How-To Library

Informatica

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

# 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

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 SAP Datasphere 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.
3. 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

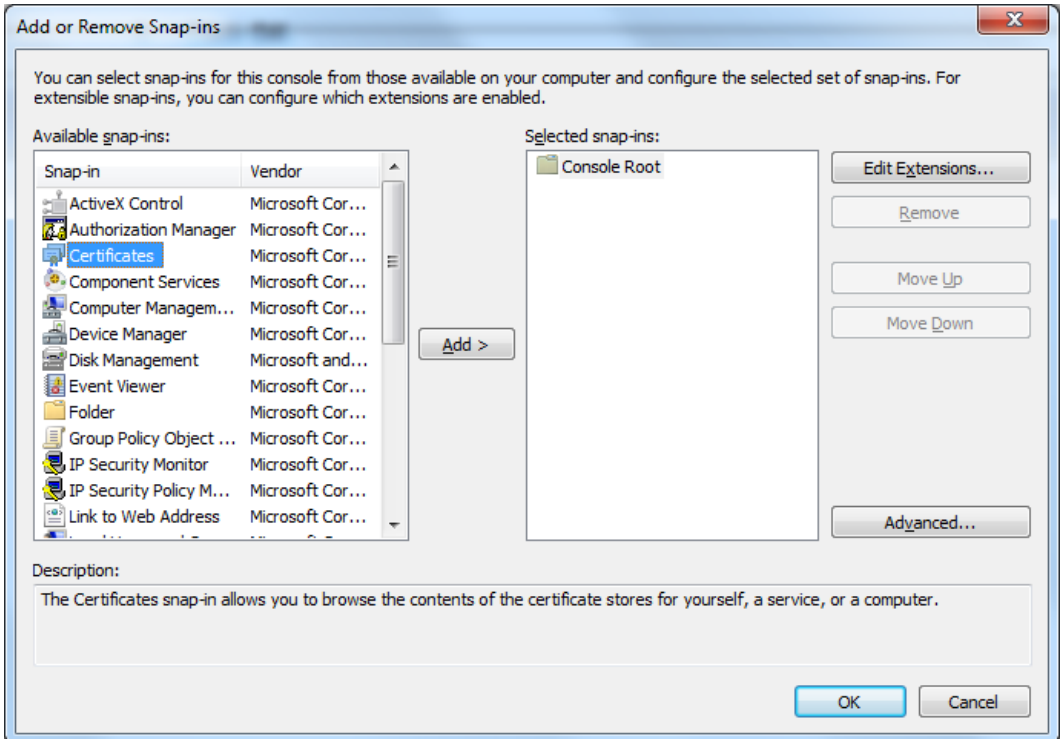
After you create the root certificate in the Secure Agent machine, you must import the `trust.pem` certificate file to trust the SAP HANA server certificate and install the ODBC driver for the SAP HANA server on the Secure Agent machine.

