How-To Library

Informatica

How to Configure the SAP Secure Network Communication Protocol in Informatica Cloud Application Integration®

Abstract

Secure Network Communication (SNC) is a software layer in the SAP system architecture that integrates third-party security products with SAP. Using the SNC protocol, you can secure communications between SAP and an external system. This article describes how to configure the SNC protocol to secure communications between Application Integration and SAP.

Supported Versions

- Informatica Intelligent Cloud Services Application Integration April 2021

Table of Contents

SNC Implementation

You can use the Secure Network Communication (SNC) protocol to secure communications between SAP and an external system. The SNC protocol is implemented by using a third-party security product.

In Application Integration, the SNC protocol is implemented by using the SAP Cryptographic Library. The SAP Cryptographic Library is a security product from SAP that is used to implement security features through SNC.

The installation package consists of the following files:

- `libsapcrypto.so`. The library file that is used for the run-time implementation of SNC on Linux-based systems.
- `sapcrypto.dll`. The library file that is used for the run-time implementation of SNC on Windows-based systems.
- `sapgenpse.exe`. The configuration tool that is used to generate the security certificates for the SAP server and the machine on which the Secure Agent is installed.
- `ticket`. The license ticket file to implement SNC.

Configuration Steps for Secure Network Communication

To secure communications between Application Integration and SAP by using the SNC protocol, you must complete configuration steps in both Application Integration and in the SAP system.

1. Download and install the SAP Cryptographic Library on the SAP server.
2. Create a Personal Security Environment (PSE) for the SAP server.
3. Install the SAP Cryptographic Library on the machine on which the Secure Agent is installed.
4. Create a PSE for the machine on which the Secure Agent is installed and export it.
5. Inform the SAP administrator to import the PSE certificate from the SAP system and add it to the SAP server trusted certificates list. This ensures that the SAP system can recognize Application Integration as an SNC-enabled communication partner. The SAP administrator must then export the SAP server PSE certificate.
6. Import the SAP server PSE certificate in Application Integration. This establishes two-way SNC-enabled communication between Application Integration and the SAP system.
7. Grant SNC permissions to the operating system user who starts the Secure Agent.
8. Grant SNC permissions to the SAP user.
9. Configure additional SAP settings for X.509 certificate
10. Configure the SNC parameters in an SAP BAPI connection

Installing the SAP Cryptographic Library on the SAP Server

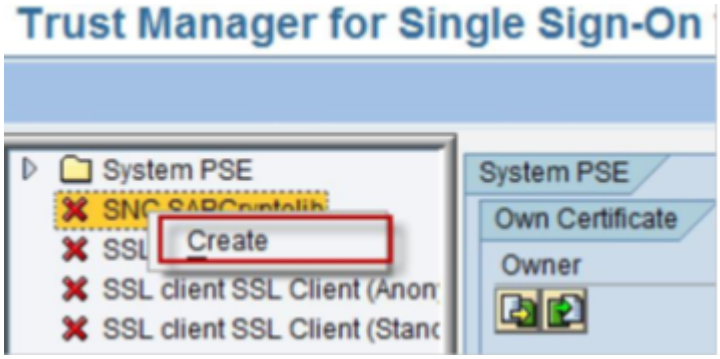
Download the SAP Cryptographic Library for the SAP server from the SAP web site. Extract the contents of the installation package and download the `libsapcrypto.so` or `sapcrypto.dll` library file, ticket file, and the `sapgenpse.exe` configuration tool. Set the environment variable SECUDIR to the directory where the ticket file is stored.

For more information about installing the SAP Cryptographic Library, see the SAP documentation.

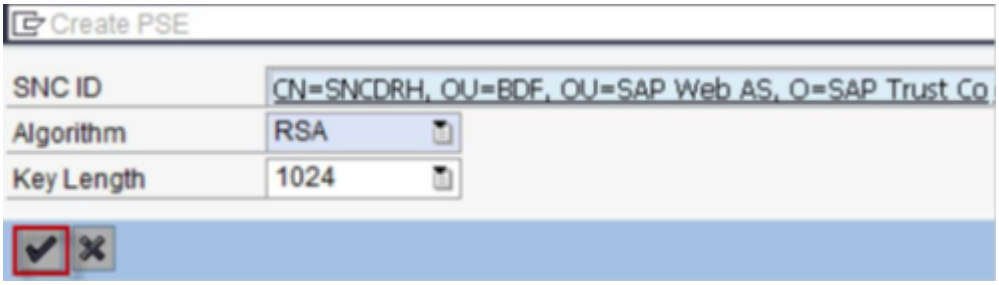
Creating the Personal Security Environment for the SAP Server

1. Go to transaction RZ10 and select the instance profile that is used by the SAP server for start-up.
2. Add the instance parameter snc/identity/as and set it to the specific name of the SAP server.

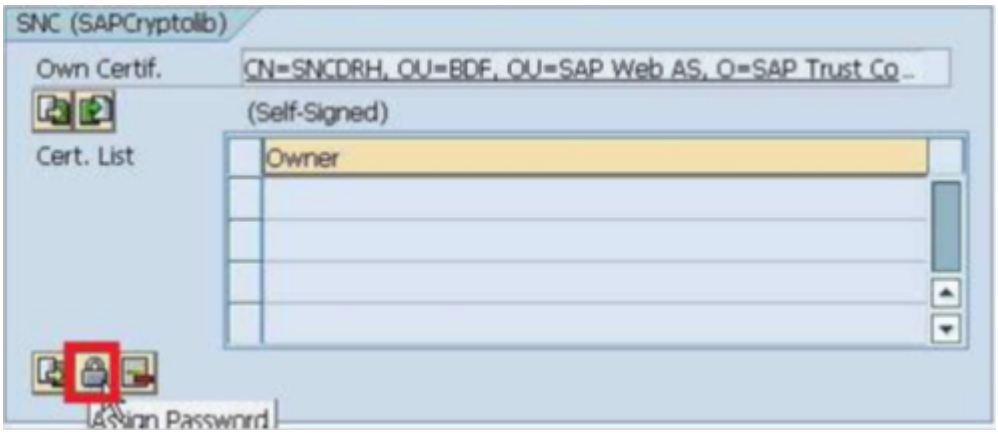
   For example, set snc/identity/as to p:CN=<x>, OU=<x>, O=<x>, C=<x> where CN = common name, OU = organizational unit, O = organization, C = country.
3. Restart the SAP server to apply the changes.
4. Go to STRUST transaction to create the SNC PSE.
5. Right-click **SNC (SAPCryptolib)** and click **Create**.



