informatica Cloud
Cloud API Response Team

Rest Connector

User Guide

Abstract

ReST user guide provides a brief introduction on cloud connectors and its features. The guide provides detailed information on setting up the connector and running data synchronization tasks (DSS). A brief overview of supported features and task operations that can be performed using ReST connector is mentioned.

Table of Contents

Overview

Informatica cloud connector developed using SDK framework are off-cycle, off release “add-ins” that facilitate data integration to SaaS and on premise applications, which are not supported natively by Informatica cloud. The cloud connectors are specifically designed to address most common use cases such as moving data into cloud and retrieving data from cloud for individual application.

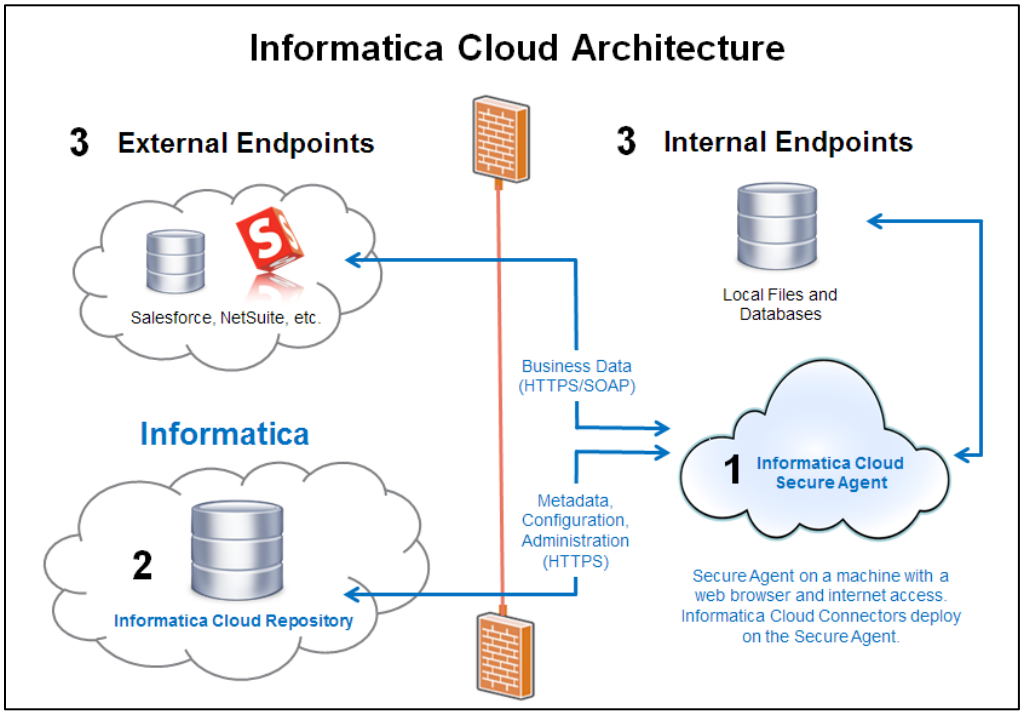

Figure 1: Informatica Cloud Architecture

Once the ReST connector is enabled for your ICS ORG Id, you need to create a connection in Informatica cloud to access the connector.

Pre-requisites for Installing the ReST Connector Plug-in

- You need ReST Application Access that is User credentials to create a ReST Connection in the Informatica Cloud.
- Provide the Base url request and authentication parameters to create a connection.
- Mention **Auth Type** and **Media Type**.

Assumptions and Considerations

ReST Connector was developed and tested considering following assumptions:

1. ReST connector supports following Media-Type:

- **application/xml**
- **application/json**

2. ReST connector supports following Request-Type:

- **GET**
- **POST**
- **PUT**
- **DELETE**

3. The supported Authentication-Type is

- **NO_AUTH**
- **BASIC_AUTH**
- **DIGEST_AUTH**
- **OAUTH**
- **CUSTOM_AUTH**

ReST Connector Description

The Informatica Cloud Web Services Connector allows you to integrate data with REST based web services applications that are either internal to an organization or external applications.

The connector supports Web Services that conform to REST methods.

Supported Objects and Task Operations

The table below provides the list of objects and task operations supported by ReST connector.

Objects	Task Operation							Data Preview	Look Up
	DSS Source	DSS Target	Query	Insert	Update	Upsert	Delete		
Rest Entity	✓	✓	✓	✓	NA	NA	NA	✓	NA

✓ : Supported
NA : Not Applicable

Enabling ReST Connector

To enable ReST connector, contact Informatica support or Informatica representative. It usually takes 15 minutes for the connector to download to secure agent, after it is enabled.

Note: To install secure agent, see Installing Informatica Secure Agent.

Understanding the ReST Connection Parameters

The section explains the ReST connection parameters in detail. The Figure below displays the connection parameters:

Connection Details	
Connection Name:*	ReST_BlueGreen_Apprimo_Describe
Description:	ReST_BlueGreen_Apprimo_Describe
Type:*	REST (Informatica Cloud Labs)
REST Connection Properties	
Secure Agent:*	s158519-vm
Base Url:*	https://api01.marketingstudio.com/api/MetaData
Is BaseUrl Dynamic:	☐
Url Request Parameters:	
Form Request Parameters:	
Header Request Parameters:	
Media Type:*	application/xml
Request Type:*	GET
Authentication Type:*	CUSTOM_AUTH
Auth UserId:	
Auth Password:	
OAuth Consumer Key:	
OAuth Consumer Secret:	
OAuth Token:	
OAuth Token Secret:	
Additional Custom OAuth Parameters:	Describe
Config File or Private Key File Name:	
Sample Response XML or JSON File:	
Response Folder path:	
URL Input Parameters Config File Name:	
FORM Input Parameters Config File Name:	
HEADER Input Parameters Config File Name:	
Create the config csv file:*	NO

Figure 2: Connection Parameters

The following table explains ReST Connection Parameters.

