS Access

Create a MS Access connection to read from or write to Microsoft Access.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the 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.
Data Source Name	System DSN name.
Code Page	The code page compatible with the Microsoft Access source. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode and non-Unicode data. - Shift-JIS. Select for double-byte character data. - ISO 8859-15 Latin 9 (Western European). - ISO 8859-2 Eastern European. - ISO 8859-3 Southeast European. - ISO 8859-5 Cyrillic. - ISO 8859-9 Latin 5 (Turkish). - IBM EBCDIC International Latin-1.

MySQL

Create a MySQL connection to read from or write to MySQL.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your MySQL Cloud account.

The following video shows you how to get information from your MySQL Cloud account:

Connection properties

The following table describes the MySQL 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.
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. **Note:** 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 at runtime. If you specify more than one property, separate each key-value pair with a semicolon.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from MySQL:

The following table describes the advanced source properties that you can configure for a MySQL source:

Property	Description
Pre SQL	Pre-SQL command that must be run before reading data from the source.
Post SQL	Post-SQL command that must be run after reading data from the source.
Output is Deterministic	Relational source or transformation output that does not change between session runs when the input data is consistent between runs. When you configure this property, the Secure Agent does not stage source data for recovery if transformations in the pipeline always produce repeatable data.

Property	Description
Output is repeatable	Relational source or transformation output that is in the same order between session runs when the order of the input data is consistent. When output is deterministic and output is repeatable, the Secure Agent does not stage source data for recovery.
SQL Override	The SQL statement to override the default query generated from the specified source type to read data from the MySQL Server source.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Microsoft SQL Server:

Property	Description
Forward Rejected Rows	Determines whether the transformation passes rejected rows to the next transformation or drops rejected rows. By default, the mapping task forwards rejected rows to the next transformation. If you select the Forward Rejected Rows option, the Secure Agent flags the rows for reject and writes them to the reject file. If you do not select the Forward Rejected Rows option, the Secure Agent drops the rejected rows and writes them to the session log file. The Secure Agent does not write the rejected rows to the reject file.
Pre SQL	Pre-SQL command to run against the target database before writing data to the target.
Post SQL	Post-SQL command to run against the target database after writing data to the target.
Update Override	An update SQL statement that updates the data in a MySQL target table. The update SQL statement you specify overrides the default update statements that the Secure Agent generates to update the target based on key columns. You can define an update override statement to update target tables based on both key or non-key columns. In the override statement, you must enclose all reserved words in quotation marks.
Reject file directory	The directory that stores the rejected files. Specify the directory where you want to store the rejected files.
Reject filename	Name of the rejected file that is stored in the reject file directory.
Schema Name	The schema name that overrides the schema name specified in the target connection.

OData

Create an OData connection to read from or write to OData.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your OData account.

The following video shows you how to get information from your OData account:

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.
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. **Note:** The service root URI must follow the OData URI Conventions.
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. **Note:** 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.

ODBC

Create an ODBC connection to connect to an application that is ODBC compliant.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

Configure the connection properties to connect to DB2.

Before you configure the connection properties, you'll need to get information from DB2.

The following table describes the ODBC 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.
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 source or target.

Property	Description
Code Page	The code page of the database server or flat file defined in the connection. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode data. - Shift-JIS. Select for double-byte character data. - ISO 8859-15 Latin 9 (Western European). - ISO 8859-2 Eastern European. - ISO 8859-3 Southeast European. - ISO 8859-5 Cyrillic. - ISO 8859-9 Latin 5 (Turkish). - IBM EBCDIC International Latin-1. - Japanese Extended UNIX Code (incl. JIS X 0212) - Japanese EUC (with \<-> Yen mapping) - Japanese EUC (Packed Format) - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - Japanese EBCDIC Fujitsu - HITACHI KEIS Japanese - NEC ACOS JIPSE Japanese - UNISYS Japanese - MITSUBISHI MELCOM Japanese - Japanese EBCDIC-Kana Fujitsu - HITACHI KEIS-Kana Japanese - NEC ACOS JIPSE-Kana Japanese - UNISYS-Kana Japanese - MITSUBISHI MELCOM-Kana Japanese - EBCDIC Japanese - EBCDIK Japanese - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - EBCDIC Japanese Katakana SBCS - EBCDIC Japanese Katakana (w/ euro) - EBCDIC Japanese Latin-Kanji (w/ euro) - EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399) - EBCDIC Japanese Latin (w/ euro update) - EBCDIC Japanese Katakana SBCS (w/ euro update) - MS Taiwan Big-5 w/ HKSCS extensions - MS Windows Traditional Chinese, superset of Big 5 - Taiwan Big-5 (w/ euro update) - Taiwan Big-5 (w/o euro update) - PC Chinese GBK (IBM-1386) - Chinese EUC - Simplified Chinese (GB2312-80) - Hong Kong Supplementary Character Set - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew (w/o euro update) - PC Hebrew (w/ euro update) - MS Windows Hebrew (older version) - MS Windows Hebrew (w/o euro update) - Lotus MBCS encoding for Windows Hebrew - EBCDIC Hebrew (updated with sheqel, control characters) - EBCDIC Hebrew (w/ euro) - EBCDIC Hebrew (updated w/ euro and new sheqel, control characters) - Israeli Standard 960 (7-bit Hebrew encoding)

Property	Description
ODBC Subtype	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. You can select the DB2 option to read from or write to DB2. The rest of the options are not applicable.
Driver Manager for Linux	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: - Data Direct - unixODBC2.3.0 - unixODBC2.3.4 The default driver manager is UnixODBC2.3.0.