The SNC identity specified in the transaction RZ10 appears.

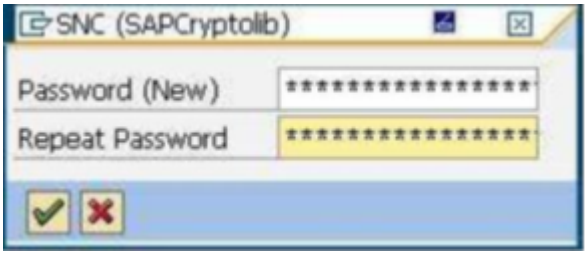


6. Click **OK**.
7. Double-click **SNC (SAPCryptolib)** and click the **Assign Password** icon to assign a password for the SNC (SAPCryptolib) PSE.



8. Enter a password for the SNC (SAPCryptolib) PSE. Each time you view or change the PSE, you will be prompted to enter the password.

   The password can contain both letters and numbers.



9. Save the changes.
10. Set the snc/enable parameter to 1 in the transaction RZ10 for the SNC instance profile.

Note: If you want to allow users who are not authorized for SNC to access the SAP server, set the following parameters in the transaction RZ10 for the SNC instance profile:

Parameter	Value
snc/accept_insecure_rfc	1
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cpic	1
snc/permit_insecure_start	1
snc/data_protection/min	1
snc/data_protection/max	3
snc/extid_login_diag	1
snc/extid_login_rfc	1

For more information about these parameters, see the *SAP documentation*.

11. Restart the SAP instance to apply the changes.

Installing the SAP Cryptographic Library on the Secure Agent Machine

1. Download the SAP Cryptographic Library from the SAP web site.
2. Connect to the Secure Agent machine with the ID of the user who starts the Secure Agent.
3. Extract the contents of the SAP Cryptographic Library installation package.
4. Copy the library file, `sapgenpse.exe` file, and ticket file to the following directory:

   ```
   <Secure Agent installation directory>/apps/process-engine/ext
   ```

5. Add the following information in the profile of the user who starts the Secure Agent:

   ```
   SNC_LIB=<Secure Agent installation directory>/apps/process-engine/ext/
   <library_file_name>; export SNC_LIB
   SECUDIR=<Secure Agent installation directory>/apps/process-engine/ext; export SECUDIR
   USER=<Name of the user who starts the Secure Agent>; export USER
   ```

   Set the library path to the following directory:

   ```
   <Secure Agent installation directory>/apps/process-engine/ext
   ```

   For example, on an HP-UX operating system, set the library path as follows:

   ```
   SHLIB_PATH=<Secure Agent installation directory>/apps/process-engine/ext:$ORACLE_HOME/lib;
   export SHLIB_PATH
   ```

   This step defines where the SNC library file and ticket file are stored, and the name of the user who will execute the SNC functions.

6. Restart the Secure Agent to apply the changes.

Creating the PSE for the Secure Agent and Exporting it to the SAP System

1. Connect to the machine on which the Secure Agent is installed with the ID of the user who starts the Secure Agent.
2. Navigate to the following directory:

   `<Secure Agent installation directory>/apps/process-engine/ext`
3. Run the following command to generate the PSE for the machine on which the Secure Agent is installed:
   `sapgenpse get_pse <additional_options> [-p <PSE_name>][DN]`

   You will be prompted to enter a PIN and an undistinguished name.
4. Enter a PIN and an undistinguished name.

   The PIN is a unique identification value for the PSE.

   The undistinguished name is the name of the machine that is registered in the SAP system and the machine on which the Secure Agent is installed. Enter the undistinguished name as CN=<x>, OU=<x>, where CN = common name, and OU = organizational unit. For example, enter the undistinguished name as: CN=INFACONTNT, OU=BDF.

   The PSE is generated under the following directory:
   `<Secure Agent installation directory>/apps/process-engine/ext`
5. Run the `chmod` command and assign read, write, and execute permissions to the generated PSE.
6. Navigate to the following directory:

   `<Secure Agent installation directory>/apps/process-engine/ext`
7. Run the following command to export the PSE certificate for the machine on which the Secure Agent is installed:

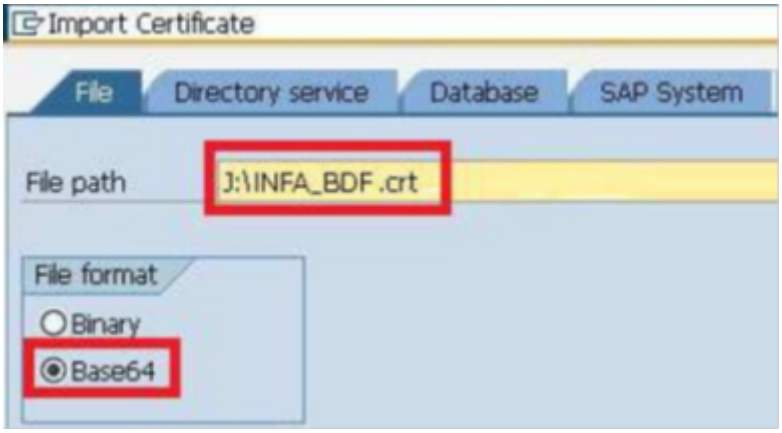
   ```
   sapgenpse export_own_cert -v -p <Name of the PSE created on the machine on which the Secure Agent is installed> -o <Name of the .crt certificate created on the machine on which the Secure Agent is installed and exported to the SAP server>
   ```

   The PSE certificate is generated under the following directory:
   `<Secure Agent installation directory>/apps/process-engine/ext`
8. Run the `chmod` command and assign read, write, and execute permissions to the generated PSE certificate.
9. Send the PSE certificate to the SAP administrator.