Connection Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select **ReST** from the list
Secure Agent	Select the appropriate secure agent from the list.
Base URL	Endpoint url of ReST (without the Query parameters)
Is Base Url Dynamic	Select the checkbox if the base url for each request is different and dynamic.
Url Request Parameters	Mention the request that is **url query** parameters. Parameters separated by semicolon (;). The Property and value is separated by 'equals' (=).
Form Request Parameters	Mention the request that is form query parameters. Parameters separated by semi-colon (;). The Property and value is separated by 'equals' (=).
Header Request Parameters	Mention request that is Header query parameters. Parameters separated by semi-colon(;). The Property and value is separated by 'equals' (=).
Media Type	Select required media type from the list. HTTP Mime Type is supported.
Request Type	Select the required Request Type from the list. HTTP Request type.
Authentication Type	Select the required authentication type such as Basic, Digest or OAuth.
Auth UserId	Mention the UserId for Basic and Form based authentication.
Auth Password	Provide the password for Basic and Form based authentication.
OAuth Consumer Key	Provide the Consumer key for OAuth authentication.
OAuth Consumer Secret	Provide the Consumer secret for OAuth authentication
OAuth Token	Mention the token key for OAuth authentication
OAuth Token Secret	Mention the Token Secret for OAuth authentication
Additional Custom OAuth Parameters	Provide additional Custom Auth parameter. This field is essentially used for Blue Green use case.
Sample Response XML or JSON File Path	Provide full file path of the xml. You can also mention the xml or JSON path of the Response.
Response Folder Path	Mention the folder path (in secure agent machine) where you want to generate the response file.

Connection Property	Description
Url Input Parameters Config File Name	Mention The URL Input Parameter File name with the path.
Form Input Parameters Config File Name	Mention the Form Input Parameter File name with Path.
Header Input Parameters Config File Name	Mention the Header Input Parameter File name with Path.
Create the config csv file	Select **Yes** and then click **Test** for testing the connection. After successfully testing the connection, select **No**.

Creating a ReST Connection (Source connector)

To use ReST connector in data synchronization task, you must create a connection in Informatica Cloud.

The following steps help you to create ReST connection in Informatica Cloud.

1. In Informatica Cloud home page, click **Configure**.
2. The drop-down menu appears, select **Connections**.
3. The Connections page appears.
4. Click **New** to create a connection.
5. The New Connection page appears.

Connection Details

Connection Name:*	ReST_RMS_Con
Description:	
Type:*	REST (Informatica Cloud Labs)

REST Connection Properties

Secure Agent:*	s158519-vm
Base Url:*	https://endpointurl
Is BaseUrl Dynamic:	☐
Url Request Parameters:	
Form Request Parameters:	
Header Request Parameters:	tenantid=<someid>;username=<username>;pa
Media Type:*	application/json
Request Type:*	POST
Authentication Type:*	CUSTOM_AUTH
Auth UserId:	
Auth Password:	••••••••
OAuth Consumer Key:	
OAuth Consumer Secret:	••••••••
OAuth Token:	
OAuth Token Secret:	••••••••
Additional Custom OAuth Parameters:	
Config File or Private Key File Name:	
Sample Response XML or JSON File:	
Response Folder path:	C:\MyWorkspace\RMS_Usecase\response
URL Input Parameters Config File Name:	
FORM Input Parameters Config File Name:	
HEADER Input Parameters Config File Name:	C:\MyWorkspace\RMS_Usecase\response\heac
Create the config csv file:*	YES

Figure 3: Connection Details

6. Specify the following details.

Connection Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select ReST from the list.
Secure Agent	Select the appropriate secure agent from the list.
Base URL	Enter **End point UR**L. For example, https://<**End point URL**>/
Is Base Url Dynamic	NA
Url Request Parameters	NA
Form Request Parameters	NA
Header Request Parameters	Enter login Credentials in the following format : **tenanted=<ID>;username=<username>;** **password=<password>;encoding=UTF-16 or UTF-8**
Media Type	Select **JSON**
Request Type	Select **POST**
Authentication Type	NA
Auth UserId	NA
Auth Password	NA
OAuth Consumer Key	NA
OAuth Consumer Secret	NA
OAuth Token	NA
OAuth Token Secret	NA
Additional Custom OAuth Parameters	Enter Additional custom OAUTH Parameters.
Config File or Private Key File Name	NA
Sample Response XML or JSON File Path	NA
Response Folder Path	Enter the folder path where you want to generate the signature file.
Url Input Parameters Config File Name	NA

Form Input Parameters Config File Name	NA
Header Input Parameters Config File Name	Enter the folder path which contains the header input parameters config file with file name. **Note**: You can modify user credentials using this config file.
Create the config csv file	Select **Yes** and then click **Test** for testing the connection. After successfully testing the connection, select **No.**

Note: The **Url request parameter, Form request parameter,** and **Header request parameter** key should not contain **Semicolon (;)** and parameter value should not contain **equals (=)** sign.

Creating a ReST Data Synchronization Task to Generate Token to run DSS Tasks

Note: You need to create a connection before getting started with data synchronization task.

Refer Creating a ReST Connection when used as Source connector

The following steps help you to setup a data synchronization task in Informatica Cloud.
Let us consider the task operation **Insert** to perform the Data synchronization task.

1. In Informatica Cloud home page, click **Apps**.
2. The drop-down menu appears, select **Data Synchronization**.
3. The **Data Synchronization** page appears.
4. Click **New** to create a data synchronization task.
5. The **Definition** tab appears.

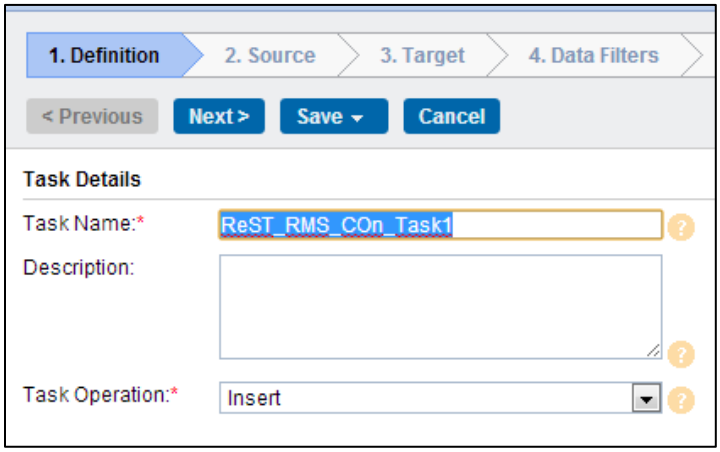

Figure 4: Definition Tab

6. Specify the **Task Name**, provide a **Description** and select the Task Operation **Insert**.
7. Click **Next**.
8. The **Source** tab appears.