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

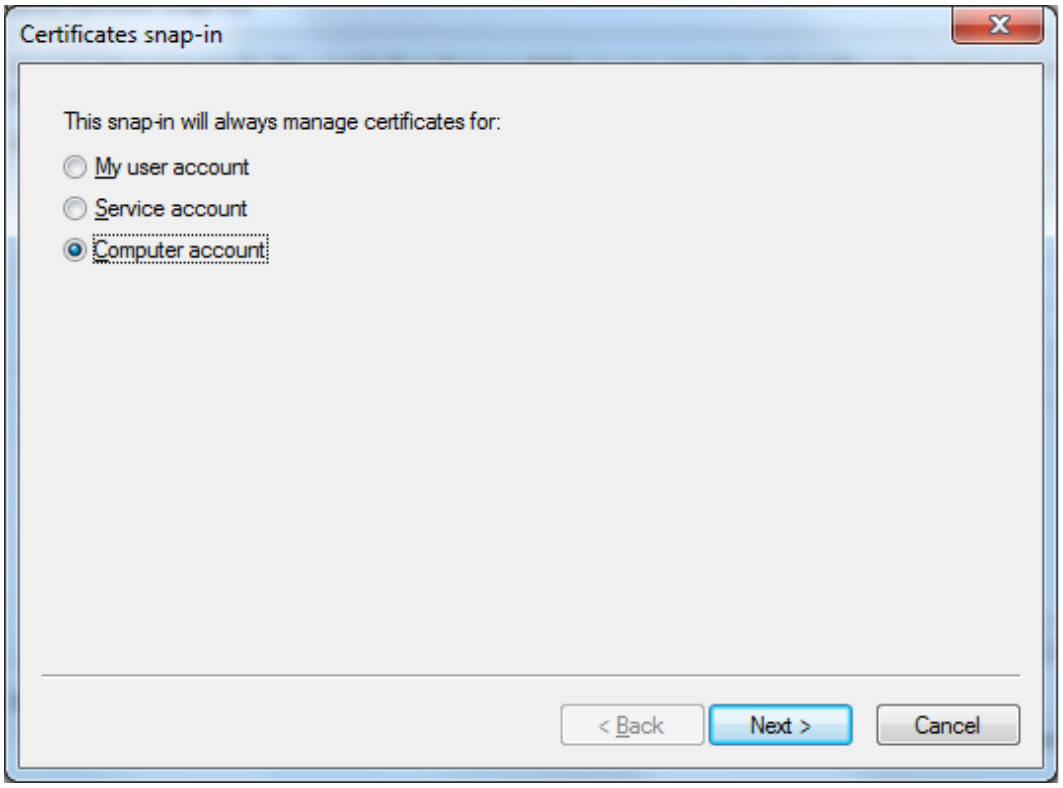
   The **Console** window appears.
2. Click **File** > **Add/Remove Snap-in**.

   The **Add/Remove Snap-ins** window appears.

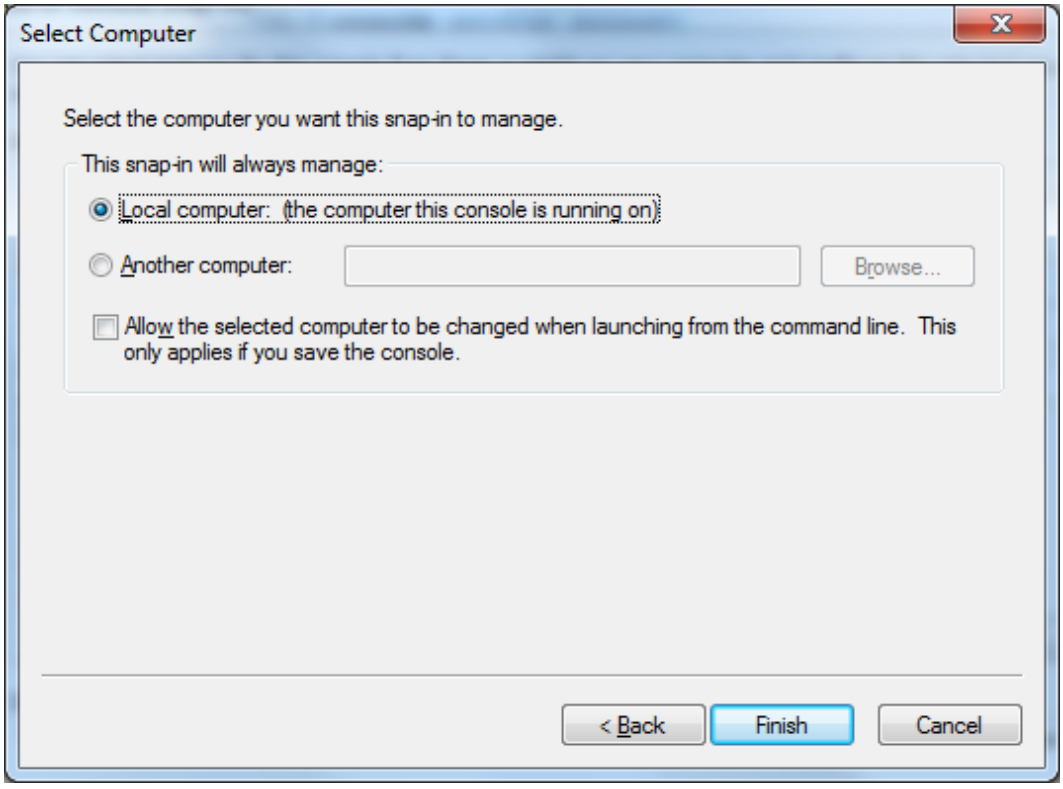
3. From the **Available snap-ins** list, select **Certificates**, and then click **Add**.




