How-To Library

Informatica

Configuring AWS KMS Customer Master Key to Encrypt Files in Amazon S3

Abstract

You can enable client-side or server-side encryption to encrypt data inserted in Amazon S3 buckets to protect data. You can generate a customer master key in AWS Key Management Service (AWS KMS) and configure the key in Amazon S3 connection properties to encrypt data. This article describes the guidelines and steps to configure AWS KMS customer master key for Informatica Cloud Amazon S3 Connector.

Supported Versions

- Informatica Cloud® Fall 2016 December

Table of Contents

Overview. 2

Generate a Customer Master Key in AWS Key Management Service (AWS KMS). 2

Enable Client-side Encryption 3

Create an Amazon S3 Connection. 3

Create a Data Synchronization Task. 3

Overview

You are a data administrator and your organization has stored huge volumes of data in a relational database. You want to collate legacy sales data to track the overall growth trend in sales from the relational database and archive it on Amazon S3. In addition, you want to secure the legacy data of your organization to avoid random access by unauthorized persons. You can enable Client-side encryption using the customer master key to encrypt data. You can read data from the relational database and use Amazon S3 Connector to upload data to Amazon S3.

You can configure AWS KMS customer master key to encrypt data to Amazon S3. You can specify a customer master key while creating an Amazon S3 connection. The Customer master key offers more control and permissions on the key to control who can use or manage the key.

Perform the following tasks to configure AWS KMS customer master key to encrypt data:

1. Generate a customer master key in AWS Key Management Service.
2. Create an Amazon S3 connection.
3. Create a Data Synchronization task.

Generate a Customer Master Key in AWS Key Management Service (AWS KMS)

Create a customer master key using the IAM section of the AWS Management Console. Generate the customer master key for the same region where your Amazon S3 bucket resides. When you generate a customer master key, you can specify either **Customer generated customer master key** or **Default customer master key** values. In this example, use the **Customer generated customer master key** value.

For more information about how to generate the customer master key in AWS Management Service (AWS KMS), see http://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html
For example, create the customer master key 11112222333 for US East (N. Virginia) region, where your S3 bucket is available.

Enable Client-side Encryption

An organization administrator must perform the tasks to enable client-side encryption. You must update the security policy .jar files on each Secure Agent machine in the runtime environment.

Update the `local_policy.jar` and the `US_export_policy.jar` files in the following directory:

```
<Secure Agent installation directory>\jre\lib\security.
```

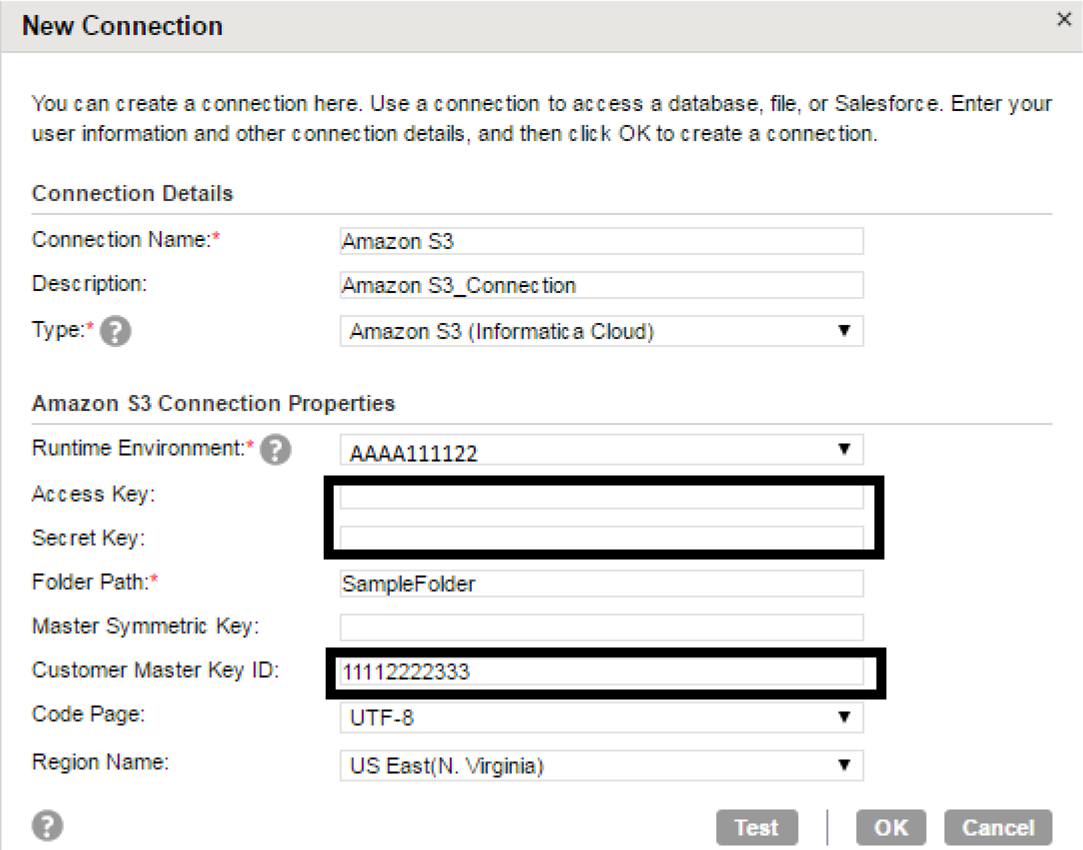
You can download the .jar files supported by the JAVA environment on the Secure Agent machine from the Oracle website.