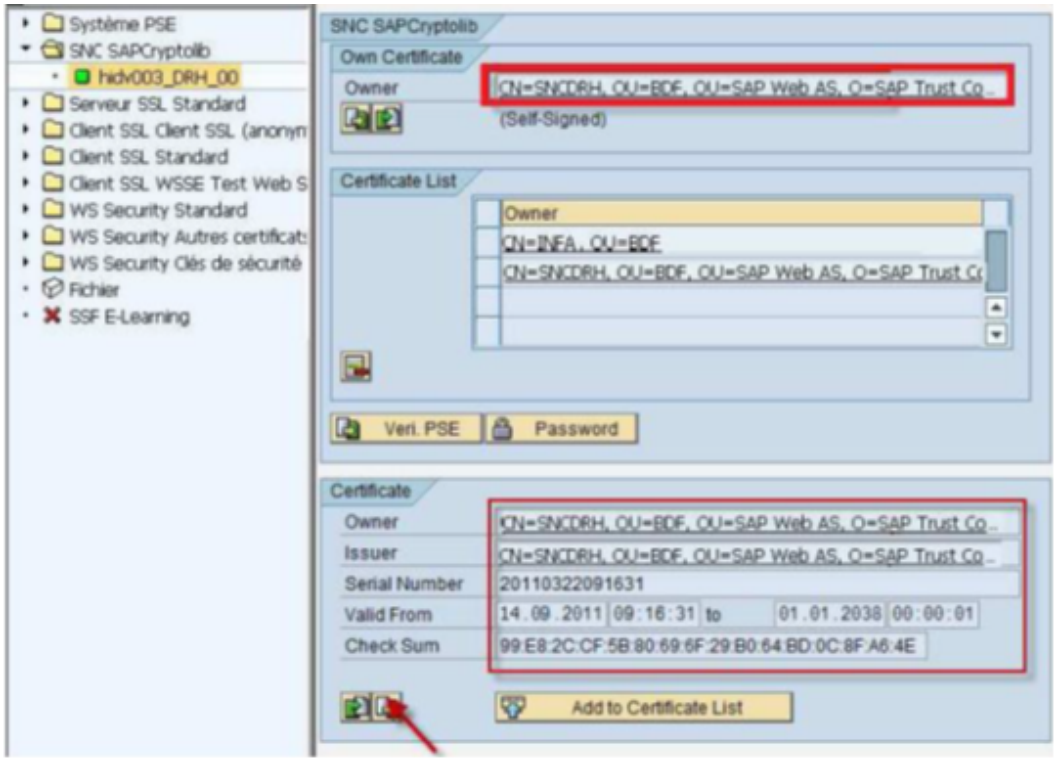
Importing the PSE Certificate in SAP and Exporting the SAP Server PSE Certificate

1. Connect to the SAP system.
2. Go to transaction STRUST to import the PSE certificate that was created on the machine on which the Secure Agent is installed.
3. Browse and select the `.crt` certificate that you created. Click the **Import Certificate** icon.

4. Select the **Base64** option and load the PSE certificate that was created on the machine on which the Secure Agent is installed.



5. Click **Add to Certificate List** to add the PSE certificate to the SAP server trusted list of certificates.
6. Go to transaction STRUST to export the SAP server PSE certificate.
7. Double-click the SAP server PSE certificate and click the **Export Certificate** icon.



8. Save the SAP server PSE certificate under the following directory:

```
<Secure Agent installation directory>/apps/process-engine/ext
```

Importing the SAP Server PSE Certificate in Application Integration

1. Copy the SAP server PSE certificate under the following directory:

```
<Secure Agent installation directory>/apps/process-engine/ext
```

2. Run the `chmod` command and assign read, write, and execute permissions to the SAP server PSE certificate.
3. Connect to the machine on which the Secure Agent is installed and run the following command to add the SAP server PSE certificate from SAP:

   ```
   sapgenpse maintain_pk -v -a <Name of the SAP server PSE certificate> -p <Name of the PSE certificate that was created on the machine on which the Secure Agent is installed>
   ```

   The SAP server PSE certificate is added to the Informatica trusted list of certificates.

Granting SNC Permissions to the Operating System User who Starts the Secure Agent

1. Navigate to the following directory:

   ```
   <Secure Agent installation directory>/apps/process-engine/ext
   ```

2. Run the following command:

   ```
   sapgenpse seclogin -p <Name of the PSE certificate that was created on the machine on which the Secure Agent is installed> -O <Name of the operating system user who starts the Secure Agent>
   ```

