Gimmal

Information Management for Everyone®

Secure Network Communications for ERP-Link

Configuration Guide

Software Version 5.4.0

March 2019

Title: *Secure Network Communications for ERP-Link Configuration Guide*

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmal.com. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

Contents

Chapter 1. Configuring Secure Network Communications for ERP-Link 1

1.1 Prerequisites 1

1.2 Downloading SAP Cryptography Software 2

1.3 Installing the SAP Cryptography Software 5

1.4 Creating the PSE for the Server 8

1.5 Setting SNC Additional Parameters 10

1.6 Creating PSE for RFC Client i-e for ERP-link iNet Connection Service 13

1.6.1 Installing SAP Cryptography on the Gimmal Connection Service Machine 13

1.6.2 Creating Client PSE 14

1.6.3 Importing and Exporting Client Certificates between Client PSE and SAP Application Server 15

1.6.4 Creating the cred_v2 File 19

1.7 Configuring SAP for Secure Network Communications 20

1.7.1 Allowing SNC Connection with RFC 20

1.7.2 Mapping X.509 Certificate to User 22

1.8 Configuring Connection Service for SNC 24

1.8.1 Configuring SNC for iNet Connection Service 24

1.8.2 Testing SNC Using the Gimmal Connection Service 26

1 Configuring Secure Network Communications for ERP-Link

This document provides information on how to install and configure secure network communications (SNC).

1.1 Prerequisites

You must have the following present in your system:

- SAP Cryptography Software download
- SAP Application server installed and configured
- ERP-Link software installed and configured

For a complete list of ERP-Link prerequisites, see the *ERP-Link V5.2.0 Installation and Administration Guide* for details on installing and configuring this product, available on the Gimmal product download site.

1.2 Downloading SAP Cryptography Software

To download SAP cryptography software, follow these steps.

1. Download the SAP cryptography software from the SAP marketplace and navigate to **Installation and Upgrade**.

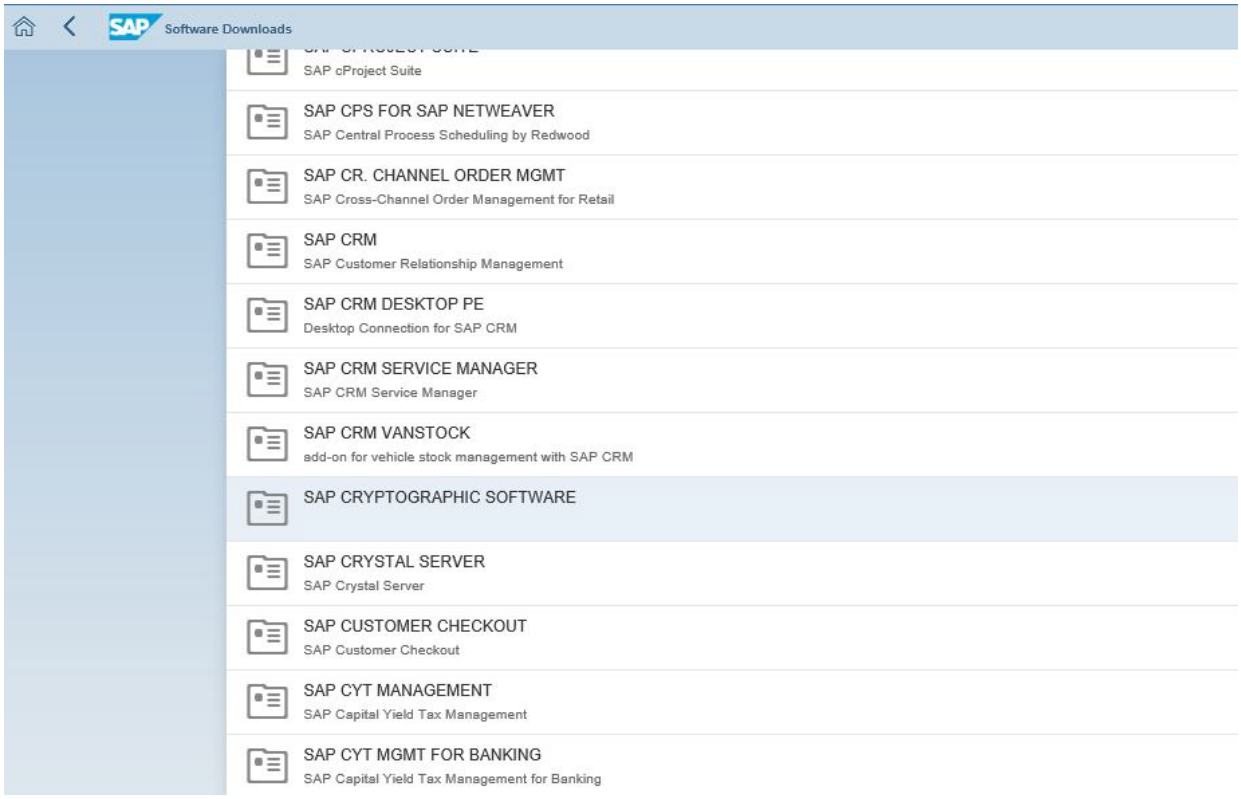


Figure 1-1 Selecting SAP CRYPTOGRAPHIC SOFTWARE to Download

2. Click **SAP CRYPTOGRAPHIC SOFTWARE.** The **SAP CRYPTOGRAPHIC SOFTWARE DOWNLOADS** options display.

Figure 1-2 SAP CRYPTOGRAPHIC SOFTWARE Download Options

3. Click **SAPCRYPTOLIB**. The **SAPCRYPTOLIB DOWNLOADS** options display.

Figure 1-3 SAPCRYPTOLIB DOWNLOADS Option

4. Download COMMONCRYPTOLIB8.

Note:

This is the latest cryptography software and it is also backward compatible with all prior cryptographic software versions.