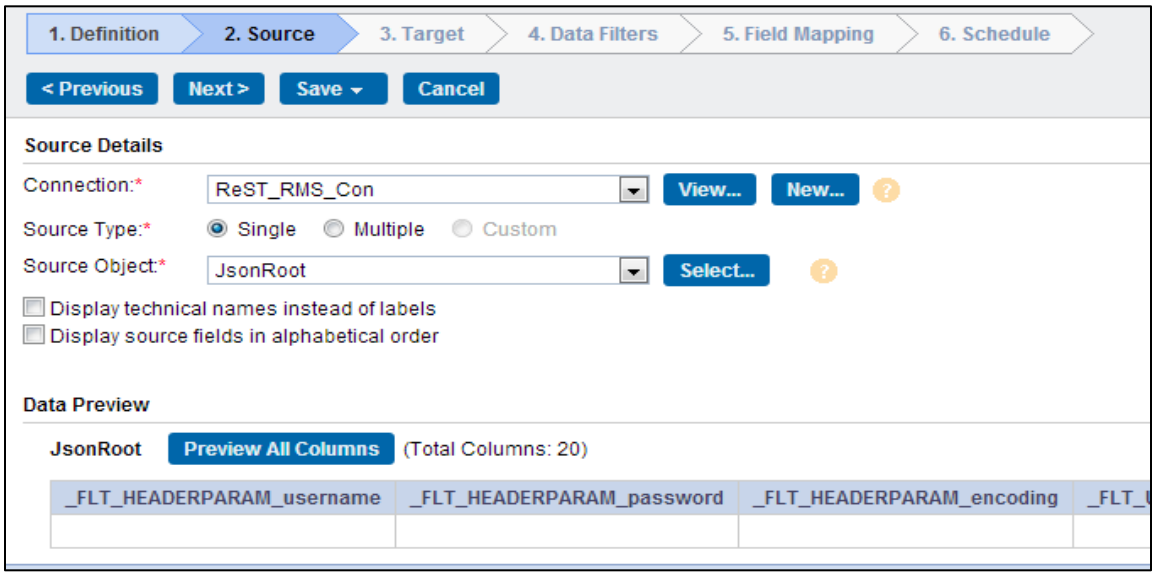

Figure 5: Source Tab

9. Select the source **Connection**, **Source Type** and **Source Object** to be used for the task.
10. Click **Next**.
11. The **Target** tab appears. Select the target **Connection** and **Target Object** required for the task.

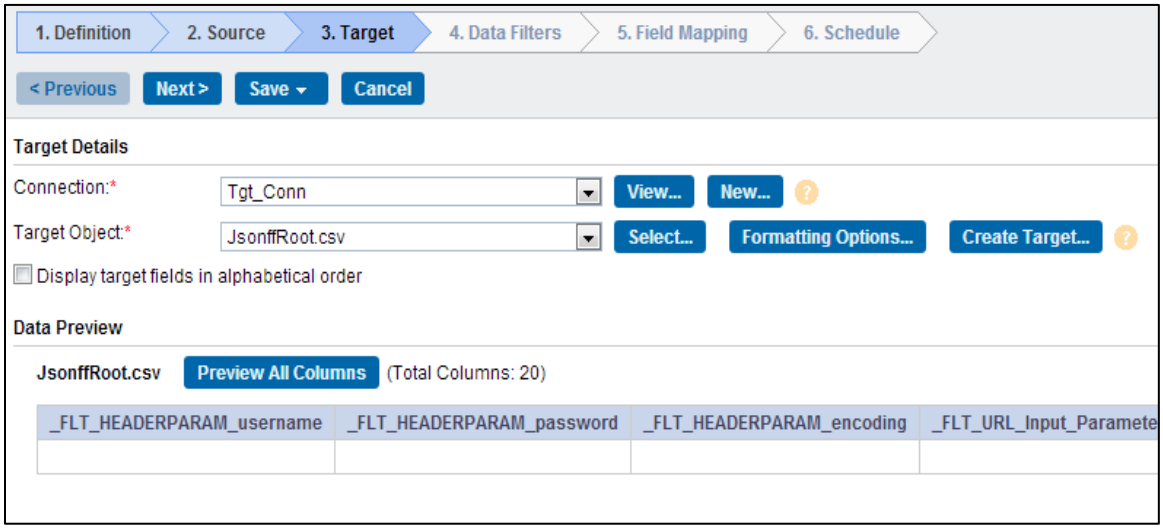

Figure 6: Target Tab

12. Click **Next**.
13. In **Data Filters** tab by default, Process all rows is chosen. To assign filters to fetch specific data, see Data Filters.

14. Click **Next**.
15. In **Field Mapping** tab, map source fields to target fields accordingly.

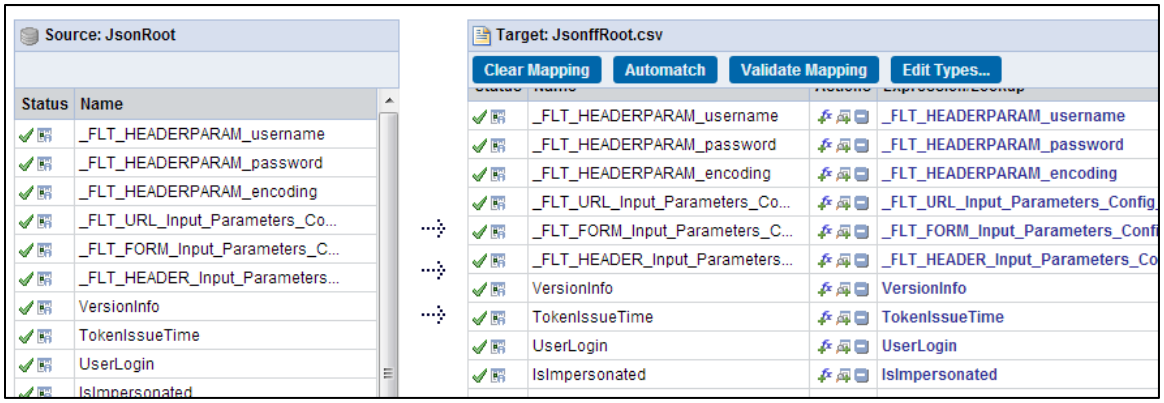

Figure 7: Field Mapping Tab

16. Click **Next**.
17. The **Schedule** tab appears.
18. The **Schedule** tab appears.
19. Click **Save and Run** If you do not want to schedule the task.

