

## How to Configure the SAP Secure Network Communication Protocol in PowerCenter

## 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 PowerCenter and SAP.

## Supported Versions

- PowerExchange for SAP NetWeaver 10.2 or later

## Table of Contents

SNC Implementation for PowerExchange for SAP NetWeaver in PowerCenter. . . . .	2
Configuration Steps for Secure Network Communication. . . . .	2
Installing the SAP Cryptographic Library on the SAP Server. . . . .	3
Creating the Personal Security Environment for the SAP Server. . . . .	3
Installing the SAP Cryptographic Library on Informatica. . . . .	5
Creating the PSE Certificate on Informatica and Exporting it to the SAP System. . . . .	6
Importing the PSE Certificate in SAP and Exporting the SAP Server PSE Certificate. . . . .	6
Importing the SAP Server PSE Certificate in PowerCenter. . . . .	8
Granting SNC Permissions to the Operating System User who Starts the Informatica Services. . . . .	8
Granting SNC Permissions to the SAP User. . . . .	8
Configuring the sapnwrfc.ini File to Enable the SNC Protocol. . . . .	10

## SNC Implementation for PowerExchange for SAP NetWeaver in PowerCenter

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 PowerCenter, 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.
- `sapgenpse.exe`. The configuration tool that is used to generate the security certificates for the SAP server and the machine on which the Informatica services are installed.
- `ticket`. The license ticket file to implement SNC.

## Configuration Steps for Secure Network Communication

To secure communications between PowerCenter and SAP by using the SNC protocol, you must complete configuration steps in both PowerCenter 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 Informatica services are installed.
4. Create a PSE for the machine on which the Informatica services are installed and export it.
5. Inform the SAP administrator to import the PSE certificate that was created on the machine on which the Informatica services are installed from the SAP system and add it to the SAP server trusted certificates list. This ensures that the SAP system can recognize PowerCenter 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 PowerCenter. This establishes two-way SNC-enabled communication between PowerCenter and the SAP system.
7. Grant SNC permissions to the operating system user who starts the Informatica services.
8. Grant SNC permissions to the SAP user.
9. Configure the `sapnwrfc.ini` file to enable the SNC protocol.

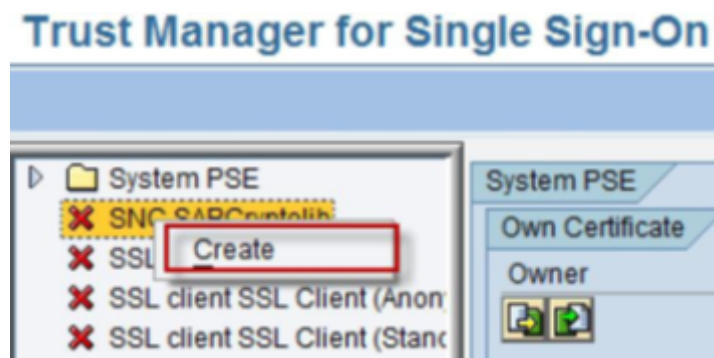
### *Installing the SAP Cryptographic Library on the SAP Server*

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` library file, ticket file, and the `sapgenpse.exe` configuration tool. Set the environment variable `SECUDIR` to the directory where the ticket file is stored.

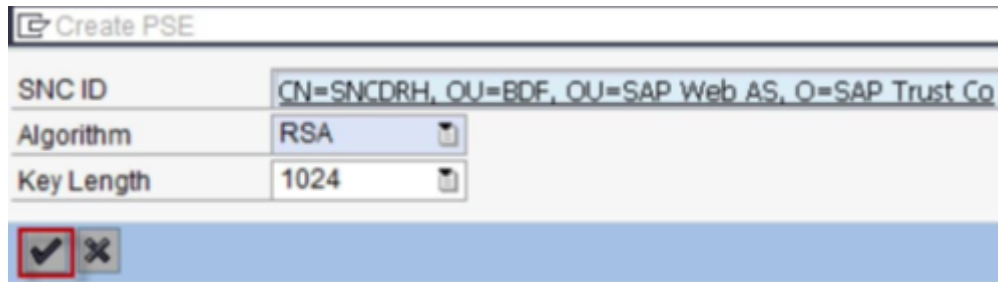
For more information about installing the SAP Cryptographic Library, see the SAP documentation.