Read properties

The following table describes the advanced source properties that you can configure in the Python code for the read operation:

Property	Description
Pre SQL	Pre-SQL command that must be run before reading data from the source.
Post SQL	Post-SQL command that must be run after reading data from the source.
SQL Override	The SQL statement to override the default query generated from the specified source type to read data from the ODBC source.

Write properties

The following table describes the advanced target properties that you can configure in the Python code for the write operation:

Property	Description
Update Override	An update SQL statement that updates the data in an ODBC target table. The update SQL statement you specify overrides the default update statements that the Secure Agent generates to update the target based on key columns. You can define an update override statement to update target tables based on both key or non-key columns. In the override statement, you must enclose all reserved words in quotation marks.

Oracle

Create an Oracle connection to read from or write to Oracle.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Amazon Web Services account.

The following video shows you how to get information from your Amazon Web Services account:

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.
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: - Oracle ADB. Connects to Oracle Autonomous Database. - Oracle On-premise. Connects to Oracle on-premises.
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.

Property	Description
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.
Encryption Method	The method that the Secure Agent uses to encrypt the data exchanged between the Secure Agent and the database server.
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption.
Validate Server Certificate	Validates the certificate that is sent by the database server. If you specify the `HostNameInCertificate` parameter, the Secure Agent also validates the host name in the certificate.
Trust Store	The location and name of the trust store file.
Trust Store Password	The password to access the contents of the trust store 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.
Key Store	The location and the file name of the key store.
Key Store Password	The password for the key store file required for secure communication.
Key Password	The password for the individual keys in the key store file required for secure communication.
Connection Retry Period	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. Used for all operations. Default is 0.

Property	Description

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.
	For example, `ConnectionRetryCount=2;`
	`ConnectionRetryDelay=20`
	To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the JDBC driver.
	For example, `EncryptionTypes=AES256;`
	`EncryptionLevel=accepted;DataIntegrityLevel=accepted;`
	`DataIntegrityTypes=SHA1`

Runtime Advanced Connection Properties	Additional properties for the ODBC driver for the runtime.
	If you specify more than one property, separate each key-value pair with a semicolon.
	For example, `charset=sjis;readtimeout=180`
	To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the ODBC driver.
	For example, `EncryptionTypes=AES256;EncryptionLevel=1;`
	`DataIntegrityLevel=1;DataIntegrityTypes=SHA1;`
	`DataIntegrityTypes=SHA1`

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Oracle:

Property	Description
Pre SQL	Pre-SQL command to run against the target database before writing data to the target.
Post SQL	Post-SQL command to run against the target database after writing data to the target.
SQL Override	The SQL statement to override the default query generated from the specified source type to read data from the Oracle source.
Schema Name	Overrides the schema name of the target object.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Oracle:

Property	Description
Forward Rejected Rows	Determines whether the transformation passes rejected rows to the next transformation or drops rejected rows. By default, the mapping task forwards rejected rows to the next transformation. If you select the Forward Rejected Rows option, the Secure Agent flags the rows for reject and writes them to the reject file. If you do not select the Forward Rejected Rows option, the Secure Agent drops the rejected rows and writes them to the session log file. The Secure Agent does not write the rejected rows to the reject file.
Pre SQL	Pre-SQL command to run against the target database before writing data to the target.
Post SQL	Post-SQL command to run against the target database after writing data to the target.
Update Override	An update SQL statement that updates the data in an Oracle target table. The update SQL statement you specify overrides the default update statements that the Secure Agent generates to update the target based on key columns. You can define an update override statement to update target tables based on both key or non-key columns. You cannot validate the update SQL statement in the SQL transformation. In the override statement, you must enclose all reserved words in quotation marks.
Reject File Directory	The directory that stores the rejected files. Specify the directory where you want to store the rejected files.
Reject File Name	Name of the rejected file that is stored in the reject file directory.
Schema Name	Overrides the schema name of the target object.

Oracle NetSuite

Create an Oracle NetSuite connection to read from or write to Oracle NetSuite.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Netsuite account.

The following video shows you how to get information from your Netsuite account:

Connection properties

The following table describes the NetSuite 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.
Username	Applicable only when you use the username and password for authentication. User name for a NetSuite account. User name is an email address.
Password	Applicable only when you use the username and password for authentication. Password for the NetSuite account.
Service URL	NetSuite WSDL URL. From version 2019_2 of the NetSuite WSDL URL, you can enter the WSDL URL used by your NetSuite account instead of the default service URL. The service URL used by the NetSuite account is in the following format: `<NetSuite account URL>/wsdl/v2019_2_0/netsuite.wsdl` The default service URL is `https://webservices.netsuite.com/wsdl/v2021_2_0/netsuite.wsdl`. Consider using the WSDL URL that is specific to your NetSuite account. For more information, see "NetSuite account-specific service URL" in the NetSuite Connector documentation in Data Integration.
Account	NetSuite account ID. To find your account ID, log in to NetSuite, and click **Setup** > **Integration** > **SOAP Web Services Preferences**.
Application ID	Optional. NetSuite application ID. If the application ID property is blank, the agent uses the Informatica application ID. To find your application ID, log in to Netsuite and click **Setup** > **Integration** > **Manage Integrations**. If you do not have an application ID, you can create one. On the **Manage Integrations** page, click **New**. After you save the application ID, you can view the application ID number on the **Manage Integrations** page.
Token ID	Applicable only when you use token-based authentication. The token ID generated in NetSuite.
Token Secret	Applicable only when you use token-based authentication. The token secret generated in NetSuite.

