



Configuring a secure connection to the SAP HANA server from CloudData Integration

[®] Copyright Informatica LLC 2021, 2025. Informatica, Informatica Cloud, and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html.

Abstract

You can use the SSL protocol to configure a secure connection to the SAP HANA server from Cloud Data Integration. This article describes how to configure the Secure Agent for SSL communication with SAP HANA and SAP Datasphere.

Supported Versions

• Informatica[®] Cloud Data Integration

Table of Contents

| Overview | 2 |
|--|----|
| Prerequisites | 2 |
| SSL configuration for the Secure Agent | 2 |
| Configuring an SSL connection on Windows | 3 |
| Configuring an SSL connection on Linux | 9 |
| Additional resources | 10 |

Overview

You can use the Secure Socket Layer (SSL) protocol to configure a secure connection to the SAP HANA server from Cloud Data Integration.

SAP HANA supports OpenSSL and the SAP Cryptographic Library to enable a secure connection through SSL. Data Integration uses the OpenSSL standard to enable a secure connection through SSL.

When you configure a secure connection through SSL, you can use this secure connection to read from or write to SAP HANA. You can also use this secure connection when you read from or write to SAP Datasphere.

For more information about the SAP Datasphere service, see <u>SAP Datasphere</u> in the SAP documentation.

Prerequisites

Before you configure the Secure Agent for SSL communication, you need to perform certain prerequisite tasks.

- 1. Install the OpenSSL libraries on the SAP HANA server.
- 2. Configure the SAP HANA server for SSL communication and restart the SAP HANA server for the configuration changes to take effect.

For information about configuring and restarting the SAP HANA server, see the SAP documentation.

3. On the SAP HANA server machine, generate the key.pem and trust.pem certificate files.

For more information about how to connect to SAP HANA databases in the cloud, see Connecting to the SAP HANA database in SAP HANA Cloud in the SAP documentation.

SSL configuration for the Secure Agent

After you configure the SAP HANA server for SSL communication, you can configure the Secure Agent for SSL communication with the SAP HANA server.

The SSL configuration steps differ based on whether the Secure Agent machine is a Windows machine or a Linux machine.

Configuring an SSL connection on Windows

Before you configure the Secure Agent for SSL communication, you must configure the Secure Agent machine to trust the SAP HANA server certificate.

For information about managing the trusted root certificates for the Secure Agent machine, see Manage Trusted Root Certificates.

On Windows, perform the following steps to configure the Secure Agent for SSL communication:

- 1. Create a Java KeyStore certificate in the Secure Agent machine.
- 2. Import the trust.pem certificate file to the Secure Agent machine where you want to configure a secure connection.
- Configure the metadata and run-time properties in the SAP HANA connection to use the SSL connection on Windows.

Create a Java KeyStore certificate

You must create a KeyStore certificate that contains all the client certificates to establish an SAP HANA connection in the Secure Agent machine.

Perform the following steps to create a KeyStore certificate for the SAP HANA connection:

- 1. Create a container that stores the KeyStore certificate in the machine.
- 2. To create a Java KeyStore file, run the following command:

```
keytool -genkey -alias mykeystore -keyalg RSA -keystore .keystore -keysize <key size in
bits> -dName "CN=<common name>, OU=<organization unit>, O=<organization>, C=<country>"
```

3. When prompted, enter the password for the destination KeyStore.

Important: Make a note of this password. You need to specify this password while importing the root certificate for the KeyStore container that you created.

4. To import the root certificate, run the following command:

```
keytool -v -importcert -alias myrootcert -file <SAP HANA certificate name with path> -
keypass <password of the keystore file> -keystore .keystore -storepass <password for
truststore>
```

5. To verify whether the root certificate is created, run the following command:

keytool -list -v -keystore .keystore -storepass <password for truststore>

Install the ODBC driver

After you create the root certificate in the Secure Agent machine, you must import the trust.pem certificate file to trust the SAP HANA server certificate and install the ODBC driver for the SAP HANA server on the Secure Agent machine.

1. Click Start, type mmc in the Search box, and press Enter.

The Console window appears.

2. Click File > Add/Remove Snap-in.

The Add/Remove Snap-ins window appears.