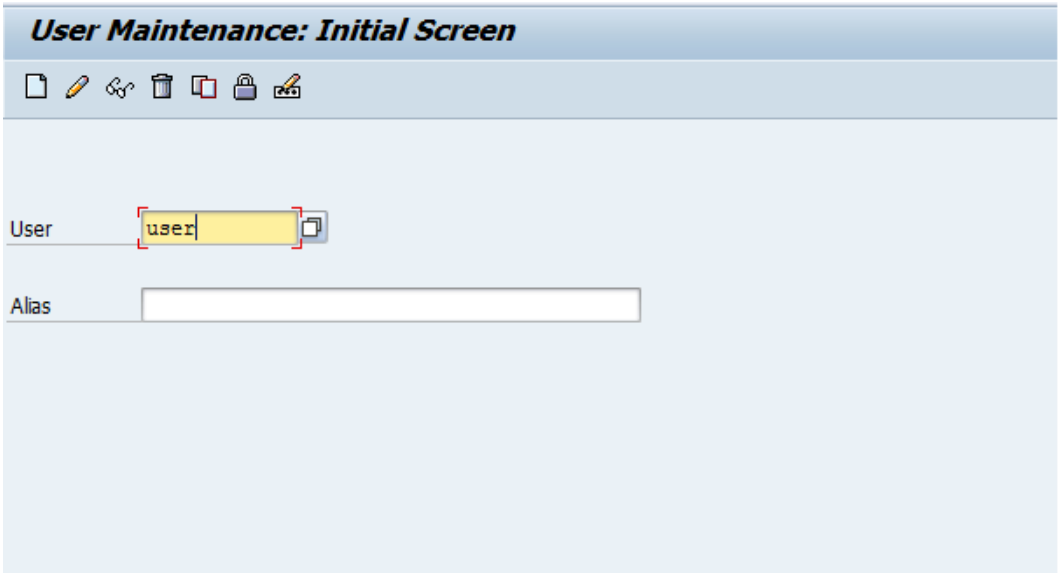
   A credentials file for the operating system user who starts the Secure Agent is generated under the following directory:

   ```
   <Secure Agent installation directory>/apps/process-engine/ext
   ```

   The credentials file defines the SNC permissions to be assigned to the operating system user who starts the Secure Agent.

Granting SNC Permissions to the SAP User

1. Go to transaction SU01.
2. In the **User** field, enter the SAP user name to which you want to grant permissions to execute the SNC functions.

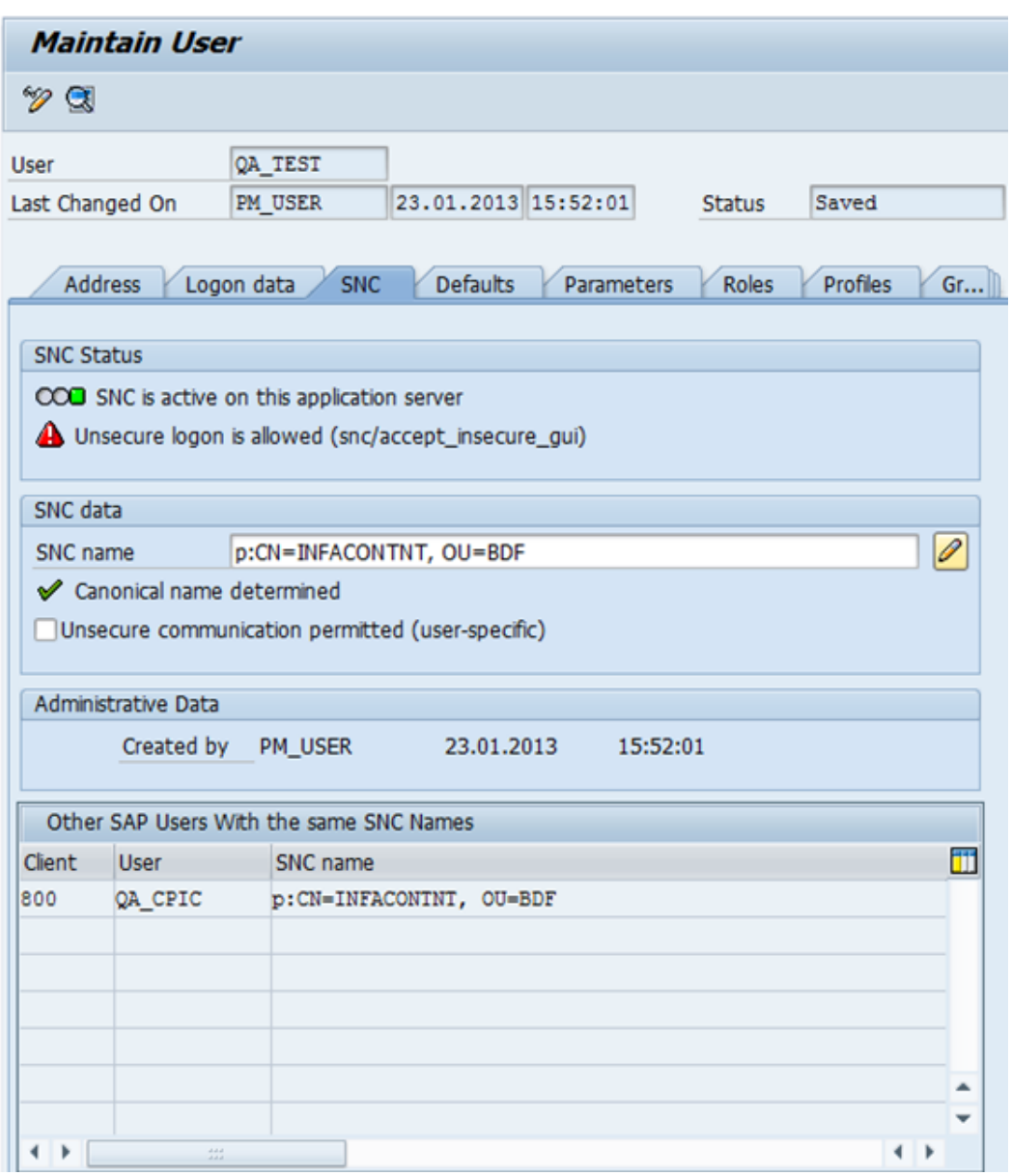


3. Click the **Change** icon.

   The **Maintain User** screen appears.