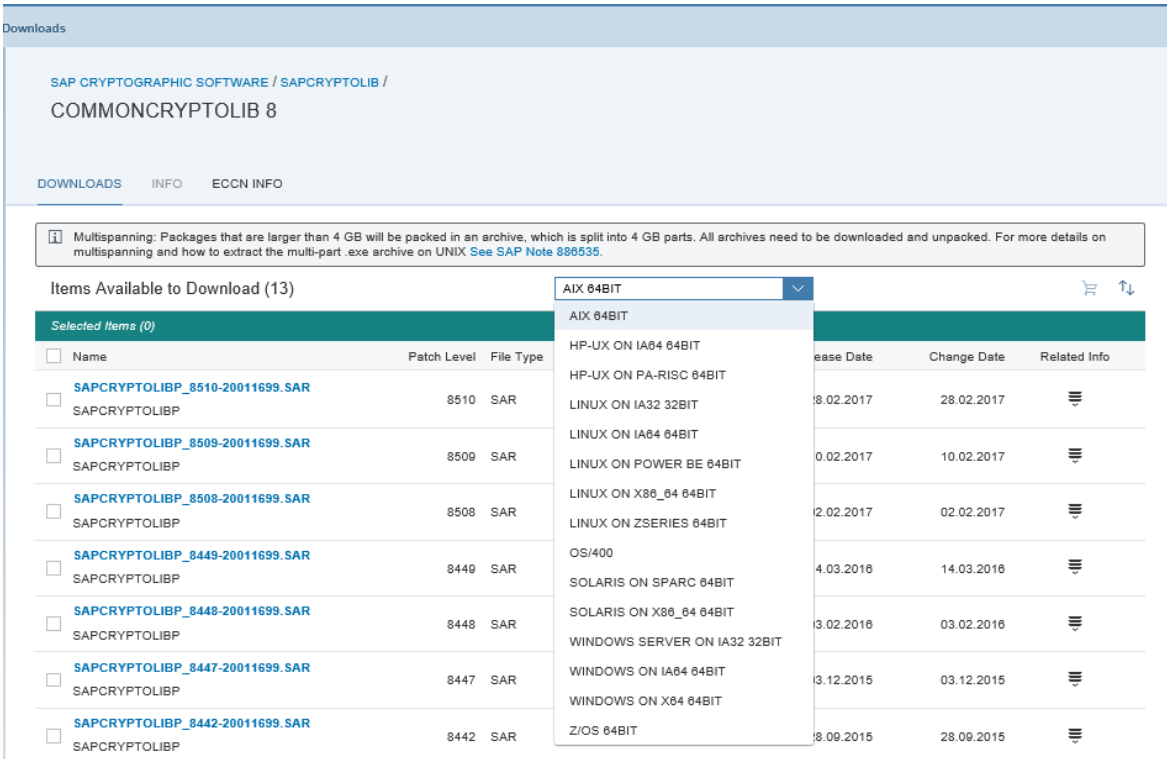


Figure 1-4 Downloading COMMONCYPTOLIB 8

5. Select your platform.

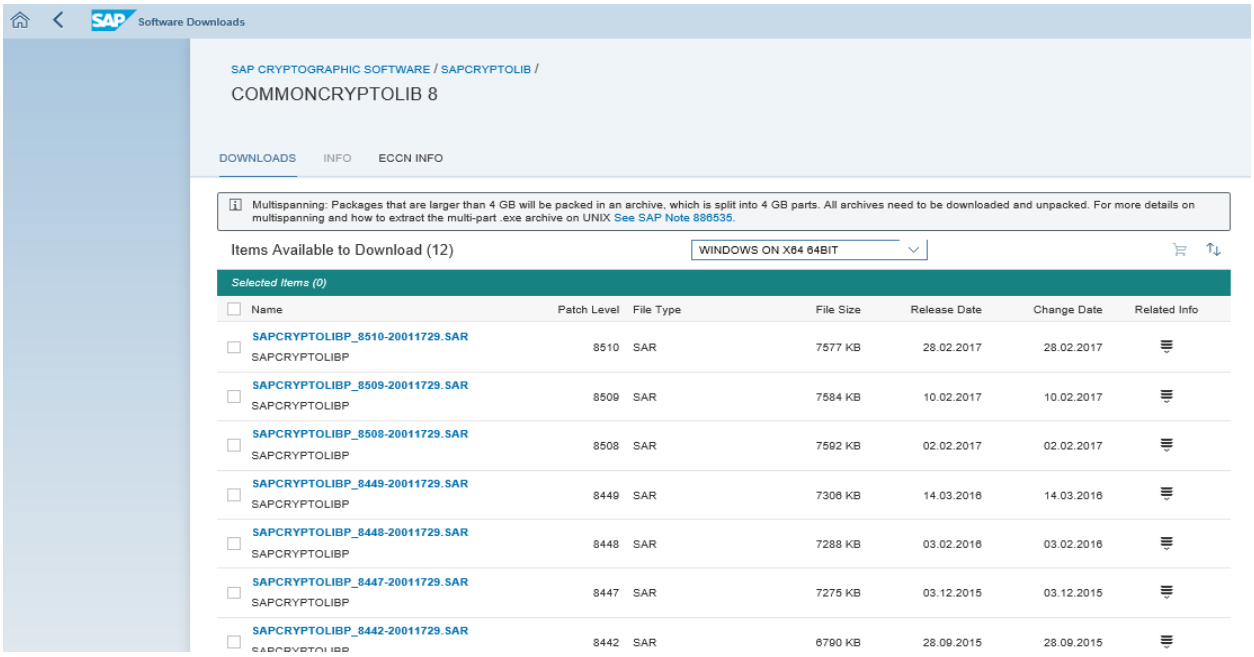


Figure 1-5 Selecting Your Platform

6. Download the latest version.

1.3 Installing the SAP Cryptography Software

To install the cryptography software, follow these steps.

1. You need the SAPCAR utility, available from the SAP download site, to extract the file you downloaded in 1.2 Downloading SAP Cryptography Software.
2. Extract the contents of the SAP Cryptographic Library installation package. The SAP cryptography is in this directory:

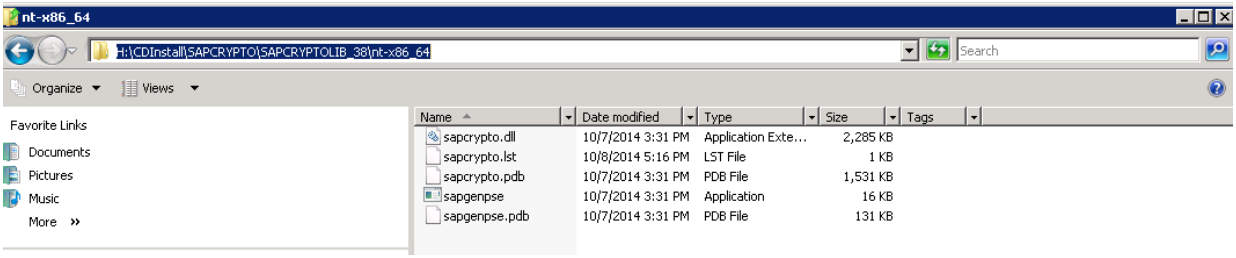


Figure 1-6 Extracting SAP Cryptographic Library Contents

3. Copy the library file and the configuration tool (`sapgenpse.exe`) to the directory specified by the application server's profile parameter `DIR_EXECUTABLE`. In the following example, this directory is represented with the notation $(`DIR_EXECUTABLE`).
4. Copy these library files to two locations:
   - `D:\usr\sap\GE2\DVEBMGS00\exe`
   - `D:\usr\sap\GE2\SYS\exe\uc\NTAMD64`
5. For both copies of the library files, follow these steps to check the permissions:
   a. Right-click `sapcrypto.dll` and select **Properties**.

b. Click the **Security** tab.