3. From the Available snap-ins list, select Certificates, and then click Add.

| | Veedee | | 1 | Console Root | Edit Extensions |
|-----------------------|---------------|---|-------|--------------|-------------------|
| hap-in | vendor | | | | Edit Extensions |
| ActiveX Control | Microsoft Cor | | | | Remove |
| Authorization Manager | Microsoft Cor | | | | |
| Certificates | Microsoft Cor | Ξ | | | |
| Component Services | Microsoft Cor | | | | Move Up |
| Computer Managem | Microsoft Cor | | | | Move Down |
| Device Manager | Microsoft Cor | | Add > | | Liste Domi |
| Disk Management | Microsoft and | | | | |
| Event Viewer | Microsoft Cor | | | | |
| Folder | Microsoft Cor | | | | |
| Group Policy Object | Microsoft Cor | | | | |
| IP Security Monitor | Microsoft Cor | | | | |
| IP Security Policy M | Microsoft Cor | | | | |
| Link to Web Address | Microsoft Cor | - | | | Ad <u>v</u> anced |
| cription: | | | | | |

4. Click Computer account, and then click Next.



5. Click Local computer, and then click Finish.

| Select Computer | X | |
|--|---|---|
| Select the computer you want | t this snap-in to manage. | |
| This snap-in will always mar Local computer: (the computer) | lage: omputer this console is running on) | |
| Another computer: | Browse | |
| Allow the selected com only applies if you save | puter to be changed when launching from the command line. This the console. | |
| | | |
| | | |
| | | |
| | | _ |
| | < <u>B</u> ack Finish Cancel |] |

6. Click OK.

The **Certificates** snap-in is added to the console tree.

7. In the console tree, double-click **Certificates**.

8. Right-click the Trusted Root Certification Authorities store, and then click All Tasks > Import.

| 🚡 Console1 - [Console Root\Certificates (l | .ocal Comp | uter)\Trusted Root Cer | tificati | on Authorities] |
|--|------------|------------------------|----------|-------------------|
| 🚡 File Action View Favorites Wi | ndow He | lp | | |
| 🗢 🔿 🔁 📰 📋 🗖 🕞 | ī | | | |
| 📔 Console Root | | Object Type | | |
| a 📮 Certificates (Local Computer) | | Certificates | | |
| Personal | | | | |
| Trusted Root Certification | Find Carti | ficator | | |
| Enterprise Trust | Find Certi | incates | | |
| Intermediate Certification | All Tasks |) | • | Find Certificates |
| Trusted Publishers | | | | |
| Untrusted Certificates | View |) | | Import |
| Third-Party Root Certificati | New Wine | dow from Here | | |
| Trusted People | | | | |
| Remote Desktop | New Task | pad View | | |
| Certificate Enrollment Requ | Refresh | | | |
| Smart Card Trusted Roots | E III | | | |
| SMS | Export Lis | t | | |
| Trusted Devices | Help | | | |
| | | | | |

The Certificate Import Wizard appears.

9. Click Next.



The File to Import dialog box appears.

10. Click Browse to import the trust.pem certificate file.

| Certificate Import Wizard |
|--|
| File to Import Specify the file you want to import. |
| Eile name: |
| Note: More than one certificate can be stored in a single file in the following formats: |
| Personal Information Exchange-PKCS #12 (.PFX,.P12) |
| Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) |
| Microsoft Serialized Certificate Store (.SST) |
| Learn more about <u>certificate file formats</u> |
| < <u>B</u> ack <u>N</u> ext > Cancel |

Note: By default, the wizard does not display the trust.pem certificate file. To view the file, click the file type list and select All Files.

11. Select the trust.pem certificate file, and then click **Open** to import the file.

12. Verify if the ODBC driver is installed in the Secure Agent machine.

| Name | | 1 | | | | |
|-------------|---------------|---------------|-------------|------------------------|-----------|---|
| | | Version | Company | File | Date | - |
| DataDirect | t CLOSED 8 | 8.00.02.2336 | Informatica | DWORA28.DLL | 8/25/2021 | |
| DataDirect | t CLOSED 8 | 8.00.02.2336 | Informatica | DWORA28.DLL | 8/25/2021 | |
| DataDirect | t CLOSED 8 | 8.00.02.381 | Informatica | DWSQLS28.DLL | 8/25/2021 | |
| DataDirect | t CLOSED 8 | 8.00.02.447 | informatica | DWSQLS28.DLL | 8/25/2021 | |
| HDBODBO | 8 | 2.01.51.58262 | SAP SE | LIBODBCHDB.DLL | 7/27/2017 | |
| HDBODBO | C_002 | 2.01.51.58262 | SAP SE | LIBODBCHDB.DLL | 7/27/2017 | |
| nformatica | a Cassandra | 2.06.08.1008 | Simba Tec | CASSANDRAODBC_SB64.DLL | 8/18/2021 | |
| nformatica | a Data Servic | 9.01.00.00 | Informatica | INFADSODBC.DLL | 3/9/2011 | |
| nformatica | a Data Servic | Not marked | Not marked | INFADSODBC.DLL | | |
| Informatica | a Data Servic | 10.05.01.00 | Informatica | INFADSODBC.DLL | 8/18/2021 | • |