### *Creating the Personal Security Environment for the SAP Server*

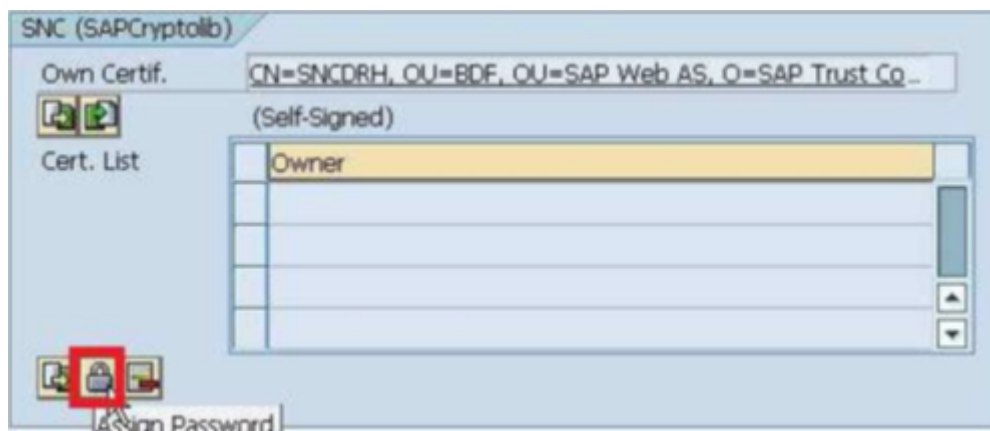
1. Go to transaction RZ10 and select the instance profile that is used by the SAP server for start-up.
2. Add the instance parameter `snc/identity/as` and set it to the specific name of the SAP server.  
For example, set `snc/identity/as` to `p:CN=<x>, OU=<x>, O=<x>, C=<x>` where CN = common name, OU = 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_cplic	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.

- Restart the SAP instance to apply the changes.

## Installing the SAP Cryptographic Library on Informatica

- Download the SAP Cryptographic Library from the SAP web site.
- Connect to the machine on which the Informatica services are installed with the ID of the user who starts the Informatica services.
- Extract the contents of the SAP Cryptographic Library installation package.
- Copy the `libsapcrypto.so` library file to the following directory: `<PowerCenter Installation Directory>/server/bin`
- Copy the `sapgenpse.exe` configuration tool to the following directory: `<PowerCenter Installation Directory>/server/bin/sec`
- Copy the ticket file to the following directory: `<PowerCenter Installation Directory>/server/bin/sec`
- Add the following information in the profile of the user who starts the Informatica services:

```
SNC_LIB=<PowerCenter Installation Directory>/server/bin/libsapcrypto.so; export SNC_LIB
SECUDIR=<PowerCenter Installation Directory>/server/bin/sec; export SECUDIR
USER=<Name of the user who starts the Informatica services>; export USER
```

Set the library path to the following directory: `<PowerCenter Installation Directory>/server/bin/sec`

For example, on an HP-UX operating system, set the library path as follows: `SHLIB_PATH=<PowerCenter Installation Directory>/server/bin/sec:$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.

- Restart the Informatica services to apply the changes.

**Note:** To secure communications between a PowerCenter Client and an SAP server by using the SNC protocol, repeat these steps on the machine on which the Powercenter Client is installed.

## Creating the PSE Certificate on Informatica and Exporting it to the SAP System

1. Connect to the machine on which the Informatica services are installed with the ID of the user who starts the Informatica services.
2. Navigate to the following directory: `<PowerCenter Installation Directory>/server/bin/sec`
3. Run the following command to generate the PSE for the machine on which the Informatica services are 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 Informatica services are 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: `<PowerCenter Installation Directory>/server/bin/sec`

5. Run the `chmod` command and assign read, write, and execute permissions to the generated PSE.
6. Navigate to the following directory: `<PowerCenter Installation Directory>/server/bin/sec`
7. Run the following command to export the PSE certificate for the machine on which the Informatica services are installed:

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

The PSE certificate is generated under the following directory: `<PowerCenter Installation Directory>/server/bin/sec`

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.