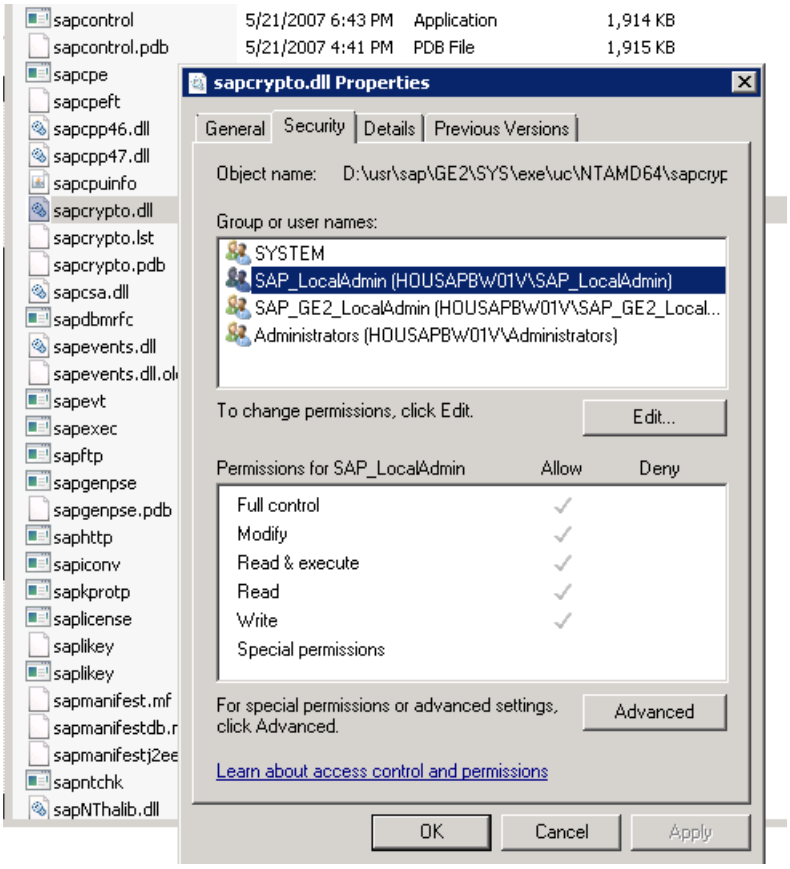


Figure 1-7 Checking DLL Permissions

c. Check the file permissions for the SAP Cryptographic Library. Make sure that `<sid>adm` (or `SAPService <SID>` under Windows) can execute the library's functions.

6. Locate the ticket `<DRIVE>:\usr\sap\<SID>\<instance>\sec\ticket`.

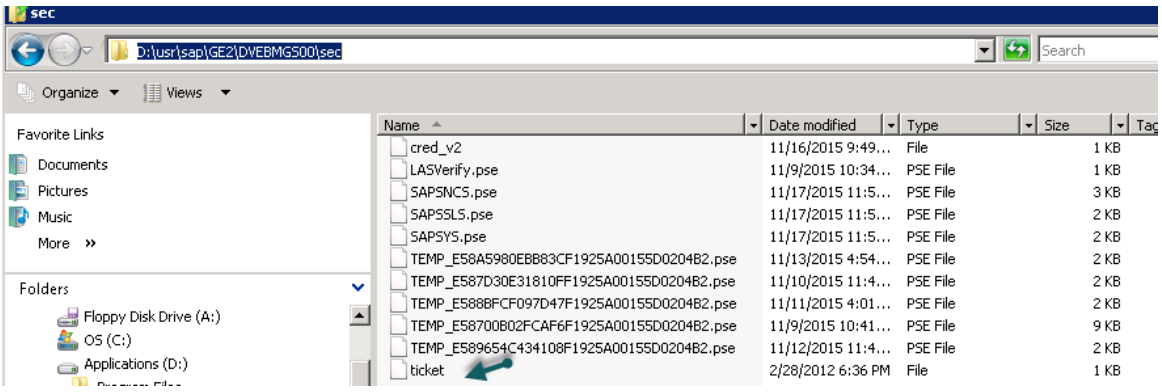


Figure 1-8 Locating the Ticket

7. Copy the ticket file to the sec subdirectory in the instance directory `$(DIR_INSTANCE)`, which is `DIR_INSTANCE`:

   `<DRIVE>:\usr\sap\<SID>\<instance>`

8. Set the environment variable SECUDIR to the sec subdirectory.

   The application server uses this variable to locate the ticket and its credentials at runtime. If you set the environment variable using the command line, the value may not be applied to the server's processes. Therefore, setting SECUDIR in the startup profile for the server's user or in the registry is recommended.

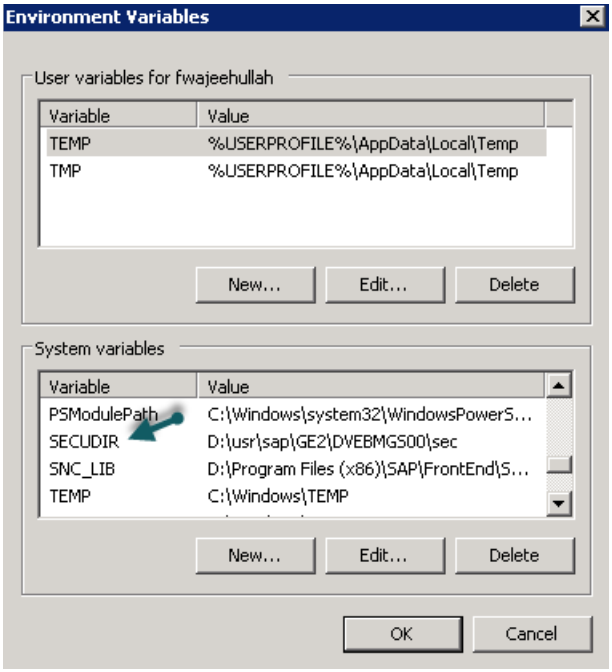
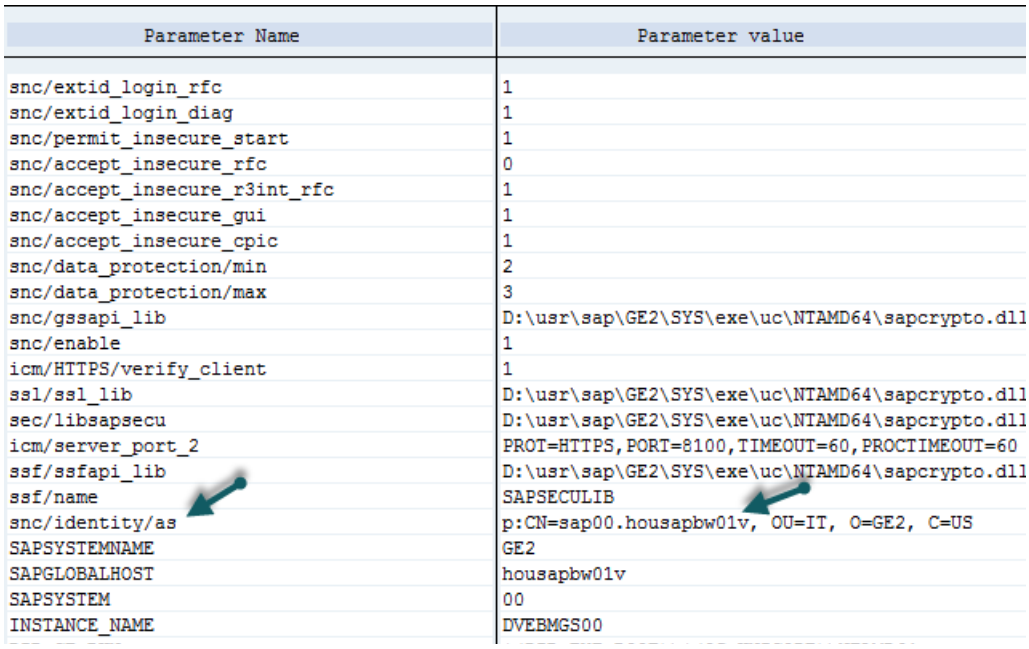


Figure 1-9 Setting the Environment Variable

1.4 Creating the PSE for the Server

To create the PSE for the server, follow these steps.