4. Click the **SNC** tab.
5. In the **SNC name** field, enter the following value: p:CN=<common name>, OU=<organizational unit>
6. Click **OK**.

   A message appears stating that the canonical name is determined.



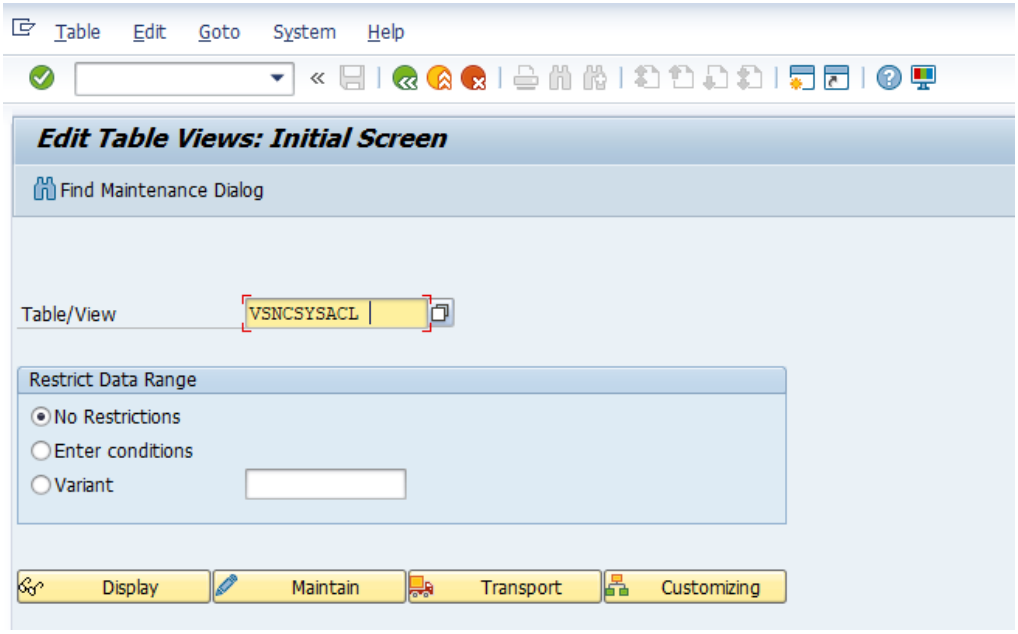
7. Click **Save** to save the changes.

Configuring Additional SAP Settings for X.509 Certificate

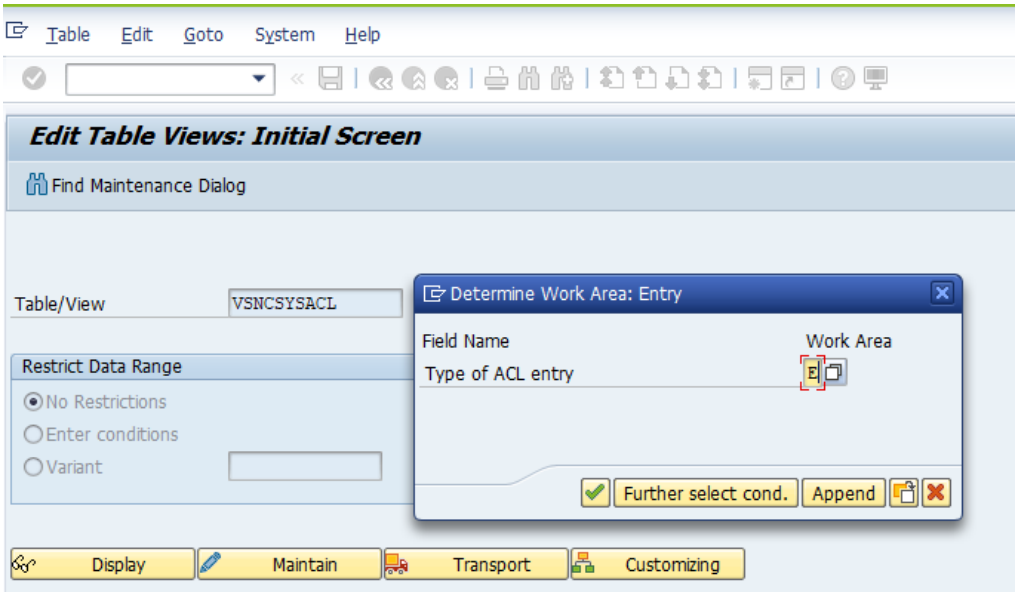
You can configure the SAP user for the X.509 SNC connection so that the client can use SNC without the need to specify the SAP user and password.

1. Go to transaction **SM30**.
2. Maintain the VSNCSYSACL and VUSREXTID tables.

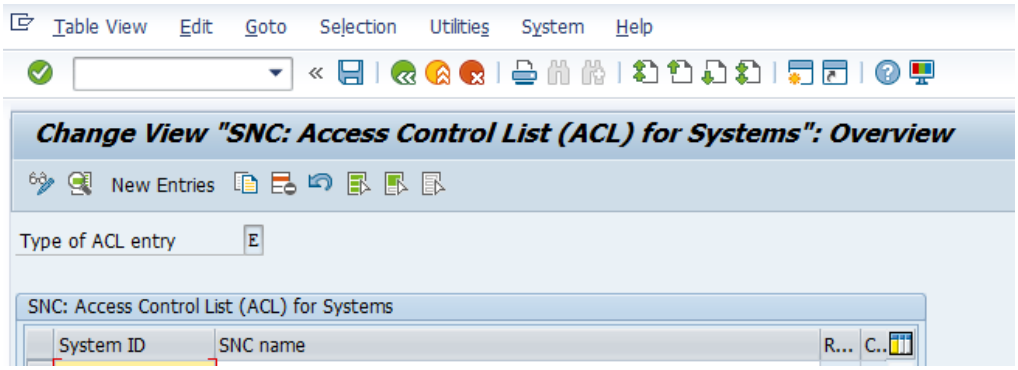
3. To maintain VSNCSYSACL, perform the following tasks:
   a. Open the table VSNCSYSACL for maintenance.