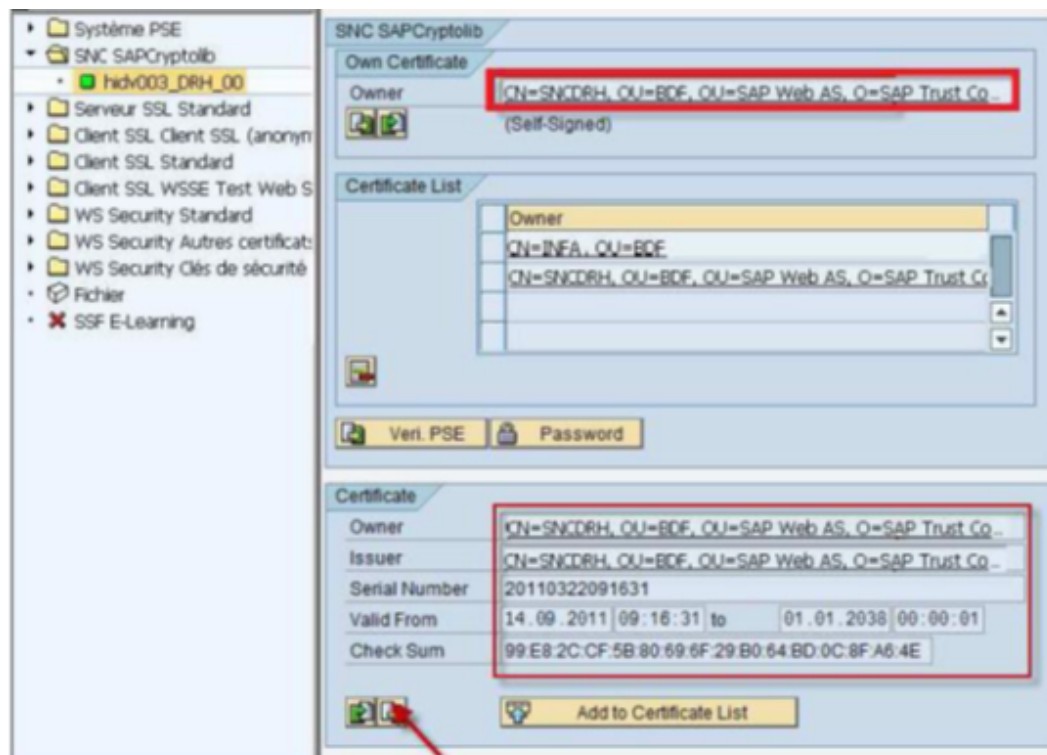
## Importing the PSE Certificate in SAP and Exporting the SAP Server PSE Certificate

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 Informatica services are installed.
3. Browse and select the `.crt` certificate that you created in step 7 as described in the earlier section. Click the **Import Certificate** icon.

4. Select the **Base64** option and load the PSE certificate that was created on the machine on which the Informatica services are installed.

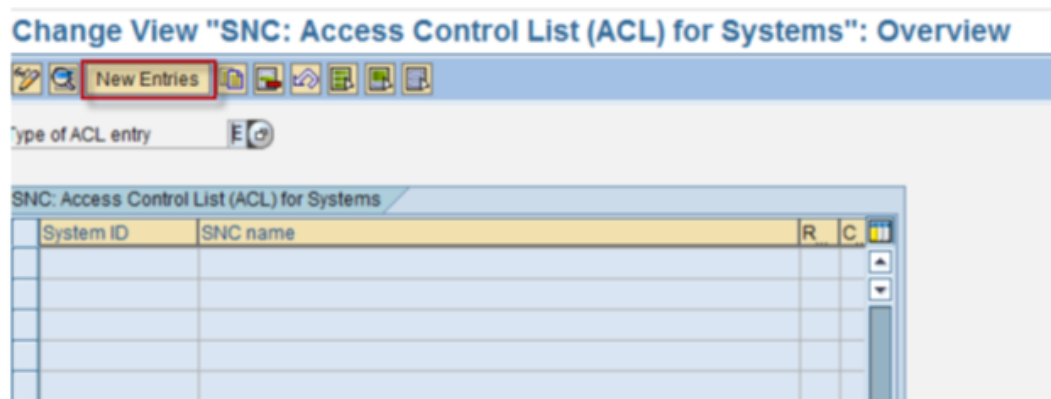


5. Click **Add to Certificate List** to add the PSE certificate that was created on the machine on which the Informatica services are installed to the SAP server trusted list of certificates.
6. Go to transaction STRUST to export the SAP server PSE certificate.
7. Double-click the SAP server PSE certificate and click the **Export Certificate** icon.



8. Save the SAP server PSE certificate under the following directory: <PowerCenter Installation Directory>/server/bin/sec
9. Go to transaction SNC0.

- Click **New Entries** to define the name of the machine on which the Informatica services are installed and the SNC name in SAP.