Note: In Schedule tab, you can schedule the task as per the requirement and save.

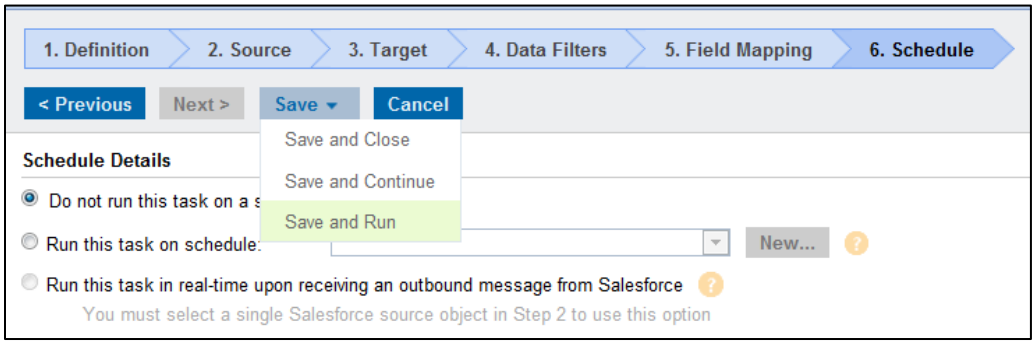

Figure 8: Save and Run the Task

After you **Save and Run** the task, you will be redirected to monitor log page. In monitor log page, you can monitor the status of data synchronization tasks.

20. Click **Ok** to save the connection.

Note: It is recommended to test the connection before saving it. Click **Test** to evaluate the connection.

Creating a ReST Connection (Target connector)

You must create a connection in Informatica Cloud to use ReST connector in data synchronization task.

Follow the given step to create ReST connection in Informatica Cloud.

1. In Informatica Cloud home page, click **Configure**.
2. The drop-down menu appears, select **Connections**.
3. The Connections page appears.
4. Click **New** to create a connection.
5. The New Connection page appears.