Create an Amazon S3 Connection

Create an Amazon S3 connection and specify the connection properties to configure AWS KMS customer master key.

When you create an Amazon S3 connection, do not provide Access Key and Secret Key if you want to configure AWS IAM authentication.

The following image shows the Amazon S3 connection properties:



New Connection

You can create a connection here. Use a connection to access a database, file, or Salesforce. Enter your user information and other connection details, and then click OK to create a connection.

Connection Details

Connection Name:*	Amazon S3
Description:	Amazon S3_Connection
Type:*	Amazon S3 (Informatica Cloud)

Amazon S3 Connection Properties

Runtime Environment:*	AAAA111122
Access Key:	
Secret Key:	
Folder Path:*	SampleFolder
Master Symmetric Key:	
Customer Master Key ID:	11112222333
Code Page:	UTF-8
Region Name:	US East(N. Virginia)

Create a Data Synchronization Task

Before you create a Data Synchronization task, create an Oracle connection to read data from the Oracle source.

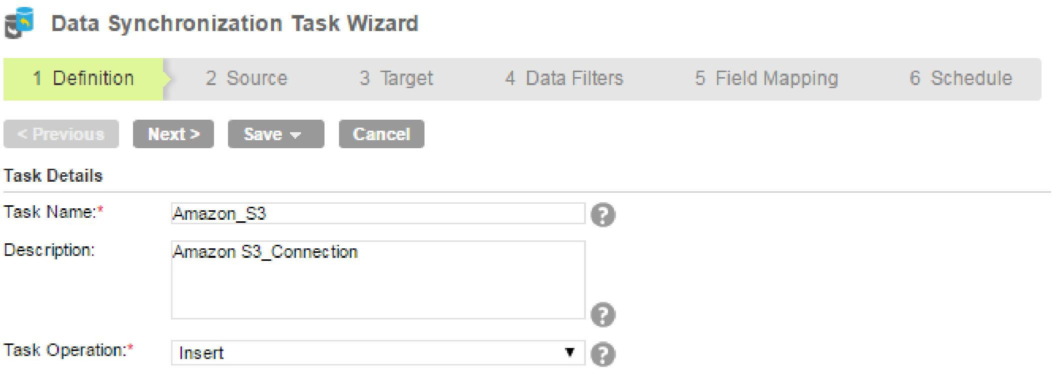
1. Click **Task Wizard** on the Informatica Cloud home page.
2. Select **Data Synchronization** from the menu.

The **Data Synchronization** page appears.

3. Click **New**.

   The **Definition** tab appears.

4. Provide the task details. The following image shows sample task details:



Data Synchronization Task Wizard

Task Details

Task Name:* Amazon_S3

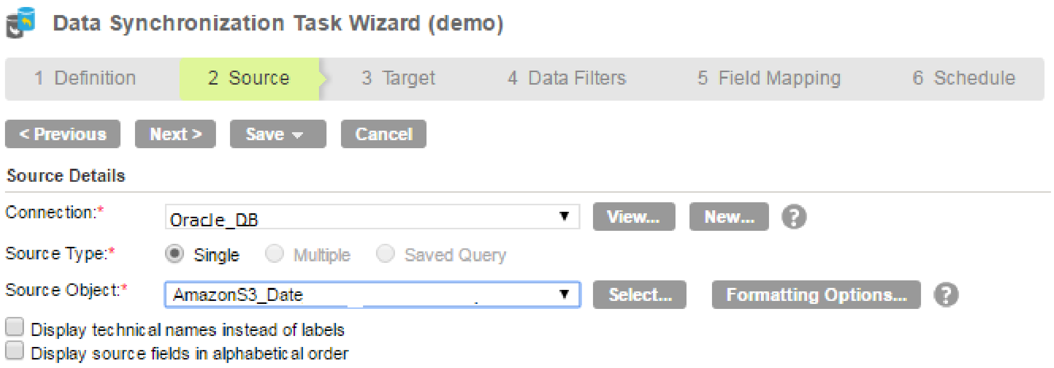
Description: Amazon S3_Connection

Task Operation:* Insert

5. Click **Next**.

   The **Source** tab appears.