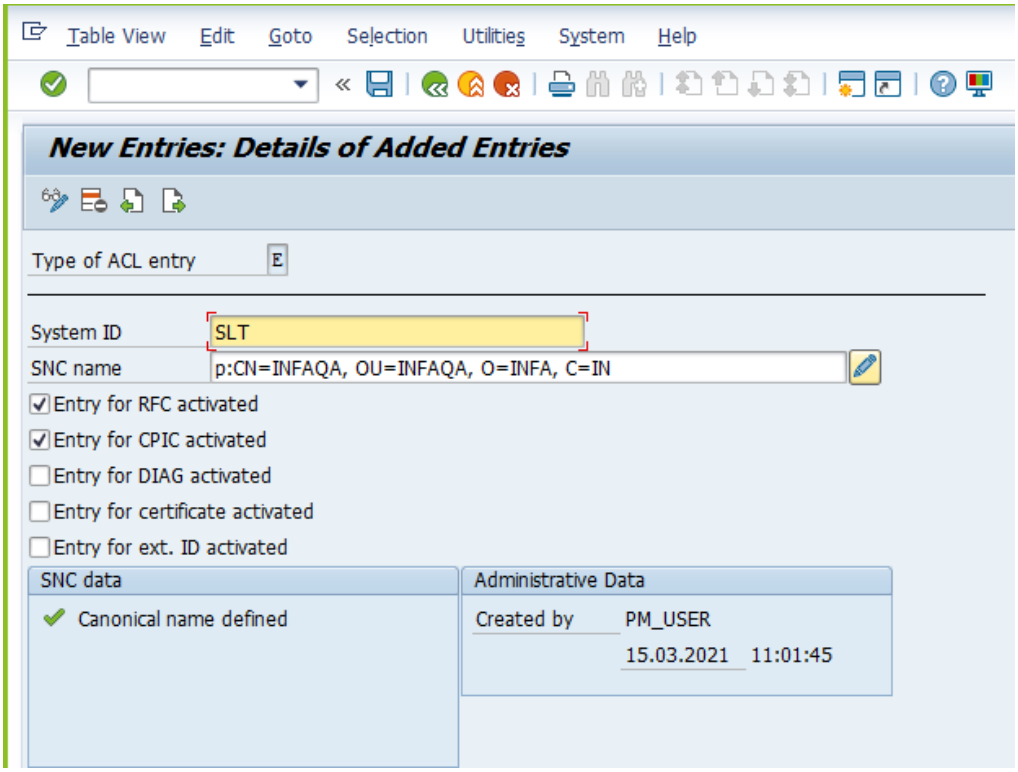
   b. Choose external type work area.



c. Select **New Entries**.

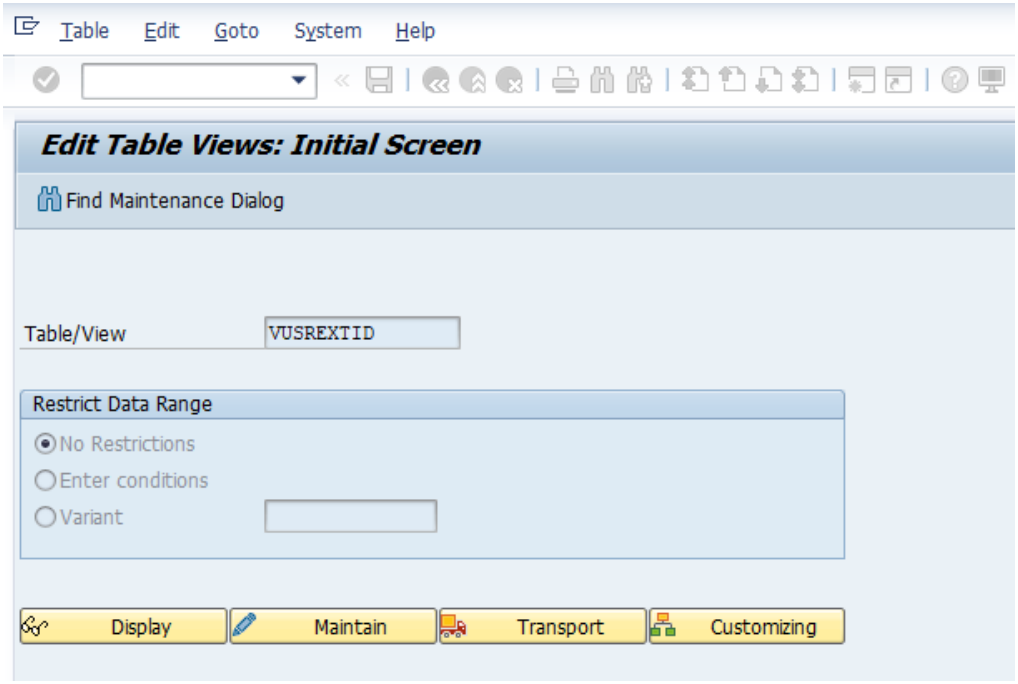


d. Enter the System ID and the SNC name.