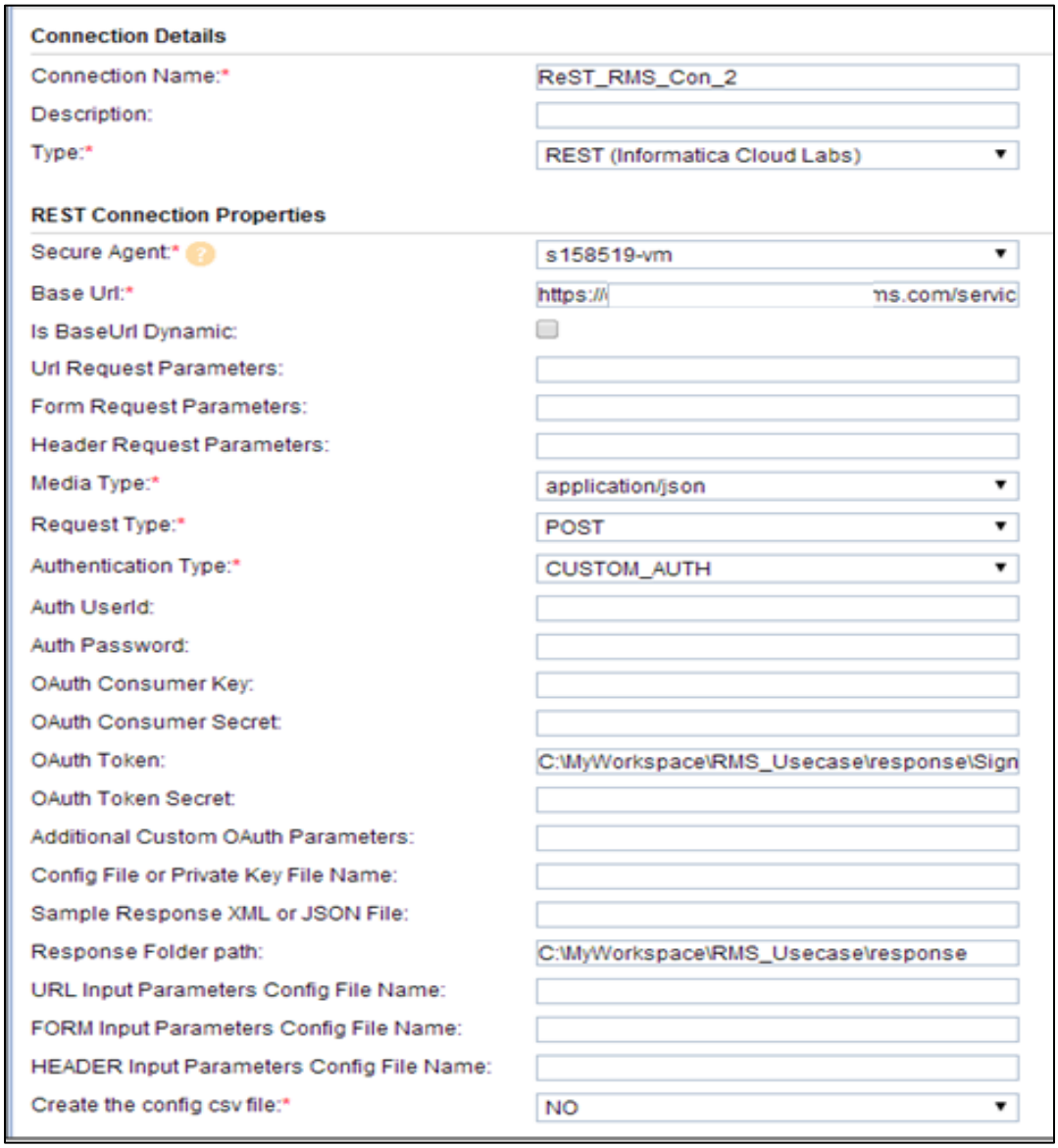

Figure 9: Creating a New Connection

6. Specify the following details.

Connection Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select **ReST** from the list.
Secure Agent	Select the appropriate secure agent from the list.
Base URL	Enter **End point URL** in the format given below: https://< **End point URL**>/
Is Base Url Dynamic	NA
Url Request Parameters	NA
Form Request Parameters	Select **JSON**
Header Request Parameters	Select **POST**
Media Type	NA
Request Type	NA
Authentication Type	NA
Auth UserId	NA
Auth Password	NA
OAuth Consumer Key	NA
OAuth Consumer Secret	NA
OAuth Token	Enter the file path generated in the DSS task.
OAuth Token Secret	NA
Additional Custom Auth Parameters	Enter Additional custom OAUTH Parameters.
Sample Response XML or JSON File Path	NA
Response Folder Path	Enter the folder path where you want to generate the signature file.
Url Input Parameters Config File Name	NA
Form Input Parameters Config File Name	NA
Header Input Parameters Config File Name	NA
Create the config csv file	Select **Yes** and click **Test** for testing the connection. After successfully testing the connection, select **No**.

Note: The **Url/Form/Header** request parameter key should not contain a **semicolon (;)** and parameter value should not contain **Equals (=)** sign.

7. Click **Ok** to save the connection.

Note: It is recommended to test the connection before saving it. Click **Test** to evaluate the connection.

Creating a ReST Data Synchronization Task to integrate with User's end point System

Note: You need to create a connection before getting started with data synchronization task.

Refer Creating a ReST Connection When used as Target connector

The following steps help you to setup a data synchronization task in Informatica Cloud.

Let us consider the task operation **Insert** to perform the Data synchronization task.

1. In Informatica Cloud home page, click **Apps**.
2. The drop-down menu appears, select **Data Synchronization**.
3. The **Data Synchronization** page appears.
4. Click **New** to create a data synchronization task.
5. The **Definition** tab appears.

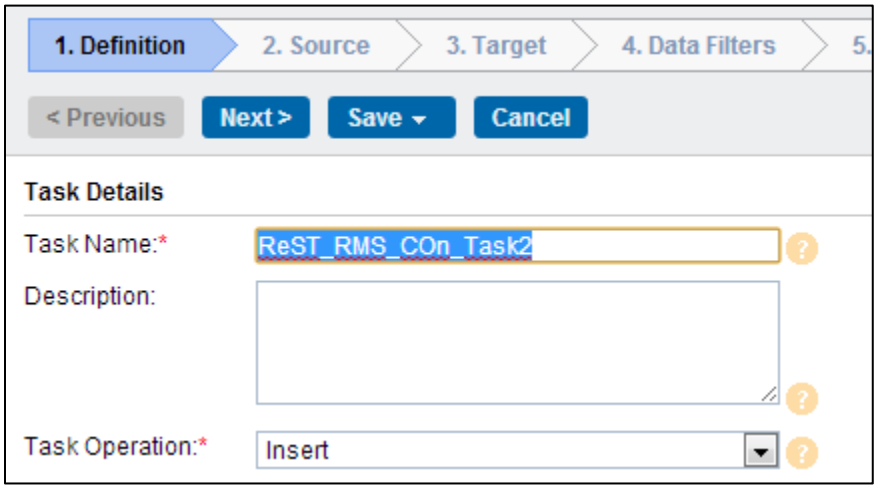

Figure 10: Definition tab

6. Specify the **Task Name**, provide a **Description** and select the Task Operation **Insert**.
7. Click **Next**.
8. The **Source** tab appears.

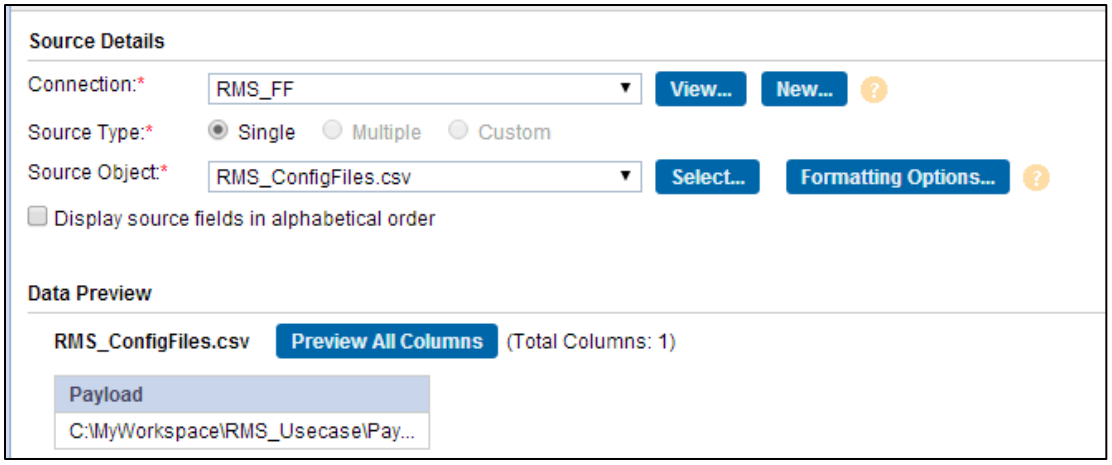

Figure 11: Source Tab

9. Select the source **Connection**, **Source Type** and **Source Object** to be used for the task.
10. Click **Next**.
11. The **Target** tab appears.
12. Select the target **Connection** and **Target Object** required for the task.

Figure 12: Target Tab

13. Click **Next**.
14. In **Data Filters** tab by default, Process all rows is chosen. Refer Data Filters to assign filters to fetch specific data,
15. Click **Next**.