1. Start transaction **RZ10** and select the instance profile used by the server startup.



Parameter Name	Parameter value
snc/extid_login_rfc	1
snc/extid_login_diag	1
snc/permit_insecure_start	1
snc/accept_insecure_rfc	0
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cpic	1
snc/data_protection/min	2
snc/data_protection/max	3
snc/gssapi_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
snc/enable	1
icm/HTTPS/verify_client	1
ssl/ssl_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
sec/libsapsecu	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
icm/server_port_2	PROT=HTTPS,PORT=8100,TIMEOUT=60,PROCTIMEOUT=60
ssf/ssfapi_lib	D:\usr\sap\GE2\SYS\exe\uc\NTAMD64\sapcrypto.dll
ssf/name	SAPSECULIB
snc/identity/as	p:CN=sap00.housapbw01v, OU=IT, O=GE2, C=US
SAPSYSTEMNAME	GE2
SAPGLOBALHOST	housapbw01v
SAPSYSTEM	00
INSTANCE_NAME	DVEBMGS00

Figure 1-10 Selecting the Instance Profile for the Server Startup

2. Add the instance parameter `snc/identity/as`.
3. Set the instance parameter `snc/identity/as` to the specific name of the server. For example:

   ```
   snc/identity/as P:CN=sap00.housapbw01v; OU=IT. O=G2, C=US
   ```

   Do not forget to add *p:* in front of the name.

Note

While specifying the distinguished name for your Client/Server `P:CN=sap00.housapbw01v, OU-IT. O=G2, C=US`, the cryptographic tool validates the country code for the **C=xx** attribute.

---

4. Restart your server.

5. Create the SNC PSE.

Figure 1-11 Creating the SNC PSE

6. Start the **STRUST** transaction.
7. Right-click **SNC (SAPCryptolib)** and select **Create**.

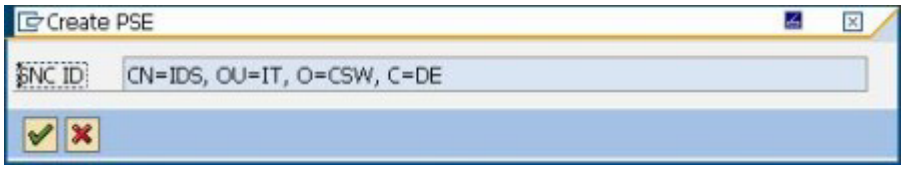


Figure 1-12 Selecting SAPCryptolib for the SNC

8. Accept the **SNC ID**, which is taken from the instance parameter `snc/identity/as`.
9. Double-click **SNC (SAPCryptolib)** and select **Assign Password** to add a password for the SNC (SAPCryptolib) PSE.

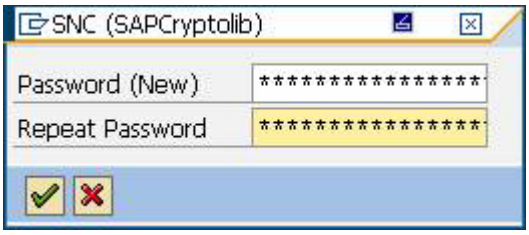


Figure 1-13 Assigning a Password for the SNC PSE

10. Type in a password. The password can contain both letters and numbers. Without the password, the server will not start when you set the instance parameter `snc/enable` to 1.
11. Save the settings.
12. Create the server `cred_v2` file.
13. After setting up the server PSE, create a file named *cred_v2*, which is used to give SAP secure access to the PSE without providing the password for the PSE.

```
C:\SAPCrypto>sapgenpse seclogin -p SAPSNCS.pse -O DV\SAPServiceGE2
```

Note:

`DV\SAPServiceGE2` should be the account SAP runs under on the server.

---

14. At the text **Please enter PIN:**, type in your PIN.

15. At the text **Added SSO-credentials for PSE <your path>/SAPSNCS.pse**, enter

```
"P:CN=sap00.housapbw01v, OU-IT. O=G2, C=US
```

1.5 Setting SNC Additional Parameters

Follow these steps to enable **Add Additional SNC parameters**.