4. Click **Computer account**, and then click **Next**.

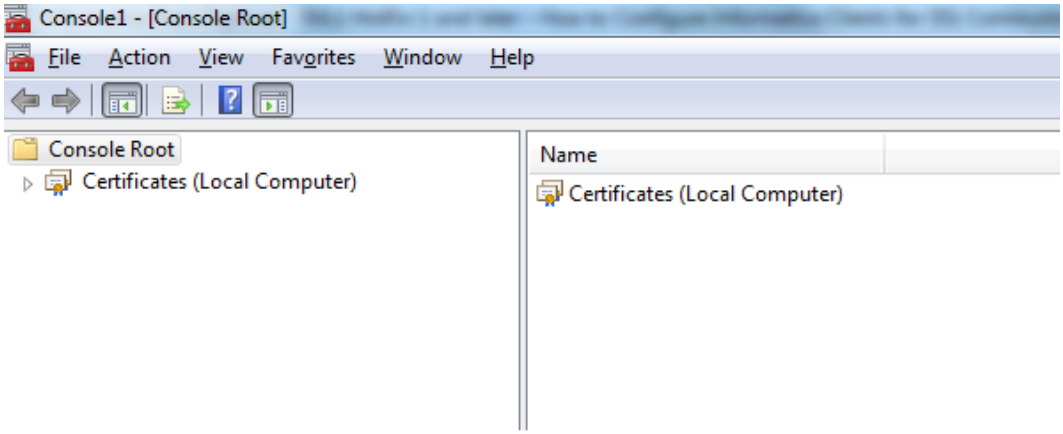


5. Click **Local computer**, and then click **Finish**.



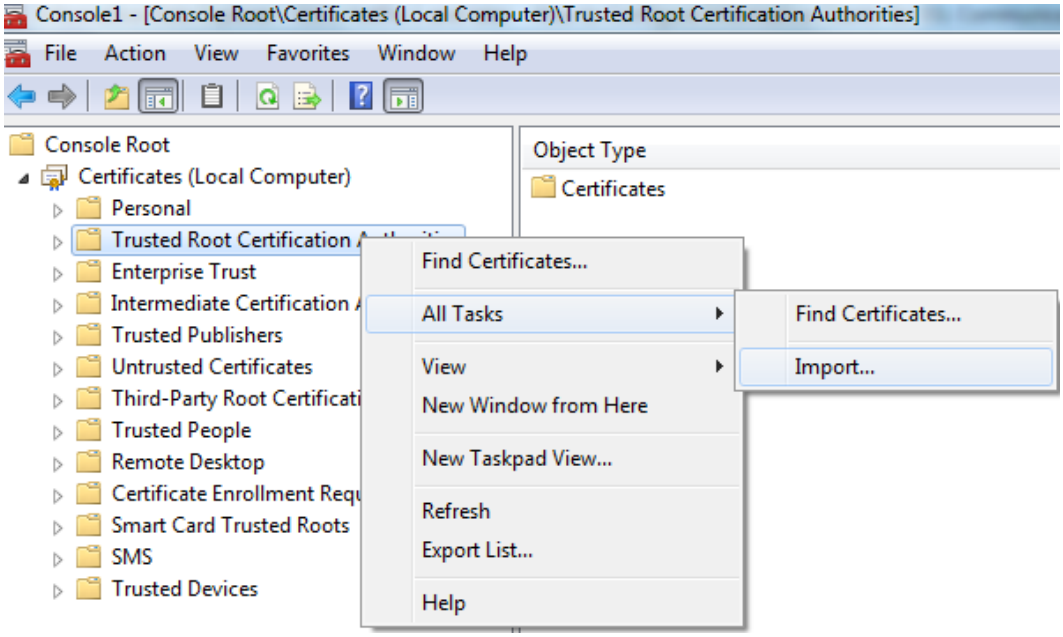

6. Click **OK**.

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



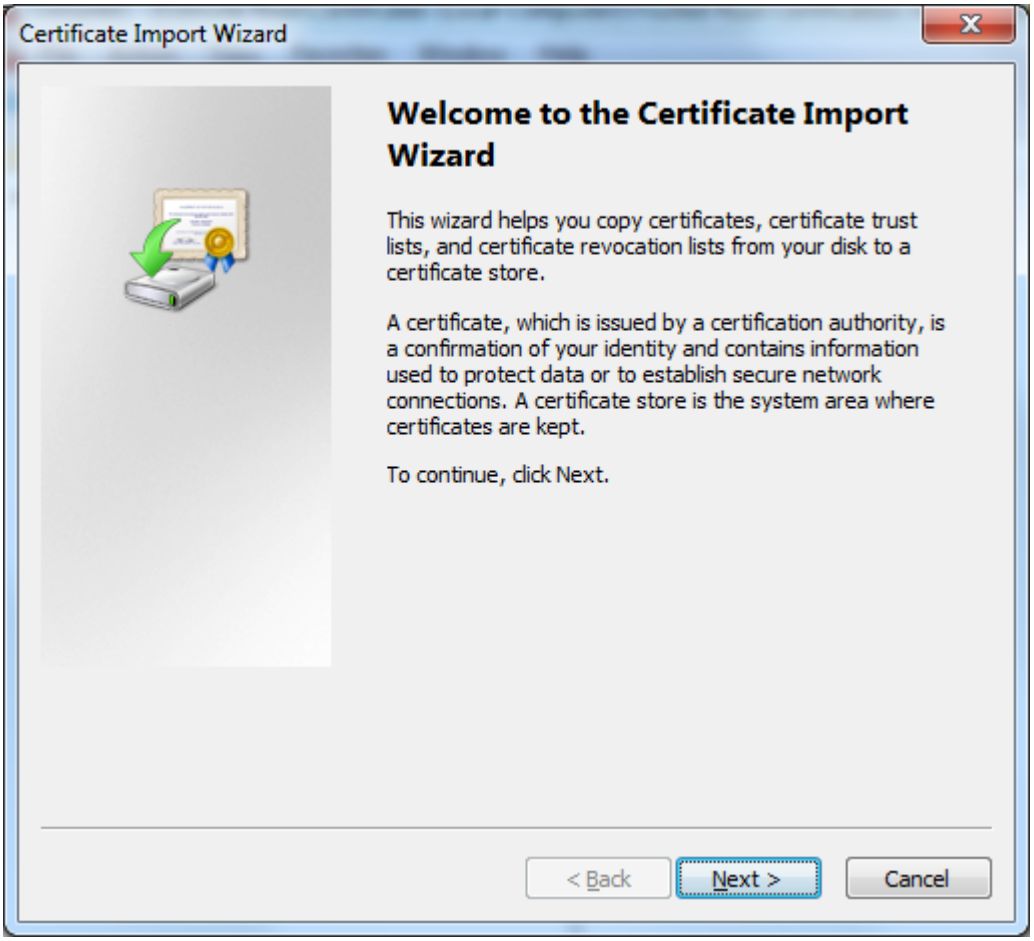