16. In **Field Mapping** tab, map source fields to target fields accordingly.

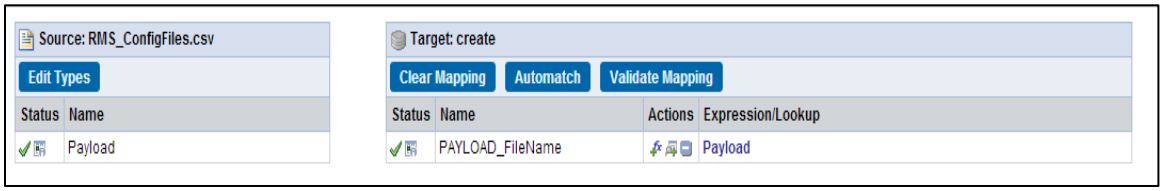

Figure 13: Field Mapping Tab

17. Click **Next**.
18. The **Schedule** tab appears.
19. Click **Save and Run** If you do not want to schedule the task.

Note: In Schedule tab, you can schedule the task as per the requirement and save.

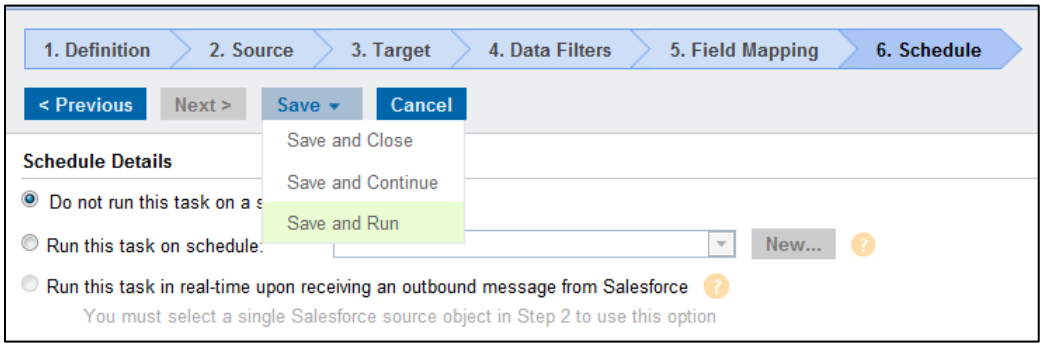

Figure 14: Save and Run the Task

After you **Save and Run** the task, you will be redirected to monitor log page. In monitor log page, you can monitor the status of data synchronization tasks.

Data Filters

Data filters help you to fetch specific data of a particular object. The DSS task will process the data based on the filter field assigned to the object.

The following steps help you to use data filters.

1. In Data synchronization task, select **Data Filters** tab.
2. The Data Filters tab appears.
3. Click **New** as shown in the figure below.

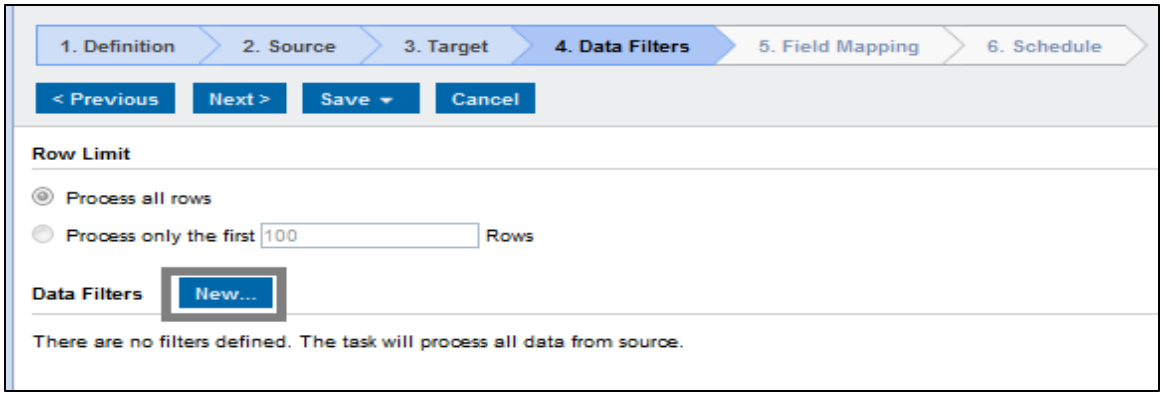

Figure 15: Data Filters -1

4. The Data Filter dialog box appears.

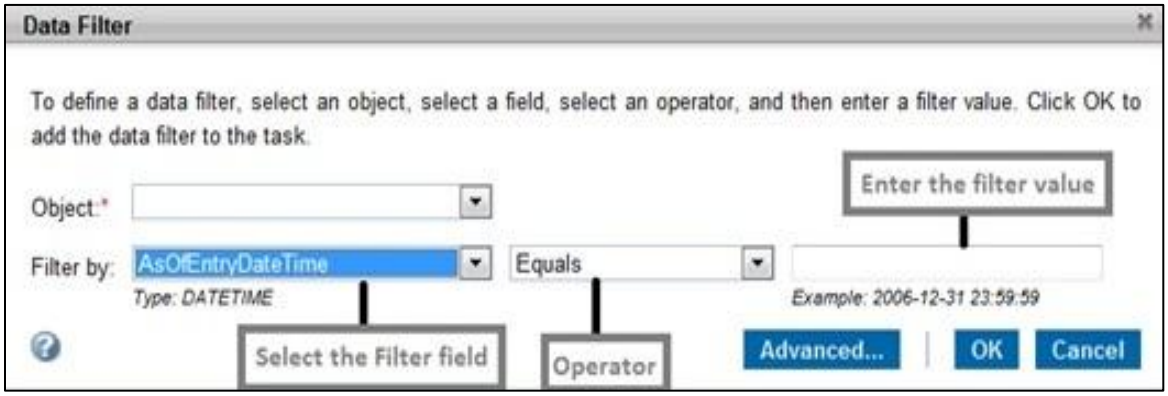

Figure 16: Data Filters-2

5. Specify the following details.

Field Type	Description
Object	Select Object for which you want to assign filter fields.
Filter By	Select the Filter Field.
Operator	Select Equals operator.
Filter Value	Enter the Filter value.

6. Click **Ok**.

Note: Advanced Data filter is not supported by Rest Connector.