Property	Description

Record Custom Fields	Specify custom NetSuite fields.
	- Add the custom fields using the following format, where the value of scriptId is the ID field in the NetSuite user interface for each custom field:
	`[<Object Name>] scriptIds = <custom field name1>, <custom field name2>,<custom field name3>`
	For example:
	`[Sales] scriptIds = discountPrice, salesDescription,salesEvent3`
	- Add the custom fields for NetSuite advanced search using the following format, where the value of scriptId is the ID field in the NetSuite user interface for each custom field:
	`[<Object Name>] scriptIds = <custom field name1>, <custom field name2>,<custom field name3>`
	For example:
	`[EmployeeSearchAdvanced]scriptIds = custentity74,custentity66`
	- To read or write custom segment data, use the following format to add the custom segment fields:
	`[<Object Name>] custSegScriptIds=custseg1: select,custseg2:multiselect,custseg3:select....`
	where the value of scriptId is the ID field in the NetSuite user interface for each custom segment field.
	For example:
	`[Employee] custSegScriptIds=custentity_cseg1: select,custentity_csegcs_multsel:multiselect`
	- To read data from or write data to child record custom segments, use the following format to add the child custom segment fields:
	`[<Object Name>] custSegScriptIds =custseg1:select,custseg2: multiselect,custseg3:select....`
	For example:
	`[JournalEntry] custSegScriptIds =custbody_cseg1:select,custbody_cseg2:select, custbody_cseg3:select`
	`[JournalEntryLineList] custSegScriptIds =custcol_cseg1:select,custcol_cseg2:select, custcol_cseg3:select`

Property	Description

Record Filter Fields	Map NetSuite record field names with related NetSuite search record field names so that you can use the fields in filters.
	List the record field names and related SearchBasic field names, as follows:
	`[<record 1>] <record field name>`
	`=<SearchBasic field name><record field name2>`
	`=<SearchBasic field name2>`
	`[<record 2>] <record field name>`
	`=<SearchBasic field name><record field name2>`
	`=<SearchBasic field name2><record field name3>`
	`=<SearchBasic field name3>`
	For example: `[Account] acctName=nameaddr1=address1`
	To read transactional data from NetSuite when memorized transaction is enabled in the NetSuite account, add the record field names and related SearchBasic field name in the following format:
	`[<record 1>] <record field name>`
	`=<SearchBasic field name>`
	For example: `[JournalEntry] reversalEntry=memorized`

Saved Search Record Fields	Create a separate section for each NetSuite saved search record for which you want to add a saved search field, identified by a unique scriptId.
	- Add the search fields using the following format:
	`<savedSearchId1>=<savedSearchDeclaredField1Name>,`
	`<savedSearchDeclaredField2Name>,<savedSearchCustomFieldScriptId1>,`
	`<savedSearchCustomFieldScriptId2>,<StandardJoin>|<FieldName1>,`
	`customSearchJoin|<scriptID1>`
	For example:
	`1000=phone,email,custentity78,custentity65, userJoin|email,customSearchJoin|`
	`custrecord1424`
	- To read custom segment data, use the following format to add the search custom segment fields:
	`[savedSearchId1]=custseg1:select, custseg2:multiselect, custseg3:select...`
	For example:
	`[741]=custseg1:select,custentity_cseg1:select,`
	`custentity_csegcs_multsel:multiselect`
	- To override the metadata of a task, which is created to read custom record standard fields with custom join, use the following format to add the search custom record standard fields:
	`<savedSearchId1>=CustomSearchJoin| <scriptId of custom record>__<standard field name>`
	For example:
	`356=CustomSearchJoin|uss_custom_code__internalId`

PostgreSQL

Create a PostgreSQL connection to read from or write to PostgreSQL and Amazon Aurora PostgreSQL databases.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your PostgreSQL Cloud account.

The following video shows you how to get information from your PostgreSQL Cloud account:

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.
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
Database	The PostgreSQL database name.
User Name	User name to access the PostgreSQL database.
Password	Password for the PostgreSQL database user name.

Property	Description
Encryption Method	Determines whether the data exchanged between the agent and the PostgreSQL database server is encrypted: Select one of the following encryption methods: - noEncryption. Establishes a connection without using SSL. Data is not encrypted. - SSL. Establishes a connection using SSL. Data is encrypted using SSL. If the PostgreSQL database server can't configure SSL, the connection fails. - requestSSL. Attempts to establish a connection using SSL. If the PostgreSQL database server can't configure SSL, the Secure Agent establishes an unencrypted connection. Default is noEncryption.
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.
TrustStore	Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts.
TrustStore Password	Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. The password to access the truststore file that contains the SSL certificate.
Host Name In Certificate	Optional when you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. 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.
KeyStore	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. 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.
KeyStore Password	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. The password for the keystore file required for secure communication.
Key Password	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. Required when individual keys in the keystore file have a different password than the keystore file.
Additional Connection Properties	Additional connection parameters that you want to use. Provide the connection parameters as semicolon-separated key-value pairs.
Crypto Protocol Versions	Required if you select SSL or requestSSL as the encryption method. A cryptographic protocol or a list of cryptographic protocols to use with an encrypted connection. You can select one of the following protocols: - SSLv3 - TLSv1_2 Default is TLSv1_2.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from PostgreSQL:

Property	Description
Pre-SQL	The pre-SQL commands to run a query before you read data from PostgreSQL. You can partially parameterize pre-SQL with values specified in a parameter file.
Post-SQL	The post-SQL commands to run a query after you write data to a target. You can partially parameterize post-SQL with values specified in a parameter file.
Fetch Size	Determines the number of rows to read in one resultant set from PostgreSQL. Specifying a number limits the number of rows to fetch with each trip to the database and avoids unnecessary memory consumption. You can specify a maximum fetch size of 2147483647. Default is 100000.
Schema Name	Overrides the schema name of the source object.
Source Table Name	Overrides the default PostgreSQL source table name.
SQL Override	The SQL statement to override the default query generated from the specified source type to read data from the PostgreSQL source. You can partially parameterize SQL override with values specified in a parameter file. Ensure that the list of selected columns, data types, and the order of the columns that appear in the query matches the columns, data types, and order in which they appear in the source object. **Note:** SQL override is not applicable when you enable partitioning. If you specify an SQL override and configure partitioning, the mapping fails.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to PostgreSQL:

Property	Description
Update Mode	Specifies the mode to write data to PostgreSQL target. You can specify the following modes: - Update As Update. Updates all rows flagged for update if the entries exist. - Update Else Insert. Updates all rows flagged for update if the entries exist in the target. If the entries do not exist, the Secure Agent inserts the entries.
Override Target Query	An SQL statement to override the default update query that the Secure Agent generates for the update operation.
Schema Name	Overrides the schema name of the target object.
Target Table Name	Overrides the default PostgreSQL target table name.
Pre-SQL	The pre-SQL commands to run a query before you read data from a source. You can partially parameterize pre-SQL with values specified in a parameter file.

Property	Description
Post-SQL	The post-SQL commands to run a query after you write data to PostgreSQL. You can partially parameterize post-SQL with values specified in a parameter file.
Truncate Target	The Secure Agent truncates the target before writing the data.
Enable target bulk load	Performs bulk upload when you configure an insert operation to write to PostgreSQL. Select this option to improve the performance of inserting data in bulk to PostgreSQL. Default is unselected. **Note:** When you enable the target bulk mode to insert data to PostgreSQL, error files are not generated for rejected records.
Batch size	The number of rows that the Secure Agent writes in a single batch to PostgreSQL. Specify a batch size value that is greater than zero. Applicable if you select the **Enable target bulk load** option.
Reject File Directory	The directory that stores the rejected files. Specify the directory where you want to store the rejected files.
Reject File Name	Name of the rejected file that is stored in the reject file directory.

Salesforce Marketing Cloud

Create a Salesforce Marketing Cloud connection to read from or write to Salesforce Marketing Cloud.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Salesforce account.

The following video shows you how to get information from your Salesforce account:

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.

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:
	`https://webservice.s7.exacttarget.com/etframework.wsdl`
	The following URL is an example for OAuth 2.0 URL:
	`https://<SUBDOMAIN>.soap.marketingcloudapis.com/etframework.wsdl`

Username	Applies to basic authentication. The user name of the Salesforce Marketing Cloud account.
Password	Applies to basic authentication. The password for the Salesforce Marketing Cloud account.
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 though proxy.
Enable Logging	Enables logging for the task. When you enable logging, you can view the session log for the log details.
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.
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.
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.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Salesforce Marketing Cloud:

Property	Description
Batch Size	Minimum number of rows that the Secure Agent reads in a batch. Enter a number greater than 0. Default is **0**.
Read Parameter File	Not applicable.
Tracing Level	Determines the amount of detail that appears in the log file. Select one of the following options: - Terse - Normal - Verbose Initialization - Verbose Data Default is **Normal**.

Note: Tracing level is not applicable for INFACore.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Salesforce Marketing Cloud:

Property	Description
Batch Size	Minimum number of rows that the Secure Agent writes in a batch. Enter a number greater than 0. Default is **0**.
Success File Directory	Directory for the success rows file. You must specify a directory path that is available on each Secure Agent machine in the runtime environment to save the success rows file. Ensure that your administrator has granted you access to this directory. If you do not specify a directory, the success rows file is not created.
Error File Directory	Directory for the error rows file. By default, the error rows file is written to the following Secure Agent directory: `<Secure Agent installation directory>/apps/Data_Integration_Server/data/error` Specify a directory path that is available on each Secure Agent machine in the runtime environment. Ensure that your administrator has granted you access to this directory.

SAP ADSO

Create an SAP ADSO connection to read from or write to SAP ADSO.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the SAP ADSO Writer 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.

SAP Server Connection Type	The SAP server connection type to use.
	Select from the following options:
	- **Application Server Connection**. Connect to an SAP Application Server using the SAP user name and password.
	- **Application Server SNC Connection**. Connect to an SAP Application Server using the secured network connection:
	  - 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.
	  - Without X.509 Certificate. You must provide the SAP user name.
	- **Load Balancing Server Connection**. Connect to an SAP Application Server with the least load at run time.
	- **Load Balancing Server SNC Connection**. Connect to an SAP Application Server using SNC with the least load at run time.
	Note: 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.

Connection property	Description
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.