7. In the console tree, double-click **Certificates**.

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



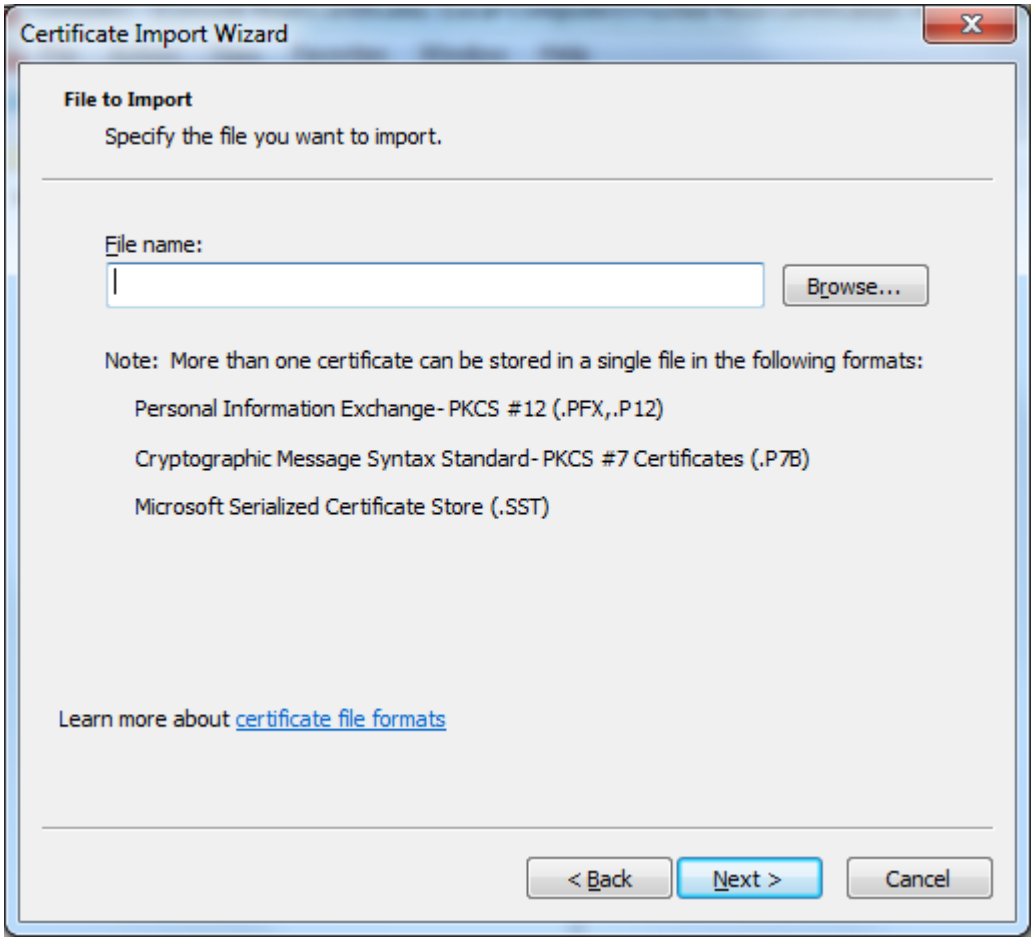

The **Certificate Import Wizard** appears.

9. Click **Next**.




The **File to Import** dialog box appears.

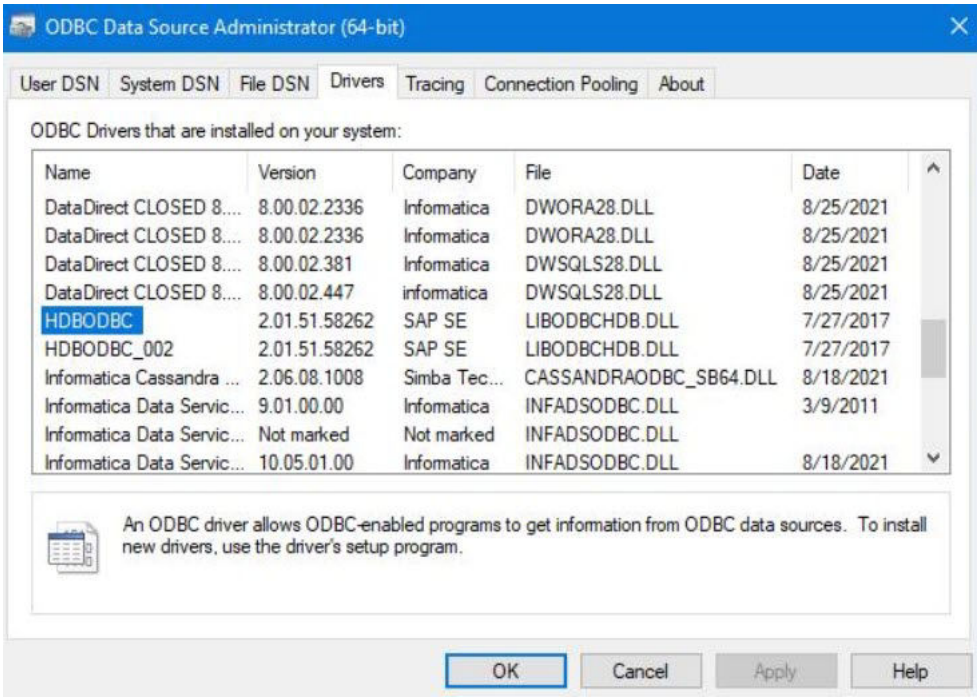
10. Click **Browse** to import the `trust.pem` certificate file.




**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.




## 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 run-time 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.
3. 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.**