Configure SSL in the SAP HANA connection

After you import the trust.pem certificate file and install the ODBC driver, you must configure the metadata and runtime properties in the SAP HANA connection to use the SSL connection on Windows.

To use the SSL connection in Cloud Data Integration, configure the following properties:

- Metadata Advanced Connection Properties: encrypt=true&truststore=/<path of the keystore file>/.keystore&truststorepassword=<password of the keystore file>
- Run-time Advanced Connection Properties: encrypt=1;sslCryptoProvider=openssl;sslKeyStore=/<path of the key.pem file>;sslTrustStore=/<path of the trust.pem certificate file>;sslValidateCertificate=true

Configuring an SSL connection on Linux

On Linux, you must define the SSL configuration properties in the SAP HANA connection to establish a secure connection to the SAP HANA server from Cloud Data Integration.

- 1. Install the OpenSSL libraries on the client machine.
- 2. Create a Java KeyStore certificate in the Secure Agent machine.
- 3. Copy the SAP HANA server certificate files to the Secure Agent machine.
- 4. Configure the metadata and run-time properties in the SAP HANA connection to use the SSL connection on Linux.

Install the OpenSSL libraries

Install the OpenSSL libraries on the Secure Agent machine where you want to configure a secure connection to the SAP HANA server.

- 1. Install the OpenSSL libraries and the soft link for the libssl.so file.
- 2. Define the LD_LIBRARY_PATH library path environment variable on Linux.
- Set the LD_LIBRARY_PATH library path environment variable to the directory where the OpenSSL libraries are installed.
- 4. Restart the Secure Agent to reflect the changes.

Copy the SAP HANA server certificate files to the Secure Agent machine

Access the SAP HANA server and download the trust.pem and key.pem certificate files. Copy the certificate files to the Secure Agent machine where you want to configure a secure connection.

Create a Java KeyStore certificate

You must create a KeyStore certificate that contains all the client certificates to establish an SAP HANA connection in the Secure Agent machine.

Perform the following steps to create a KeyStore certificate for the SAP HANA connection:

- 1. Create a container that stores the KeyStore certificate in the machine.
- 2. To create a Java KeyStore file, run the following command:

keytool -genkey -alias mykeystore -keyalg RSA -keystore .keystore -keysize <key size in bits> -dName "CN=<common name>, OU=<organization unit>, O=<organization>, C=<country>"

3. When prompted, enter the password for the destination KeyStore.

Important: Make a note of this password. You need to specify this password while importing the root certificate for the KeyStore container that you created.

4. To import the root certificate, run the following command:

```
keytool -v -importcert -alias myrootcert -file <SAP HANA certificate name with path> -
keypass <password of the keystore file> -keystore .keystore -storepass <password for
truststore>
```

5. To verify whether the root certificate is created, run the following command:

keytool -list -v -keystore .keystore -storepass <password for truststore>

Configure SSL in the SAP HANA connection

Configure the metadata and run-time properties in the SAP HANA connection to use the SSL connection on Linux.

To use the SSL connection in Cloud Data Integration, configure the following properties:

- Metadata Advanced Connection Properties: encrypt=true&truststore=/<path of the keystore file>/.keystore&truststorepassword=<password of the keystore file>
- Run-time Advanced Connection Properties: encrypt=1;sslCryptoProvider=openssl;sslKeyStore=/<path of the key.pem file>;sslTrustStore=/<path of the trust.pem certificate file>;sslValidateCertificate=true

Additional resources

For more information about the SAP HANA security configuration, see SAP HANA Security Guide for SAP HANA Platform.

Author

Anirban Biswas

Acknowledgements

The author would like to acknowledge Kanika Agarwal and P. Sansha for their technical assistance with this article.