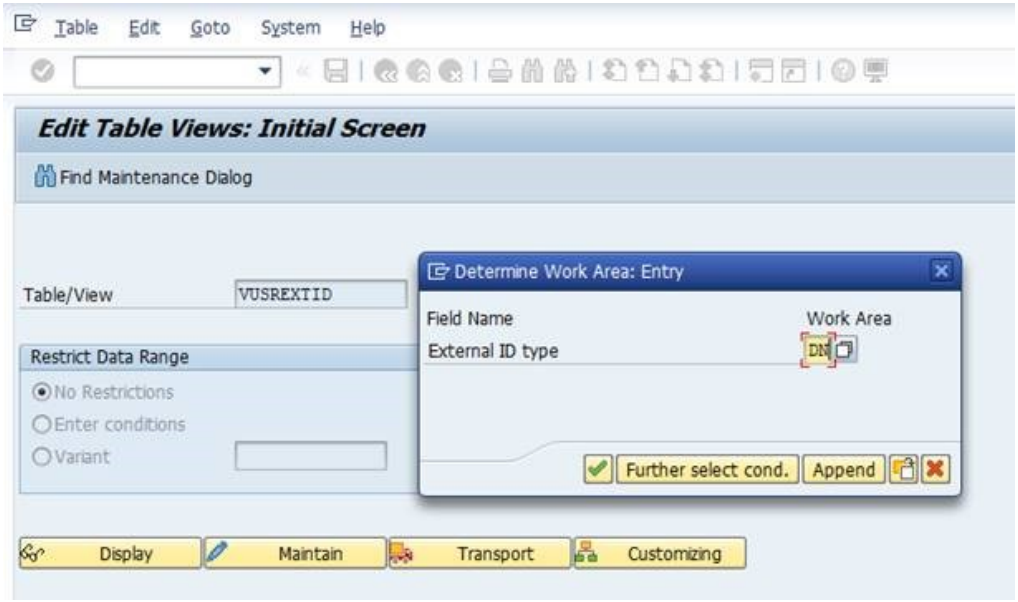


e. Save the data.

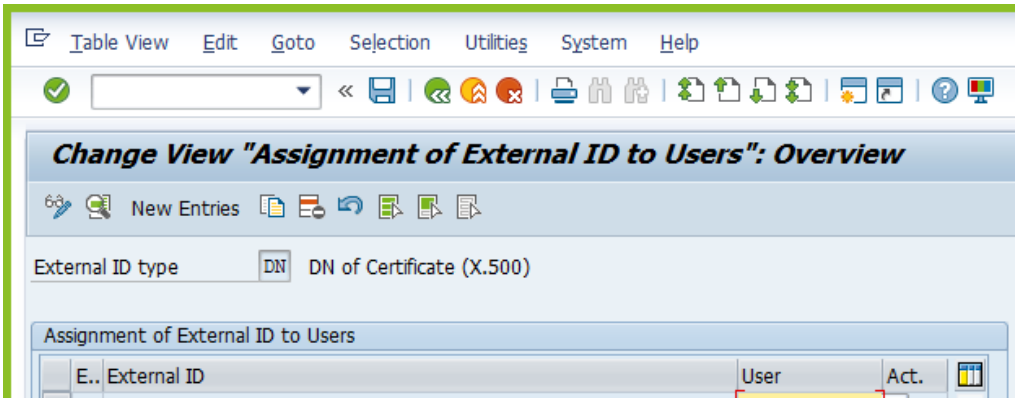
4. To maintain VUSREXTID, perform the following tasks:
   a. Open the table VUSREXTID for maintenance.



   b. Choose the work ID as DN.

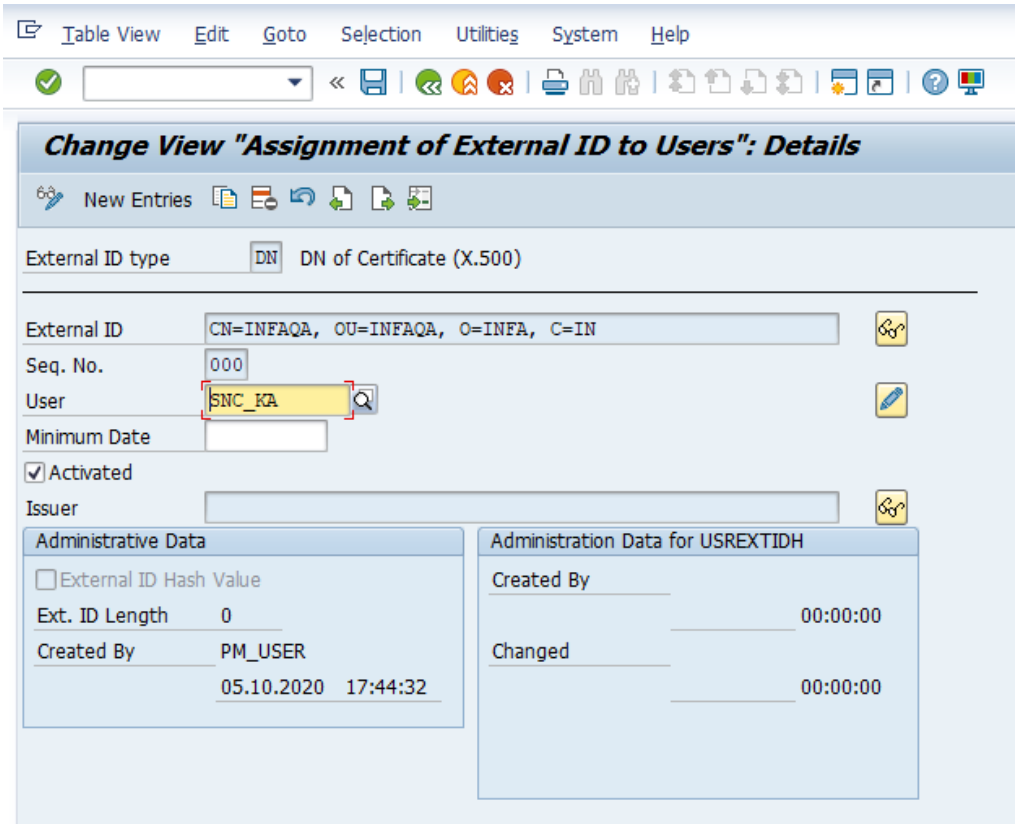


c. Select **New Entries**.



d. Enter the following details:

- **User**. The user that the client uses to connect to the SAP server.
- **Sequence Number**. The SAP client number.
- **SNC Name**. The DN associated with the client PSE.
- **Activated**. Select this option to activate the VUSREXTID for maintenance.



e. Save the data.