1. Start transaction **RZ10**.

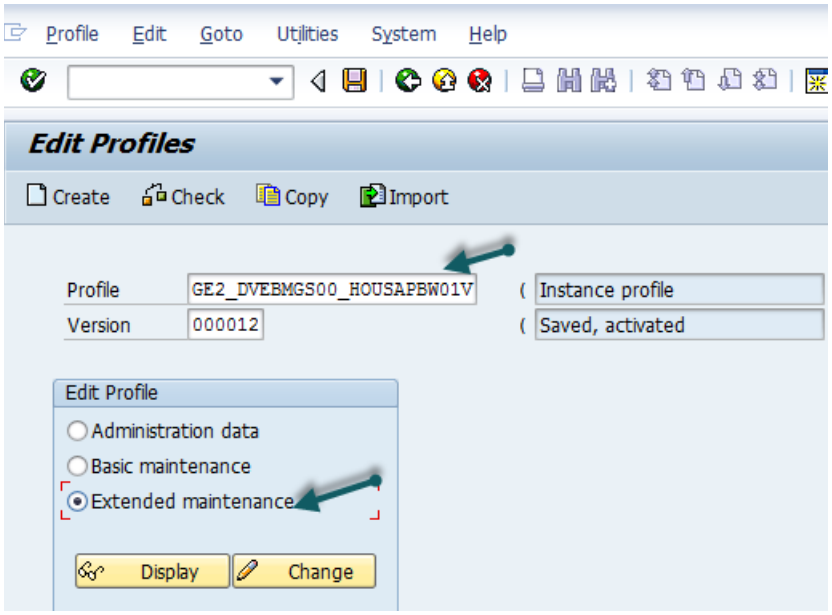


Figure 1-14 Starting Transaction RZ10

2. Select the instance profile used by the server startup.

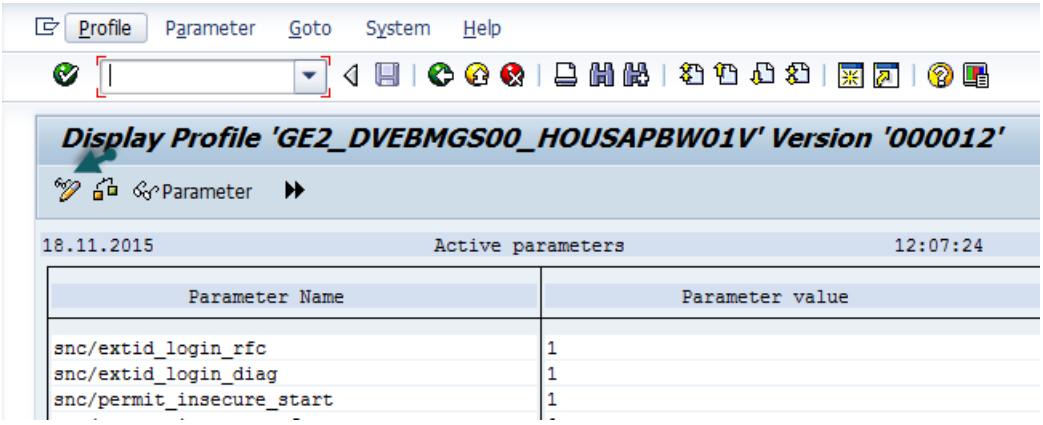


Figure 1-15 Selecting the Instance Profile

3. Click the **Change** button.

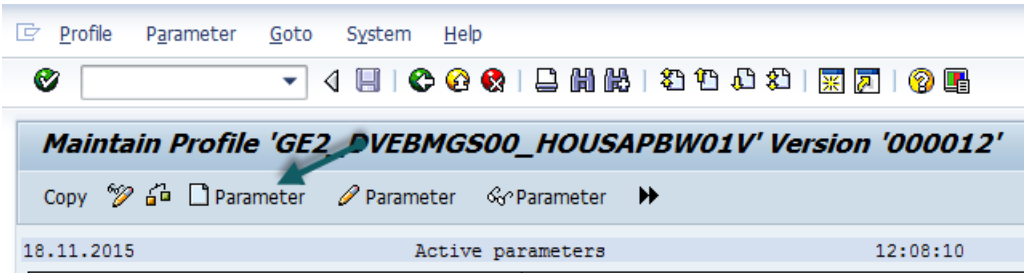


Figure 1-16 Changing the Parameter

4. Click **Create Parameter**.

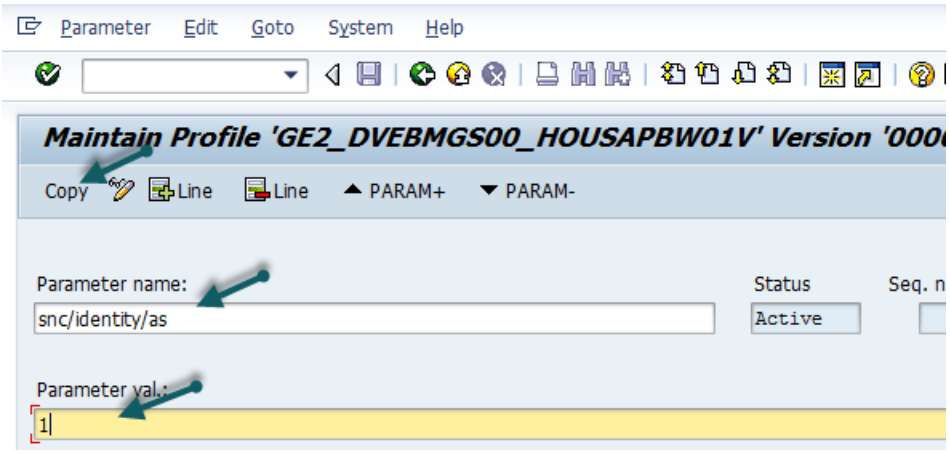


Figure 1-17 Creating the Parameter

5. Add the **Parameter** name and value.

Table 1-1 SNC Profile Parameters

Profile Parameter	Value	Example
`snc/enable`	1	1
`snc/gssapi_lib`	Path and filename where the SAP Cryptographic Library is located	UNIX: `usr/sap/<SID>/SYS/exe/ run/libsapcrypto.so` Windows: `D:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll`
`snc/identity/as`	Application server's SNC name Syntax: `p:<Distinguished_Name>` The Distinguished Name part must match the Distinguished Name that you specify when creating the SNC PSE.	`p:CN=ABC, OU=Test, O=MyCompany, C=US`

Table 1-1 SNC Profile Parameters (Continued)

Profile Parameter	Value	Example
snc/data_protection/max	1: Authentication only 2: Integrity protection 3: Privacy protection	3
snc/data_protection/min	1: Authentication only 2: Integrity protection 3: Privacy protection	1
snc/data_protection/use	1: Authentication only 2: Integrity protection 3: Privacy protection 9: Use the value from snc/data_protection/max	9
snc/accept_insecure_cpic	0: do not accept 1: accept	1
snc/accept_insecure_gui	0: do not accept 1: accept	1
snc/accept_insecure_r3int_rfc	0: do not accept 1: accept	1
snc/accept_insecure_rfc	0: do not accept 1: accept	1
snc/r3int_rfc_secure	0: Internal RFCs are unprotected 1: Internal RFCs are protected with SNC	1
snc/r3int_rfc_qop	1: Secure authentication only 2: Data integrity protection 3: Data privacy protection 8: Use the value from snc/data_protection/use 9: Use the value from snc/data_protection/max	8

6. Repeat steps 2 to 5 for all parameters.
7. Save the settings.
8. Restart the SAP Application server.

1.6 Creating PSE for RFC Client i-e for ERP-link iNet Connection Service

This section contains steps for configuring SAP cryptography on the RFC Client side (i.e., ERP-link Connection Service).

1.6.1 Installing SAP Cryptography on the Gimmal Connection Service Machine

Follow these steps.

1. Log on to the ERP-link server machine where the Connection Service is running.

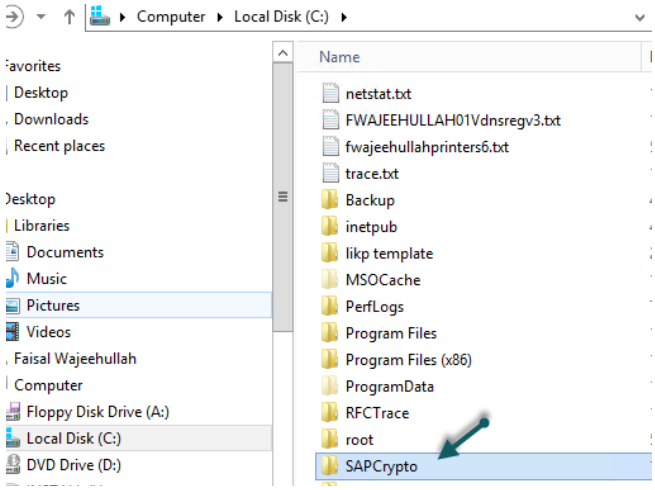


Figure 1-18 Logging onto the ERP-Link Server

2. Create a directory named *SAPCrypto* and make sure the login account has full permission to the directory.

3. Make sure you set the `SECUDIR` environment variable to the directory `SAPCrypto` and copy the library to a different directory.

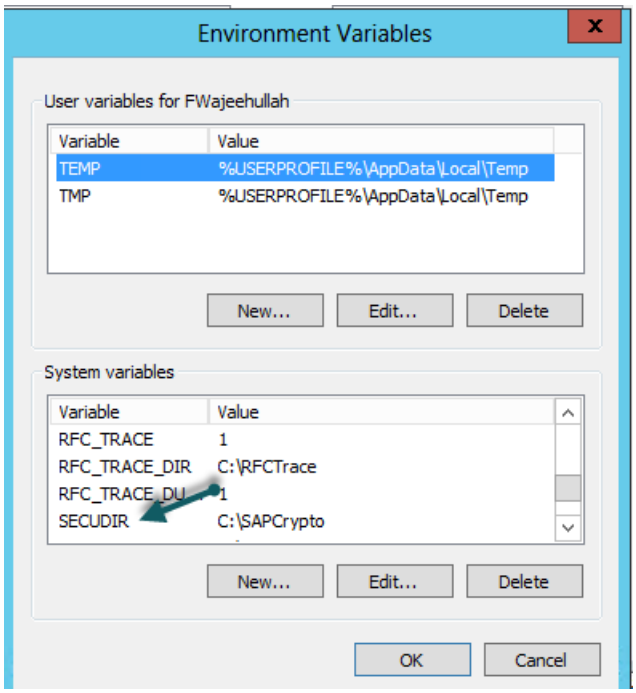


Figure 1-19 Setting the Environment Variable

4. Add this path to your **PATH** environment variable.

1.6.2 Creating Client PSE

Follow these steps to create the client PSE.