Known Future Enhancements and Current Issues

1. **CLOB, BLOB or base64Encode data** field attached to the ReST table is not supported.
2. **Big Data fields** will be supported in the future release.
3. If you click **Refresh Field**s after creating DSS tasks, you will see a change in number of fields. This happens because the xml (or) JSON response from same end point (with same filter condition) fetches different result for second URL hit.
4. Lookup in the field mapping tab is not supported.

Recommendations

Follow the given recommendations to optimize the connector functionality efficiently.

1. It is recommended to give the **Url request parameter**, **Form request parameters** and **Header request parameters** such that it fetches maximum data from ReST endpoint Server. This allows the connector to analyze and store more metadata.
2. It is recommended to go for JSON based response, as it is proven more stable when the same endpoint supports both xml and JSON based responses.
3. Use the **Sample Response Xml or Jason File** field to manually control the metadata .
4. Any manual change in the file will change the list of Tables (records) or the Fields once you click **Refresh Fields**.

Incorporating Custom Authentication

Business Use case

ReST endpoint or server use authentication other than OAuth, Basic, Digest, and other out-of-box authentication.

ReST Connector Custom Function

Custom Authentication allows you to implement your own authentication logic. Custom Authentication function provides a pre-defined java template to implement custom authentication logic.

Note: If you want the Informatica to create the Custom Authentication for you, then contact Sales team or Informatica Cloud API Response Team team or Customer Service

The following section explains the significance of Custom Authentication Java Template:

- The Java template is shared with the user on request.
- You must contact the Sales team or Informatica Cloud API Response Team team or Customer Service to get the java template.
- The Java Template is a Class. The name of the Class is **CustomAuth.java**. You must not change the name of the Class.

- The CustomAuth should be in package **com.informatica.cloudlabs.adapter.rest.CustomAuth .**

Follow the given steps to deploy the Ja**r** fil**e:**

1. Create a separate jar out of **CustomAuth.java.**
2. Follow the **CustomAuth_<UserCompanyName/EndpointName>.jar** format to name the file
3. Stop the Informatica Cloud Secure agent Service Before deployment of the jar.
4. Copy the created Jar in the following Informatica secure agent path.
   - ***C:\Program Files\Informatica Cloud Secure Agent\main\bin\rdtm\javalib\<Plugin-Id>***
   - ***C:\Program Files\Informatica Cloud Secure Agent\main\tomcat\plugins\<Plugin-Id>***
5. Start the Informatica Cloud Secure agent services.

The technical details of **CustomAuth.java** are discussed below.

1. There is a method, an Inner Class and an Enum defined in this template.

Method	Method signature is **String GetCustomAuthParams(RequestInfo , Ilogger)**
RequestInfo	A bean class that captures all the connection UI parameters
Inner Class	Bean class
Enum	Defines the types of parameter present in Custom Authentication

2. You need to include new Form, Url or Header parameter Irrespective of type of Authentication to implement custom authentication.
3. User needs to implement a method called **GetCustomAuthParams().**
4. The method signature is **String response GetCustomAuthParams(RequestInfo,Ilogger).**
5. There is inner class called **CustomParams**.
6. The return value is always a vector of **CustomParams Objects**.
7. Define Custom Parameter you need to set as an instance of this class.
8. Set all the bean method values to use the Custom Parameter.
9. There is an enum in the CustomAuth class called **enumParamType.**
10. The enum is used for categorizing a given CustomParam to URL, Form or Header.

The figure given below displays the code discussed the section.

```
 */
@Override
public String GetCustomAuthParams(RequestInfo reqInfo,ILogger ilogger) throws Exception{

    String methodName = "GetCustomAuthParams";
    if (ilogger != null) {
        ilogger.logMessage(clazz_Name, methodName, ELogMsgLevel.INFO,
                "Entered the CustomAuth Class and Method GetCustomAuthParams !!!");
    }
    Map<String, String> mapURLRequestParams                =       reqInfo.getMapUrlRequestParams();
    Map<String, String> mapFormRequestParams               =       reqInfo.getMapFormRequestParams();
    Map<String, String> mapHeaderRequestParams             =       reqInfo.getMapHeaderRequestParams();

    String sURLRequestParams                =       null;
    Vector<CustomParams> vcCustomParams =   new Vector<CustomAuthImpl_BlueGreen.CustomParams>();
    String      sPublicKey              =   null;
    String      sPrivateKey             =   null;
    String method                       =   null;
    String      sEndpointUrl            =   reqInfo.getBaseUrl();
    String response=null;
    //Added to call custom auth additional params list
    //Start
    String absolutePath;
    File propFile=null;
    try {
        if(reqInfo.getConfigKeyOrPrivateKeyFileName()!=null && !reqInfo.getConfigKeyOrPrivateKeyFileName().equalsIgnoreCase(RESTConstants.EMPTY_STRING)){
            propFile=new File(reqInfo.getConfigKeyOrPrivateKeyFileName());
        }else{
            absolutePath = RESTRegistrationInfo.class.getProtectionDomain().getCodeSource().getLocation().toURI().getPath();
            if(absolutePath!=null && !absolutePath.equalsIgnoreCase(RESTConstants.EMPTY_STRING)){
                absolutePath = absolutePath.substring(0, absolutePath.lastIndexOf("/"));
                propFile=new File(absolutePath+"/"+RESTConstants.CONFIG_FILE_NAME);
            }else{
                throw new FatalRuntimeException("Could not able to read the config file !! Please check the file path!!");
            }
```

Troubleshooting configuration issues

The log and exception messages thrown while configuring the DSS tasks are captured in the log files. These log files are saved in specific location**.**

For example, C:\Program Files\Informatica Cloud Secure Agent\main\tomcat\log\<connectorname><date & time stamp>.

The log file name is the connector name appended with time stamp.

Troubleshooting Data Synchronization Task (DSS)

While creating DSS task, the “NULL” error message appears when a connector with invalid configuration is selected. The null error message files are saved in specific location.

For example, C:\Program Files\Informatica Cloud Secure Agent\main\tomcat\log\<connectorname><date & time stamp>.