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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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	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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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: - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is *3 - Apply privacy protection (integrity and authentication)*.
SAP Cryptographic Library Path	The path to the cryptographic library. Specify `sapcrypto.dll` for Windows or `libsapcrypto.so` 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 .crt 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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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: - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is *3 - Apply privacy protection (integrity and authentication)*.
SAP Cryptographic Library Path	The path to the cryptographic library. Specify `sapcrypto.dll` for Windows or `libsapcrypto.so` 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 .crt 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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

SAP BW

Create an SAP BW connection to read from SAP BW.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Connection properties

The following table describes the SAP BW 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.
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: - Application. Create an application connection when you want to connect to a specific SAP BW server. - Load balancing. Create a load balancing connection when you want to use SAP load balancing. Default is Application.
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	Use this option to track the JCo calls that the SAP system makes. Specify one of the following values: - 0. Off - 1. Full Default is 0. SAP stores information about the JCo calls in a trace file. You can access the trace files from the following directories: - Design-time information: `<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<Latest version>\ICS\main\tomcat` - Run-time information: `<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<Latest version>\ICS\main\bin\rdtm`
Additional parameters	Additional JCo connection parameters that you want to use. Use the following format: `<parameter name1>=<value1>, <parameter name2>=<value2>`
Port Range	HTTP port range that the Secure Agent must use to read data from the SAP BW server in streaming mode. 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. Default is 10000-65535.
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	Additional SAP parameters that the Secure Agent uses to connect to the SAP system as an RFC client.
	You can specify the required RFC-specific parameters and connection information to enable communication with SAP.
	For example, you can specify the SNC connection parameters as additional arguments to connect to SAP:
	`MSHOST= <Message server hostname>`
	`GROUP=PUBLIC`
	`R3NAME=SLT`
	`SNC_MODE=1`
	`SNC_QOP=3`
	`SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country> This is the SNC name of the Secure Agent machine.`
	`SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, OU=SAP Web AS, O=<Organization>, C=<Country>. This is the SNC name of the SAP system.`
	`SNC_LIB =<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/<libsapcrypto.so for Linux/sapcrypto.dll for Windows>`
	`X509CERT=<X509 certificate>`
	Note: For information about the SNC parameters that you can configure in this field, see the Informatica How-To Library article.
	Note: If you have specified the mandatory connection parameters in the connection, those values override the additional parameter arguments.

SAP ODP

Create an SAP ODP connection to read from SAP ODP.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Connection properties

The following table describes the SAP ODP Extractor 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.

SAP Server Connection Type	The SAP server connection type to use.
	Select from the following options:
	- **Application Server Connection**. Connect to an SAP Application Server using the SAP user name and password.
	- **Application Server SNC Connection**. Connect to an SAP Application Server using the secured network connection:
	  - 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.
	  - Without X.509 Certificate. You must provide the SAP user name.
	- **Load Balancing Server Connection**. Connect to an SAP Application Server with the least load at run time.
	- **Load Balancing Server SNC Connection**. Connect to an SAP Application Server using SNC with the least load at run time.
	Note: 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.

Connection property	Description
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.

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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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.

Connection property	Description
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.

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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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: - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is *3 - Apply privacy protection (integrity and authentication)*.
SAP Cryptographic Library Path	The path to the cryptographic library. Specify `sapcrypto.dll` for Windows or `libsapcrypto.so` for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.

Connection property	Description
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 .crt 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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

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	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.

Connection property	Description
SNC Quality of Protection (QoP)	Specifies the SAP PSE or certificate name. You can select from the following options: - 1 - Apply authentication only. - 2 - Apply integrity protection (authentication). - 3 - Apply privacy protection (integrity and authentication). - 8 - Apply the default protection. - 9 - Apply the maximum protection. Default is *3 - Apply privacy protection (integrity and authentication)*.
SAP Cryptographic Library Path	The path to the cryptographic library. Specify `sapcrypto.dll` for Windows or `libsapcrypto.so` 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 .crt 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:
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	During the runtime, the JCo and CPIC traces file are generated in the following location:
	`<Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	During the design time, the CPIC traces are generated in the `tomcat.out` files at the following location:
	`<Informatica Secure Agent installation directory>\apps \Data_Integration_Server\<DIS version>tomcat.out`

SAP Table

Create an SAP Table connection to read from SAP Table.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Connection properties

The following table describes the SAP Table 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.
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 `sapnwrfc.ini` 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`
Destination	Required. DEST entry that you specified in the `sapnwrfc.ini` file for the SAP application server. Destination is case sensitive. **Note:** Use all uppercase letters for the destination.
Port Range	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. 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.
Test Streaming	Tests the connection. When selected, tests the connection using both RFC and HTTP protocol. When not selected, tests connection using HTTP protocol.
Https Connection	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.

Property	Description
Keystore Location	The absolute path to the JKS keystore file.
Keystore Password	The destination password specified for the .JKS file.
Private Key Password	The export password specified for the .P12 file.

ServiceNow

Create a ServiceNow connection to read from or write to ServiceNow.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your ServiceNow account.

The following video shows you how to get information from your ServiceNow account:

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.
Username	User name of the ServiceNow instance.
Password	Password for the ServiceNow instance.