1. Launch the `cmd` process as an admin.
2. Change the directory to `C:\SAPCrypto` directory.
3. Issue the following command:

```
C:\SAPCrypto>sapgenpse gen_pse -v -p RFC.pse
```

4. You will have to provide the PIN and the distinguished name (DN) of the user.

```
===========================================================
 Got absolute PSE path "C:\SAPCrypto\RFC.pse".
Please enter PIN:
Please reenter PIN:
get_pse: Distinguished name of PSE owner: CN=RFC, OU=IT, O=GE, C=US
     Supplied distinguished name: "CN=RFC, OU=IT, O=GE, C=US"
Creating PSE with format v2 (default)
Generating key (RSA, 2048-bits) ... succeeded.
 Certificate creation... ok
```

```
 PSE update... ok
 PKRoot... ok
Generating certificate request... ok.
PKCS#10 certificate request for "C:\SAPCrypto\RFC.pse":
-----BEGIN CERTIFICATE REQUEST-----
MIICejCCAWICAQAwNTELMAkGA1UEBhMCVVMxCzAJBgNVBAoTAkdFMQswCQYDVQQL
EwJJVDEMMAoGA1UEAxMDUkZDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA/+xtO0KoMapkf7GThgOFEBM62OSZU6ptDd6/drOm/HLvYNVtBF9bWTp67NAt
o4qhLwF0YEvRhT+1b5Ac5G7a4CppW0rFyew81naPaO1yGqjCQTTesM44QXC5pBrj
PP+Om6Q8FtLRfnpBGiKu1MsABFnIln/R3rTXj9mLEAd43nvN8w7LL+mL9g/1ZyC8
KGGsG74oKsPM5jP5/FBBzlh8jgjMtCWJWPOV9qunToTWwBV1drXmOpJy2xcfA7Qy
n+H3yhO8WrBVQb85IsEy3udeJEeZqKyM363GEiaiXn5ZqsBYJb1dqxMM7nVkTpOs
eF0ftZMaU6HbThg29NjACsD5aQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAEX+
xdvffsiCP71I2N/U3/s5l1/E5wS7aFRfxX86tcuVEFx+QRkoMAxVRwQu6tfGTCY2
EPTagbNFx1+Txjks48j/sbgzrv4yllKdf9Nw1pDcjYAZRzTYrbyj6HNqNWUdaphS
+Inc/HP5Tn4CEwHI6yvOBcVuT2wANJOQV5e+b6LHwUC+9OwER+Jq4p2VmH/oI2zf
/sHNyWYNnKmQuvGpA3eI5gtlscU1OZzrWQT+lMLiR411pJIlDcaS0eZQDLbBczm5
ftNMGIdRq5xU+hYG4VaCVGH2R70B3mIOrc+2hpRI7hnf2pqmtTxknOXQO7WdfaNg
8l+6GH6DOQpvosSpKyU=
-----END CERTIFICATE REQUEST---
```

1.6.3 Importing and Exporting Client Certificates between Client PSE and SAP Application Server

For the Client RFC to communicate successfully with the SAP Application server, you must take the application server's certificate in STRUST and put it into the client's PSE. You must also take the RFC client's user certificate and add it to the server's PSE (typically via STRUST).

You can retrieve the certificates by following these steps.

1. Log in to `cmd` as an admin and issue the following command:

   ```
   C:\SAPCrypto>sapgenpse export_own_cert -v -p RFC.pse -o RFC.crt
   ```

2. The following text displays.

   ```
    Opening PSE "C:\SAPCrypto\RFC.pse"...
    No SSO credentials found for this PSE.
   Please enter PIN:
    PSE (v2) open ok.
   Retrieving my certificate... ok.
    Writing to file (PEM-framed base64-encoded)... ok.
   ```

Note:

The `RFC.pse` file is under the `c:\SAPCrypto` directory.

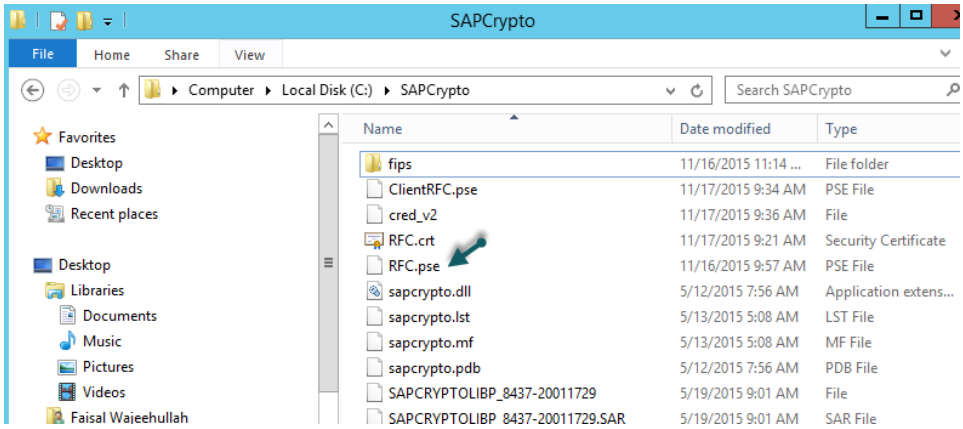


Figure 1-20 Location of the RFC.pse File

Importing the Client Certificate to Server PSE

You can import the client certificate via transaction **STRUST**.