Configuring the SNC Parameters in an SAP BAPI Connection

To use SNC with the SAP BAPI Connector, you must configure the SNC parameters in the connection properties. You can configure SNC for the following logon types in application and load balancing connections:

- X.509 certificate
- Single sign on

1. Open the SAP BAPI connection in Application Integration.
2. To enable the SNC protocol and secure communications between Application Integration and SAP, add the following properties in the **SAP Additional Parameters** field in the SAP BAPI connection:
   a. To use the application connection with SNC and single sign on, specify the following parameters:
      - SNC_MODE = 1
      - SNC_QOP=3
      - SNC_MYNAME = p:CN=<common name>, OU=<organizational unit>. This is the SNC name of the machine on which the Secure Agent is installed.
      - 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/process-engine/ext/<filename>`

        Note: The file name for the SNC_LIB parameter is `libsapcrypto.so` for Linux and `sapcrypto.dll` for Windows.

   b. To use the application connection with SNC and X.509 log on, specify the following parameters:
      - 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 machine on which the Secure Agent is installed.
      - 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/process-engine/ext/<filename>`

        Note: The file name for the SNC_LIB parameter is `libsapcrypto.so` for Linux and `sapcrypto.dll` for Windows.
      - X509CERT=MIIC8TCCAdkCCAogIAkiCAhIMA0GCSqGSIb3DQ (…)

   c. To use the load balancing connection with SNC and single sign on, specify the following parameters:
      - MSHOST= <Message server hostname>
      - GROUP= <Message server group>
      - R3NAME =<SAP system SID>
      - 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 machine on which the Secure Agent is installed.
      - 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/process-engine/ext/<filename>`

  Note: The file name for the SNC_LIB parameter is `libsapcrypto.so` for Linux and `sapcrypto.dll` for Windows.

d. To use the load balancing connection with SNC and X.509 log on, specify the following parameters:

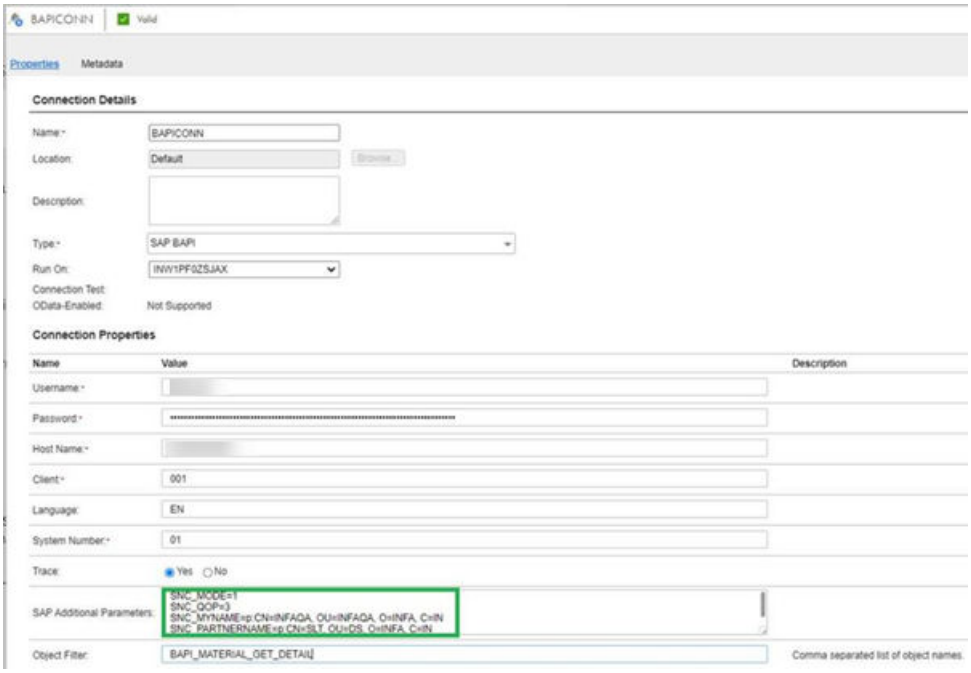
- MSHOST= <Message server hostname>
- GROUP = <Message server group>
- R3NAME=<SAP system SID>
- SNC_MODE=1
- SNC_QOP=3
- SNC_MYNAME= p:CN=<common name>, OU=<organizational unit>,O=<organization>, C=<country> This is the SNC name of the machine on which the Secure Agent is installed.
- SNC_PARTNERNAME= 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/process-engine/ext/<filename>`

  Note: The file name for the SNC_LIB parameter is `libsapcrypto.so` for Linux and `sapcrypto.dll` for Windows.
- X509CERT= MIIC8TCCAdkCCAogIAkiCAhIMA0GCSqGSIb3DQ (…)

3. Add the following entries for the SAP gateway service and message server that you want to use:

- `sapgw <system number> <port number of gateway service>/tcp`
- `Sapms <System SID> <port number of gateway service>/tcp`

The following image shows the SNC properties configured in an SAP BAPI connection:



4. Save and publish the SAP BAPI connection.

   For more information about SAP BAPI connections, see *SAP BAPI Connector Guide*.

Author

Sonali Kumbhalkar
Senior Technical Writer