Property	Description
EndPoint URL	The ServiceNow endpoint URL.
Instance Type	Type of ServiceNow instance. Select JSONv2.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from ServiceNow:

Source Property	Description
Read Batch Size	The maximum number of records that the Secure Agent reads in a batch from ServiceNow. **Note:** You can specify a maximum batch size of up to 10,000 records. If you specify a batch size beyond 10,000 records, data loss is encountered.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to ServiceNow:

Target Property	Description
Insert Batch Size	The maximum number of records that the Secure Agent writes in a batch to ServiceNow. You can specify a maximum batch size of up to 10,000 records. If you specify a batch size beyond 10,000 records, data loss is encountered. **Note:** When you insert records and a single record fails in the batch, the number of success rows in the **Job Properties** page is displayed as 0.
Success File Directory	Directory for the success rows files. Specify a directory path that is available on each Secure Agent machine in the runtime environment. By default, the success rows file is written to the following directory: <Secure Agent installation directory>/apps/Data_Integration_Server/data/success
Error File Directory	Directory for the error rows files. Specify a directory path that is available on the Secure Agent machine in the runtime environment. By default, the error rows file is written to the following directory: <Secure Agent installation directory>/apps/Data_Integration_Server/data/error

SharePoint

Create a SharePoint connection to read from or write to SharePoint.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Microsoft SharePoint 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.
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, `https://infasharepoint.abcd.com/ Site/_vti_bin/ Data.svc`
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.

Sharepoint Online

Create a Sharepoint Online connection to read from or write to Sharepoint Online.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Microsoft Sharepoint Online 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.
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 **URL** property.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Sharepoint Online:

Property	Description
Indirect File Path	The file path of the folder that you want to download.
Preserve Directory Structure	Retains the same folder structure as that of Sharepoint Online.

Snowflake

Create a Snowflake connection to read from or write to Snowflake tables and views. You can also read from Snowflake external tables, hybrid tables, and materialized views.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Snowflake account.

The following video shows you how to get information from your Snowflake account:

You can use the following authentication methods to connect to Snowflake:

- Standard. Uses Snowflake account user name and password credentials to connect to Snowflake.
- 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.

Connection properties

For the connection properties, see the following topics:

- "Standard authentication" on page 135
- "Key pair authentication" on page 137
- "OAuth 2.0 authorization code authentication" on page 136

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Snowflake:

Advanced Property	Description
Database	Overrides the database specified in the connection.
Schema	Overrides the schema specified in the connection.

Advanced Property	Description
Warehouse	Overrides the Snowflake warehouse name specified in the connection.
Role	Overrides the Snowflake role assigned to user you specified in the connection. The warehouse name in the mapping overrides the warehouse name you specify in the connection. Even though you provide an incorrect warehouse name in the connection properties, the connection is successful. However, before you run the mapping, ensure that you specify the correct warehouse name in the mapping properties.
Pre SQL	The pre-SQL command to run on the Snowflake source table before the agent reads the data. For example, if you want to update records in the database before you read the records from the table, specify a pre-SQL statement. The query must include a fully qualified table name. You can specify multiple pre-SQL commands, each separated with a semicolon.
Post SQL	The post-SQL command to run on the Snowflake table after the agent completes the read operation. For example, if you want to delete some records after the latest records are loaded, specify a post-SQL statement. The query must include a fully qualified table name. You can specify multiple post-SQL commands, each separated with a semicolon.
Table Name	Overrides the table name of the imported Snowflake source table.
SQL Override	The SQL statement to override the default query used to read data from the Snowflake source.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Snowflake:

Advanced Property	Description
UpdateMode	Loads data to the target based on the mode you specify. Applicable when you select the Update operation or the Data Driven operation. Select from one of the following modes: - Update As Update. Updates all rows flagged for update if the entries exist. - Update Else Insert. The agent first updates all rows flagged for update if the entries exist in the target. If the entries do not exist, the agent inserts the entries.
Database	Overrides the database that you used to import the object.
Schema	Overrides the schema that you used to import the object.
Warehouse	Overrides the Snowflake name specified in the connection. The warehouse name in the mapping overrides the warehouse name you specify in the connection. Even though you provide an incorrect warehouse name in the connection properties, the connection is successful. However, before you run the mapping, ensure that you specify the correct warehouse name in the mapping properties.
Role	Overrides the Snowflake role assigned to the user specified in the connection.

Advanced Property	Description
Pre SQL	The pre-SQL command to run before the agent writes to Snowflake. For example, if you want to assign sequence object to a primary key field of the target table before you write data to the table, specify a pre-SQL statement. You can specify multiple pre-SQL commands, each separated with a semicolon.
Post SQL	The post-SQL command to run after the agent completes the write operation. For example, if you want to alter the table created by using create target option and assign constraints to the table before you write data to the table, specify a post-SQL statement. You can specify multiple post-SQL commands, each separated with a semicolon.
Batch Row Size	The number of rows written to a single file in the agent location. When the number of rows written to the file reaches the value specified, the agent flushes the data queue and starts processing the write commands.
Number of local staging files	The number of files that represents a single batch of data. The default number of files is 64. After the agent uploads the specified number of local staging files to the Snowflake user stage, Snowflake unloads the data to the target table.
Truncate Target Table	Truncates the database target table before inserting new rows. Select one of the following options: - True. Truncates the target table before inserting all rows. - False. Inserts new rows without truncating the target table Default is false.

Additional Write Runtime Parameters	Specify additional runtime parameters.
	For example, if you want to specify the user-defined stage in the Snowflake database to upload the local staging files, specify the name of the stage location in the following format:
	`remoteStage=REMOTE_STAGE`
	If you want to optimize the write performance, you can choose to compress files before writing to Snowflake tables. You can set the compression parameter to On or Off, for example:
	`Compression=On`
	By default, compression is on.
	Separate multiple runtime parameters with &.