1. Open the **Node SNC (SAPCryptolib)**.

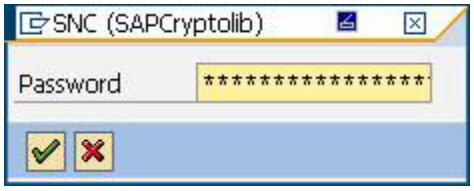


Figure 1-21 Opening the Node SNC

2. Provide the password set when prompted.

Figure 1-22 Selecting Import Certificate

3. Click the **Import certificate** button.

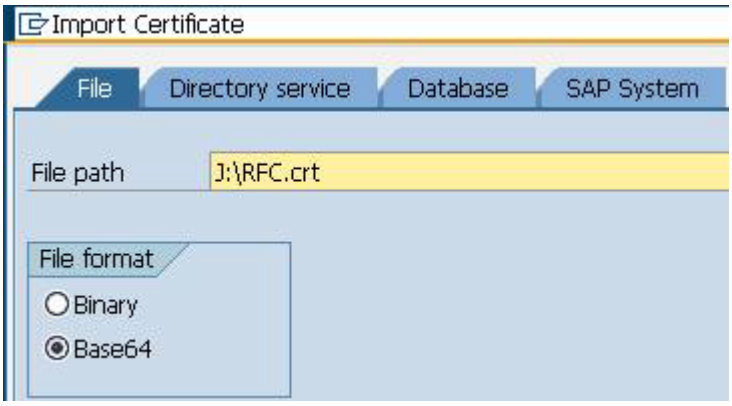


Figure 1-23 Importing the Certificate

4. Select **File format** *Base64* and select the file.

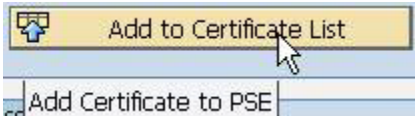


Figure 1-24 Adding the Certificate

5. Click **Add to Certificate List**. The certificate displays in the certificate list in SNC (SAP-Cryptolib).

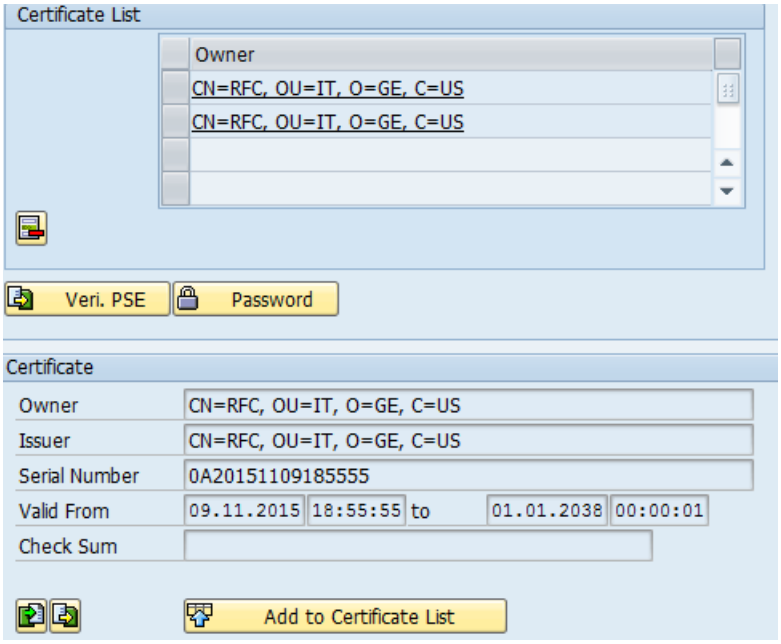


Figure 1-25 Verifying the Certificate

Note:

Two different certificates in the `certificate list.sap`.

Exporting the Server Certificate

To export the server certificate, follow these steps.

1. In the STRUST node SNC (SAPCryptolib), double-click on your server's certificate to display it in the **Certificate** field.
2. Click **Export certificate**.
3. At node **SNC (SAPCryptolib)**, double-click your server's certificate to display it in the **Certificate** field.
4. Click **Export certificate**.
5. Click the **File** tab.

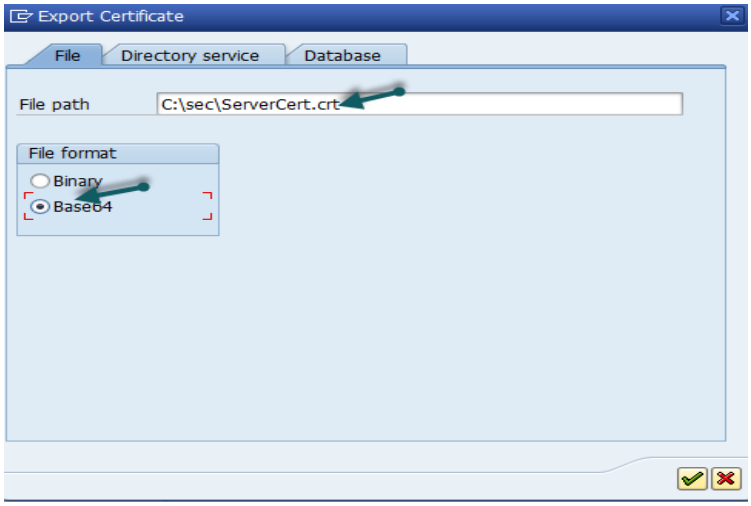


Figure 1-26 Exporting the Certificate

6. Select **Base64** for the **File format** and provide a name for the file.
7. Click the **Ok** button.

Importing the Server Certificate to the Client PSE

To import your server's certificate to the client PSE, follow these steps.

1. Copy the server certificate that you saved in Exporting the Server Certificate to the ERP-link iNet Connection Service machine.

2. Issue the following command from the command prompt:

Note:

You have to provide the pin you set earlier. //?

```
C:\SAPCrypto>sapgenpse maintain_pk -v -a C:\SAPCrypto\ServerRFC.crt -p C:\SAP-
Crypto\RFC.pse

 Opening PSE "C:\SAPCrypto\RFC.pse"...

 No SSO credentials found for this PSE.

Please enter PIN:

 PSE (v2) open ok.

 retrieving PKList

 Adding new certificate from file "C:\SAPCrypto\ServerRFC.crt"

----------

Subject : CN=housapbw01v.dv.local, OU=IT, O=GE, C=US

Issuer  : CN=housapbw01v.dv.local, OU=IT, O=GE, C=US

Serialno: 0A:20:15:11:08:18:06:26

KeyInfo : RSA, 1024-bit

Validity  -  NotBefore:   Sun Nov 08 12:06:26 2015 (151108180626Z)

NotAfter:   Thu Dec 31 18:00:01 2037 (380101000001Z)
```

1.6.4 Creating the cred_v2 File

After setting up the client PSE, you must create a file called `cred_v2`, which is used to give the RFC Program (iNet CS) secure access to the PSE without providing the password for the PSE.

Note

The `cred_v2` file is created through calling `sapgenpse` using the `seclogin` parameter. It is created in the same directory as the `.pse` file.

---

1. Run this operating:

```
C:\SAPCrypto>sapgenpse seclogin -p RFC.pse -O DV\ConnectorService
```

Note:

`DV\ConnectorService` should be the account that the iNetRemote service or the Connector 5.0 Application pool account is using.

2. Enter information as you are requested to do so.

```
Please enter PIN: ********

Added SSO-credentials for PSE "<your path>/RFC.pse"

"CN=RFC, OU=IT, O=CSW, C=DE
```

Run this operation for each user account that might need to access the PSE file.

1.7 Configuring SAP for Secure Network Communications

Now you need to map the x.509 certificates that were created for the user accounts on the SAP Server.

1.7.1 Allowing SNC Connection with RFC

Perform these steps to allow Secure Network Communications to connect with the RFC.

1. Start transaction **SM30**.

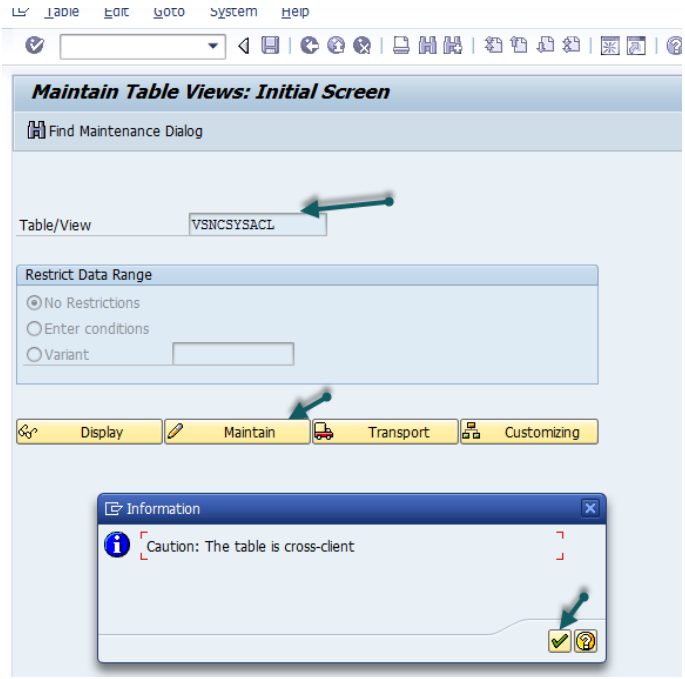


Figure 1-27 Starting Transaction SM30

2. Enter the **View** *VSNCSYSACL*. This view restricts the SNC RFC Connections by an Access Control List (ACL).
3. When an alert displays, click the **right** button on the bottom.