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

### *Importing the SAP Server PSE Certificate in PowerCenter*

- Copy the SAP server PSE certificate under the following directory: <PowerCenter Installation Directory>/server/bin/sec
- Run the `chmod` command and assign read, write, and execute permissions to the SAP server PSE certificate.
- Connect to the machine on which the Informatica services are 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 Informatica services are 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 Informatica Services*

- Navigate to the following directory: <PowerCenter Installation Directory>/server/bin/sec
  - Run the following command:
- ```
sapgenpse seclogin -p <Name of the PSE certificate that was created on the machine on which the Informatica services are installed> -O <Name of the operating system user who starts the Informatica services>
```

A credentials file for the operating system user who starts the Informatica services is generated under the following directory: <PowerCenter Installation Directory>/server/bin/sec

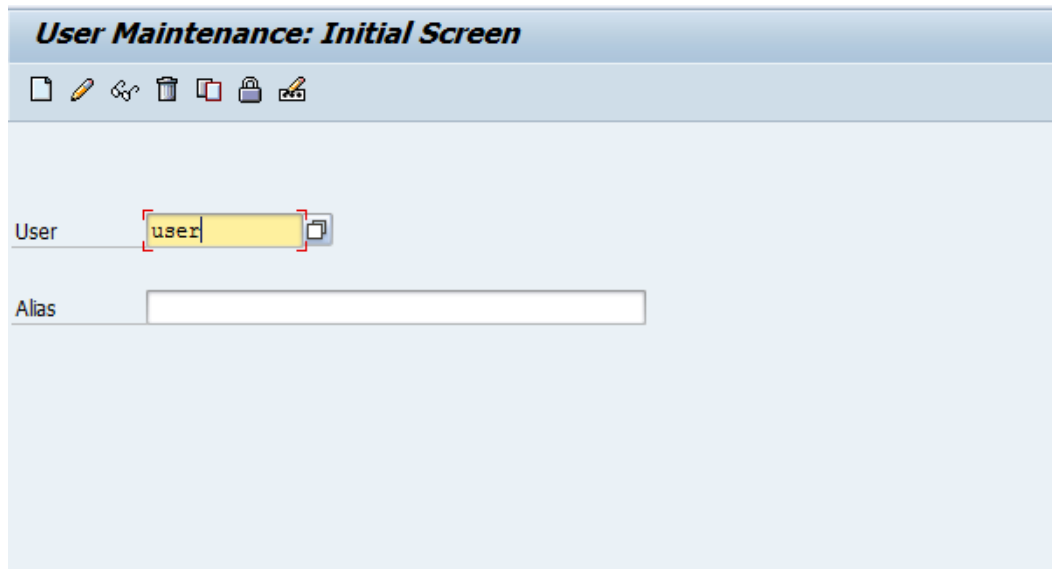
The credentials file defines the SNC permissions to be assigned to the operating system user who starts the Informatica services.

### *Granting SNC Permissions to the SAP User*

- 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.



**User Maintenance: Initial Screen**

User

Alias

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.

**Maintain User**

User: QA\_TEST

Last Changed On: PM\_USER 23.01.2013 15:52:01 Status: Saved

Address Logon data **SNC** Defaults Parameters Roles Profiles Gr...

**SNC Status**

●●● SNC is active on this application server

⚠ Unsecure logon is allowed (snc/accept\_insecure\_gui)

**SNC data**

SNC name: p:CN=INFACONTNT, OU=BDF

✓ Canonical name determined

☐ Unsecure communication permitted (user-specific)

**Administrative Data**

Created by: PM\_USER 23.01.2013 15:52:01

**Other SAP Users With the same SNC Names**

| Client | User    | SNC name                |
|--------|---------|-------------------------|
| 800    | QA_CPIC | p:CN=INFACONTNT, OU=BDF |
|        |         |                         |
|        |         |                         |
|        |         |                         |
|        |         |                         |
|        |         |                         |
|        |         |                         |
|        |         |                         |

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

### Configuring the sapnwrfc.ini File to Enable the SNC Protocol

- Open the sapnwrfc.ini file.
- Add the following parameters in the sapnwrfc.ini file to enable the SNC protocol and secure communications between PowerCenter and SAP:
  - SNC\_MODE = 1
  - SNC\_MYNAME = p:CN=<common name>, OU=<organizational unit>. This is the SNC name of the machine on which the Informatica services are 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 =<PowerCenter Installation Directory>/server/bin/libsapcrypto.so
3. Add the following entry for the SAP gateway service that you want to use: `sapgw <system number> <port number of gateway service>/tcp`

## Authors

Anu Chandrasekharan

## Acknowledgements

The author would like to acknowledge Sivaramakrishnan Kalyanaraman and Raghu Rajanna for their technical assistance.