The log and exception details of a failed DSS task are captured in the **Session Log.**

Note: You need special permission privileges to run the application in debug mode.

Increasing Secure Agent Memory

To overcome memory issues faced by secure agent follow the steps given below.

1. In Informatica Cloud home page, click **Configuration**.
2. Select **Secure Agents**.
3. The secure agent page appears.
4. From the list of available secure agents, select the secure agent for which you want to increase memory.
5. Click **pencil** icon corresponding to the secure agent. The pencil icon is to edit the secure agent.
6. The Edit Agent page appears.
7. In **System Configuration** section, select the **Type** as “**DTM**”.
8. Edit **JVMOption1** as “**-Xmx512m**” as shown in the figure below.

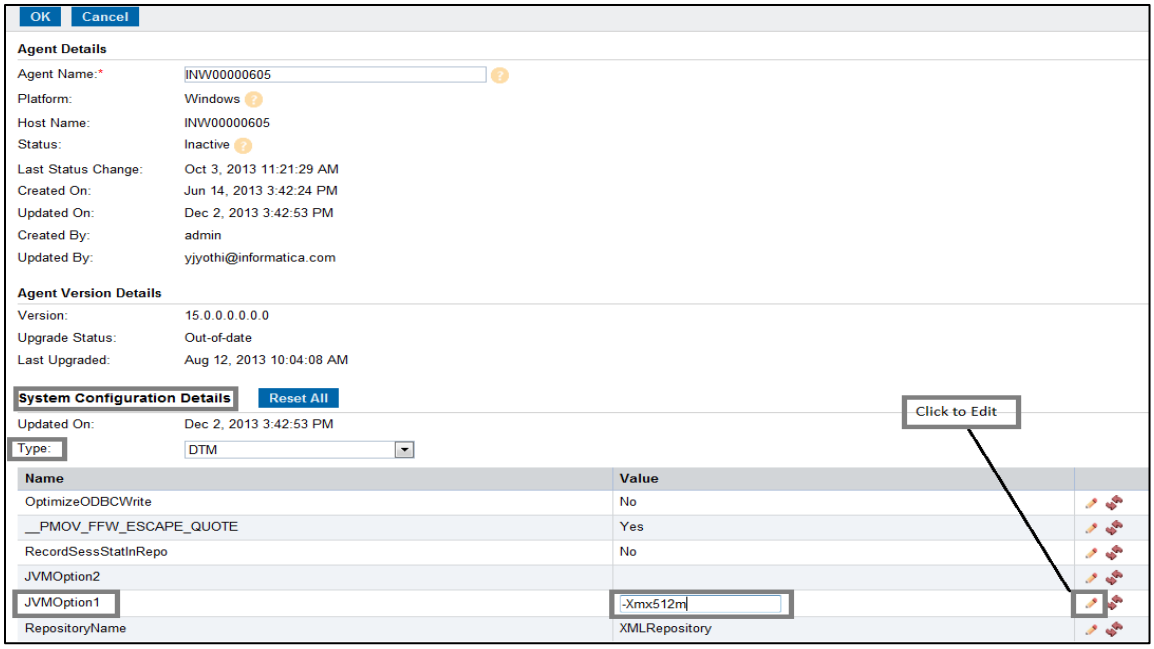

Figure 11. Increasing Secure Agent Memory-1

9. Again in **System Configuration** section, select the **Type** as "**TomCatJRE**".
10. Edit **INFA_memory** as "**-Xms256m -Xmx512m**" as shown in the figure below.

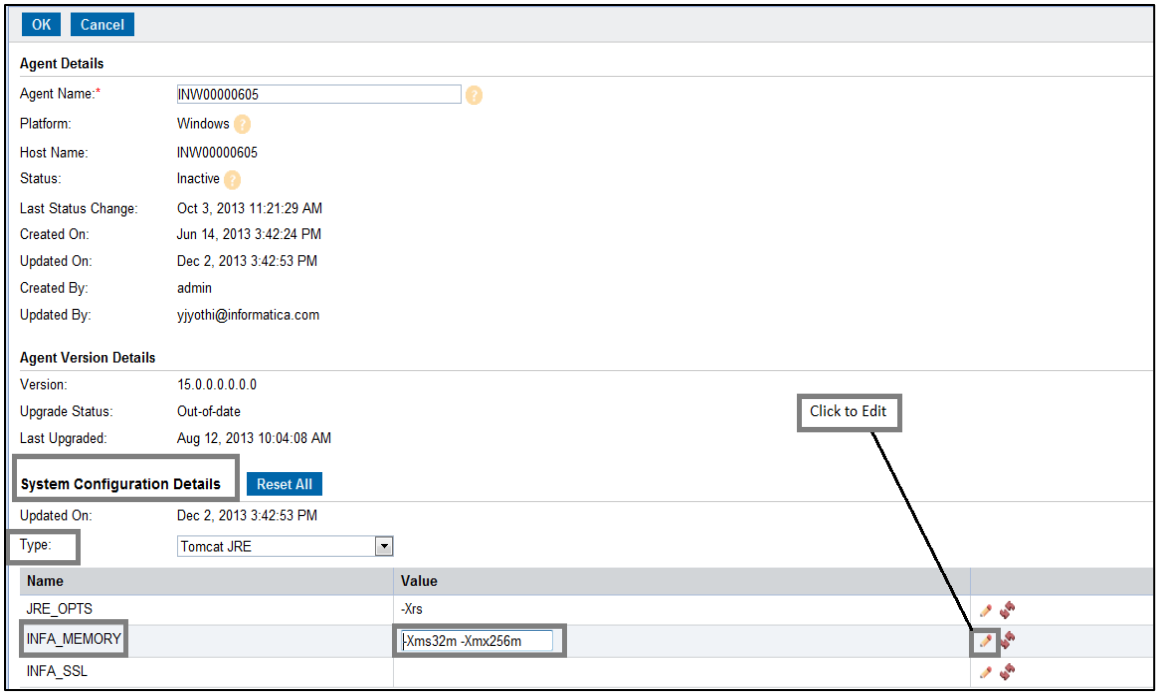

Figure 17: Increasing Secure Agent memory

11. Restart the secure agent.

The secure agent memory has been increased successfully.