Table Name	Overrides the table name of the Snowflake target table.
Rejected File Path	The filename and path of the file on the agent machine where you want to write the rejected records. For example, `\rejectedfiles\reject7`
Update Override	Overrides the default update query that the agent generates for the update operation with the update query.

Standard authentication

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

The following table describes the Snowflake 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.
Authentication	The authentication method that the connector must use to log in to Snowflake. Select **Standard**. Default is **Standard**.
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 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 **Note:** 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:
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	For example:
	`user=jon&warehouse=mywh&db=mydb&schema=public`
	Important: 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 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.
Authentication	The authentication method that the Snowflake connection must use to log in to Snowflake. Select **AuthorizationCode**.
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 **Note:** 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:
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	For example:
	`user=jon&warehouse=mywh&db=mydb&schema=public`
	Important: 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 **Note:** 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.
Access Token URL	The Snowflake access token endpoint that is used to exchange the authorization code for an access token. The access token URL is https://<account name>.snowflakecomputing.com/oauth/token-request, where <account name> specifies the full name of your account provided by Snowflake. For example, https://<abc>.snowflakecomputing.com/oauth/token-request **Note:** If the account name contains underscores, use the alias name.
Client ID	Client ID of your application that Snowflake provides during the registration process.
Client Secret	Client secret of your application.

Property	Description
Scope	Determines the access control if the API endpoint has defined custom scopes. Enter space-separated scope attributes. For example, specify `session:role:CQA_GCP` as the scope to override the value of the default user role. The value must be one of the roles assigned in Security Integration.
Access Token Parameters	Additional parameters to use with the access token URL. Define the parameters in the JSON format. For example, define the following parameters: `[{"Name":"code_verifier","Value":"5PMddu6Zcg6Tc4sbg"}]`

Authorization Code Parameters	Additional parameters to use with the authorization token URL.
	Define the parameters in the JSON format.
	For example, define the following parameters:
	`[{"Name":"code_challenge","Value":"Ikr-vv52th0UeVRi4"},`
	`{"Name":"code_challenge_method","Value":"S256"}]`

Access Token	The access token value. Enter the populated access token value, or click **Generate Token** to populate the access token value.
Generate Token	Generates the access token and refresh token based on the OAuth attributes you specified.
Refresh Token	The refresh token value. Enter the populated refresh token value, or click **Generate Token** 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. **Note:** If the refresh token expires, provide a valid refresh token or regenerate a new refresh token by clicking **Generate Token**.

Key pair authentication

The following table describes the Snowflake 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.
Authentication	The authentication method to log in to Snowflake. Select **KeyPair**.
Username	The user name to connect to the Snowflake account.

Connection property	Description
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. **Note:** 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	Optional. The additional JDBC connection parameters.
	Enter one or more JDBC connection parameters in the following format:
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	For example:
	`user=jon&warehouse=mywh&db=mydb&schema=public`
	Important: Ensure that there is no space before and after the equal sign (=) when you add the parameters.

Private Key File	Path to the private key file, including the private key file name, that the Secure Agent uses to access Snowflake. **Note:** Verify that the keystore is FIPS-certified.
Private Key Password	Password for the private key file.

SQL Server

Create a SQL Server connection to read from or write to the Microsoft SQL Server database.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your Amazon Web Services account.

The following video shows you how to get information from your Amazon Web Services account:

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.
SQL Server Version	Microsoft SQL Server database version.
Authentication Mode	Authentication method to access Microsoft SQL Server. Select one of the following methods: - SQL Server Authentication. Uses your Microsoft SQL Server user name and password to access Microsoft SQL Server. - Windows Authentication (Deprecated). Uses the Microsoft Windows authentication to access Microsoft SQL Server. This option is available when you use Microsoft Windows. - Active Directory Password. Uses the Azure Active Directory user name and password to authenticate and access the Microsoft Azure SQL Database. - Windows Authentication v2. Uses this authentication method to access Microsoft SQL Server using the agent hosted on a Linux or Windows machine. When you choose this option, enter your domain name and Microsoft Windows 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 when you use the Windows agent.
Domain	Applies to Windows Authentication v2. The domain name of the Windows user.
User Name	User name for the database login. The user name can't contain a semicolon. To connect to Microsoft Azure SQL Database, specify the user name in the following format: `username@host` For Windows Authentication v2, specify the Windows NT user name. **Note:** This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Password	Password for the database login. The password can't contain a semicolon. For Windows Authentication v2, specify the Windows NT password. **Note:** This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Host	Name of the machine hosting the database server. To connect to Microsoft Azure SQL Database, specify the fully qualified host name. For example, `vmjcmwxsfboheng.westus.cloudapp.azure.com`.

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. 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.
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 trust store file. The trust store file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication. `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename>`
Trust Store Password	The password to access the contents of the trust store 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 for the runtime. If you specify more than one property, separate each key-value pair with a semicolon.

Read properties

The following table describes the advanced source properties that you can configure in the Python code to read from Microsoft SQL Server:

Property	Description
Pre SQL	Pre-SQL command that must be run before reading data from the source.
Post SQL	Post-SQL command that must be run after reading data from the source.
Output is Deterministic	Relational source or transformation output that does not change between session runs when the input data is consistent between runs. When you configure this property, the Secure Agent does not stage source data for recovery if transformations in the pipeline always produce repeatable data.
Output is repeatable	Relational source or transformation output that is in the same order between session runs when the order of the input data is consistent. When output is deterministic and output is repeatable, the Secure Agent does not stage source data for recovery.
SQL Override	The SQL statement to override the default query generated from the specified source type to read data from the Microsoft SQL Server source.