6. Provide source details to read data from Oracle source. The following image shows sample source details:



Data Synchronization Task Wizard (demo)

Source Details

Connection:* Oracle_DB

Source Type:* ● Single ○ Multiple ○ Saved Query

Source Object:* AmazonS3_Date

□ Display technical names instead of labels

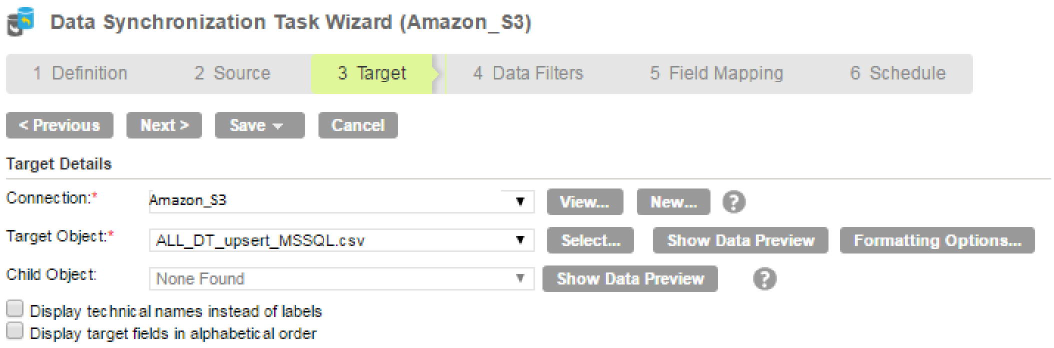
□ Display source fields in alphabetical order

7. Click **Next**.

   The **Target** tab appears.

8. Select the target **Connection** and **Target Object** required for the task.

   The following image shows sample target details:



Data Synchronization Task Wizard (Amazon_S3)

Target Details

Connection:* Amazon_S3

Target Object:* ALL_DT_upsert_MSSQL.csv

Child Object: None Found

□ Display technical names instead of labels

□ Display target fields in alphabetical order

9. Click **Next**.

   The **Data Filters** tab appears in which, Process all rows is chosen by default.

10. Click **Next**.

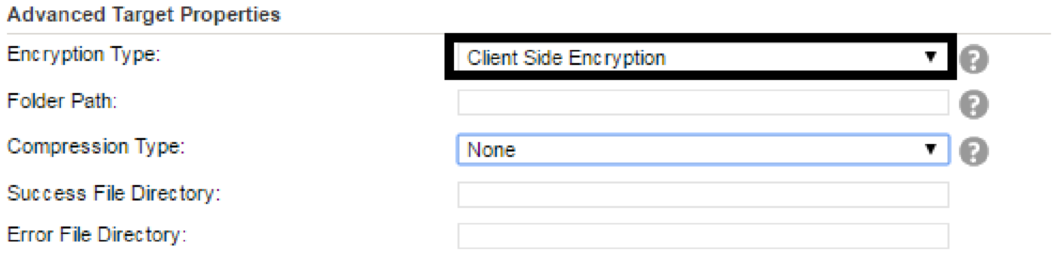
    In the **Field Mapping** tab, map source fields to target fields accordingly.

11. Click **Next**.

    The **Schedule** tab appears where you can schedule the task for each requirement and save.

12. Provide appropriate values in the **Advanced Target Properties**. You must select the **Encryption Type** as **Client Side Encryption**.

    The following image shows sample advanced target properties details:



Advanced Target Properties

Encryption Type: Client Side Encryption

Folder Path:

Compression Type: None

Success File Directory:

Error File Directory:

13. Click **Save and Run** to run the Data Synchronization task.

    When you run the task, the Secure Agent uses algorithm and keys defined by AWS KMS to encrypt data. To verify that the encryption using the customer master key has taken place, you can check the session log for the job. Click **Monitor** > **Activity Log** to view the session log for jobs.

    The session log contains the following message if the task completed successfully:

```
The agent successfully connected to Amazon S3 with client-side encryption support.
```

Authors

Subhashree Salam

Chanchal Das

Madhuri Veluri