Write properties

The following table describes the advanced target properties that you can configure in the Python code to write to Microsoft SQL Server:

Property	Description
Forward Rejected Rows	Determines whether the transformation passes rejected rows to the next transformation or drops rejected rows. By default, the mapping task forwards rejected rows to the next transformation. If you select the Forward Rejected Rows option, the Secure Agent flags the rows for reject and writes them to the reject file. If you do not select the Forward Rejected Rows option, the Secure Agent drops the rejected rows and writes them to the session log file. The Secure Agent does not write the rejected rows to the reject file.
Pre SQL	Pre-SQL command to run against the target database before writing data to the target.
Post SQL	Post-SQL command to run against the target database after writing data to the target.
Update Override	An update SQL statement that updates the data in a Microsoft SQL Server target table. The update SQL statement you specify overrides the default update statements that the Secure Agent generates to update the target based on key columns. You can define an update override statement to update target tables based on both key or non-key columns. In the override statement, you must enclose all reserved words in quotation marks.
Reject file directory	The directory that stores the rejected files. Specify the directory where you want to store the rejected files.
Reject filename	Name of the rejected file that is stored in the reject file directory.
Schema Name	The schema name that overrides the schema name specified in the target connection.

SuccessFactors LMS

Create a SuccessFactors LMS connection to read from SuccessFactors LMS.

Feature snapshot

Operation	Support
Read	Yes
Write	No

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.

Service URL	OData service root URL that exposes the data that you want to read.
	Enter the URL in the following format:
	`https://<rooturl>/learning/odatav4/<webservicename>/v1/`
	For example, if the root URL is `partner0370.scdemo.successfactors.com:443` and the Web Service name is `curriculum`, enter the URL as follows:
	`https://partner0370.scdemo.successfactors.com:443/learning/odatav4/curriculum/v1/`
	For information about the Web Service names, see the *SuccessFactors Learning Web Services OData API Reference Guide*.

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 **admin** if you run the Web Service with an administrator user account. - user. Select **user** if you run the Web Service with an end-user account.

SuccessFactors ODATA

Create a SuccessFactors ODATA connection to read from or write to SuccessFactors.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Before you begin

Before you configure the connection properties, you'll need to get information from your SAP SuccessFactors account.

The following video shows you how to get information from your SAP SuccessFactors account:

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.
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. **Important:** 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 https://apisalesdemo8.successfactors.com/odata/v2.
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.

Property	Description
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: - HTTP Basic Authentication. Requires administrator access to the OData API and credentials for a valid account. - OAuth 2.0. Requires a valid token and a registered OAuth 2.0 client application.
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.
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.

Tableau

Create a Tableau connection to read from or write to Tableau Desktop, Tableau Server, or Tableau Online.

Feature snapshot

Operation	Support
Read	Yes
Write	Yes

Connection properties

The following table describes the Tableau 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.
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the `.hyper` file: **Tableau Desktop** Creates a `.hyper` or TWBX files in the Secure Agent machine. You can then manually import the `.hyper` or TWBX files to Tableau Desktop and use the files to perform append or overwrite operation. **Tableau Server** Publishes the generated `.hyper` file to Tableau Server. **Tableau Online** Publishes the generated `.hyper` file to Tableau Online.
Connection URL	The URL of Tableau Server or Tableau Online to which you want to publish the `.hyper` file. The URL has the following format: `http://<Host name of Tableau Server or Tableau Online>:<port>` **Note:** This property is applicable when you select the value of the **Tableau product** as Tableau Server or Tableau Online.
User Name	User name of the Tableau Server or Tableau Online account. **Note:** This property is applicable when you select the value of the **Tableau product** as Tableau Server or Tableau Online.
Password	Password for the Tableau Server or Tableau Online account. **Note:** This property is applicable when you select the value of the **Tableau product** as Tableau Server or Tableau Online.

Connection property	Description
Site ID	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. **Note:** This property is applicable when you select the value of the **Tableau product** as Tableau Server or Tableau Online.
Schema File Path	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: - Absolute path to the `.hyper` file. - Directory path for the `.hyper` files. - Empty directory path. You can only specify an empty directory if you want to publish the `.hyper` file to Tableau Server or Tableau Online. 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 **Object** target properties. The Secure Agent uses the following default file path for the target `.hyper` file: `<Secure Agent installation directory>/apps/Data_Integration_Server/<latest version>/main/bin/rdtm`

Zendesk

Create a Zendesk connection to read from Zendesk.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Before you begin

Before you configure the connection properties, you'll need to get information from your Zendesk account.

The following video shows you how to get information from your Zendesk account:

Connection properties

The following table describes the Zendesk 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.
Username	Username of the Zendesk account.
Password	Password of the Zendesk account.
URL	URL of the Zendesk account. Specify the complete URL. For example, https://informaticabusinesssolution13.zendesk.com/api/v2.
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.

Zuora AQuA

Create a Zuora AQuA connection to read data and to retrieve deleted rows from Zuora AQua.

Feature snapshot

Operation	Support
Read	Yes
Write	No

Before you begin

Before you configure the connection properties, you'll need to get information from your Zuora account.

The following video shows you how to get information from your Zuora account:

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.
Endpoint URL	The URL of the Zuora server. For example, you can specify the URL as https://www.zuora.com/apps/api/.
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 lastruntime data filter field to read data from Zuora based on the specified time zone.

INDEX