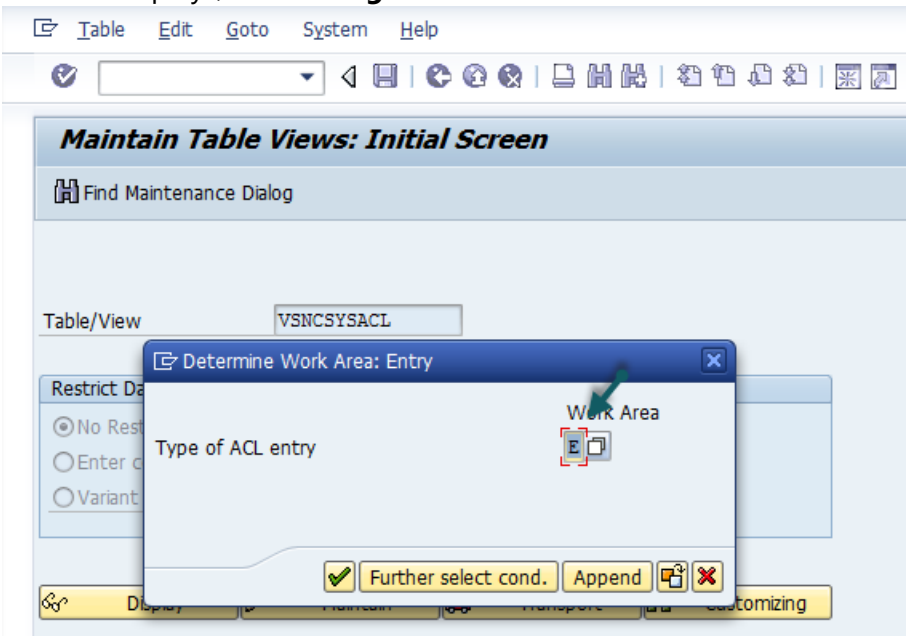


Figure 1-28 Selecting ACL Entry

4. Select *E* for the **Type of ACL entry** and click the **right** button on the bottom.

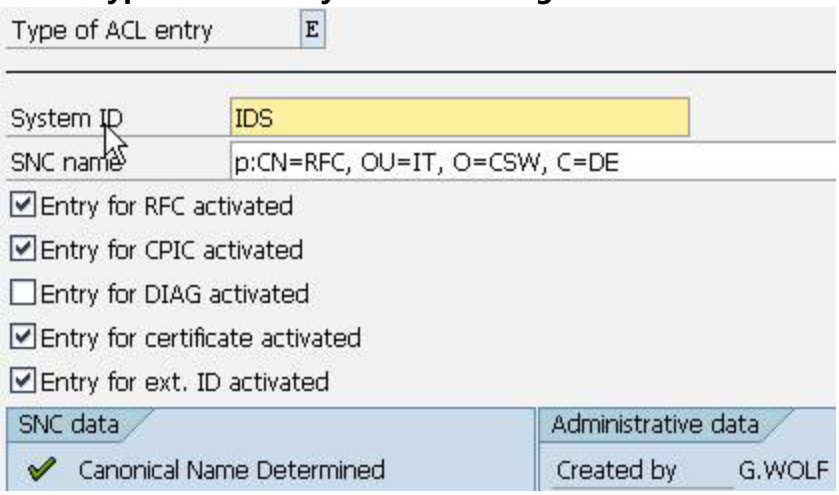


Figure 1-29 Selecting Type of ACL Entry

5. Enter **System ID** and **SNC name**.

Note:

Do not forget the `p:` in front of the DN.

---

6. Select the following check boxes:
   - Entry for RFC activated
   - Entry for CPIC activated
   - Entry for certificate activated
   - Entry for ext. ID activated
7. Save the entry.

Note:

When trying to edit the entry, you might see an alert window display. Click the **right** symbol and make your changes.

1.7.2 Mapping X.509 Certificate to User

To map the X.509 Certificate to the user for a successful login, follow these steps.

1. Start **Transaction SM30**.
2. Enter *VUSREXTID* and click **Maintain**.
3. Using the view **VUSREXTID**, set up a mapping between the **DistinguishedName** provided by an X.509 Certificate and an ABAP User.

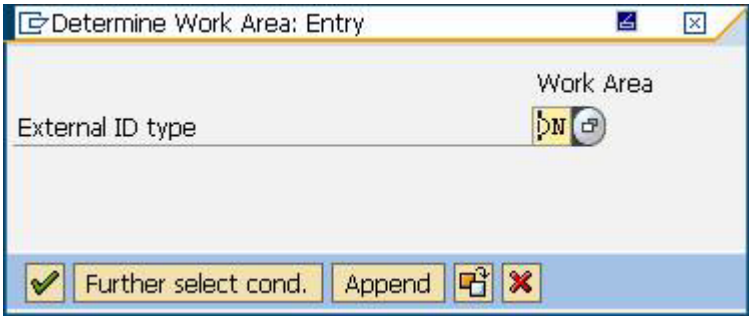


Figure 1-30 Setting Mapping

4. Select the **Distinguished Name** for the **External ID type**.

5. Create a new entry and activate it.

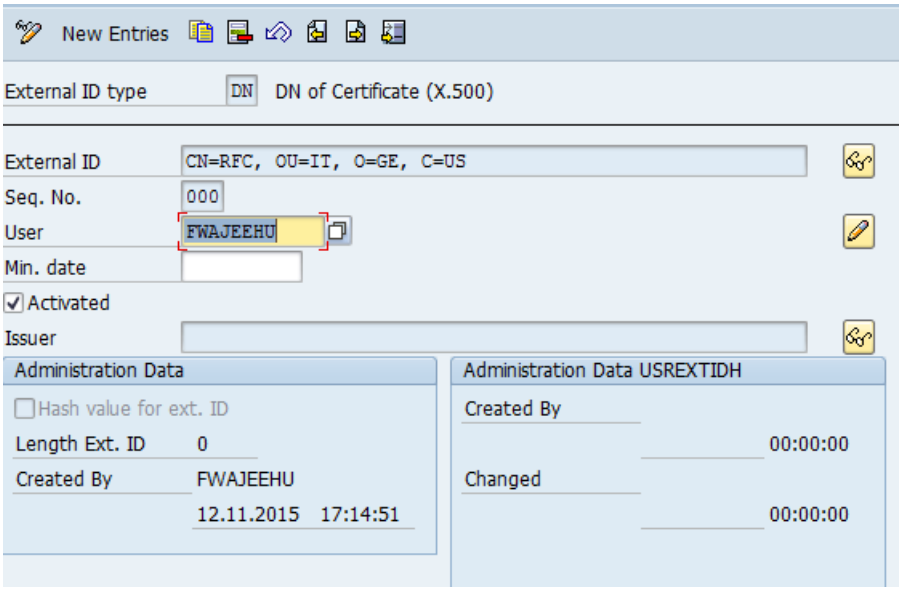


Figure 1-31 Activating Mapping

6. Save the entry.

1.8 Configuring Connection Service for SNC

This section contains the steps necessary to configure the Connection Service to use SNC.

1.8.1 Configuring SNC for iNet Connection Service

Before starting these steps, make sure that the ERP-link product has been installed and configured. Refer to the latest version of the *ERP-link Installation and Administration Guide* for more information.

1. Log in to the iNetCSAdmin Console.
2. Click the Connection Pool to configure the connection settings.

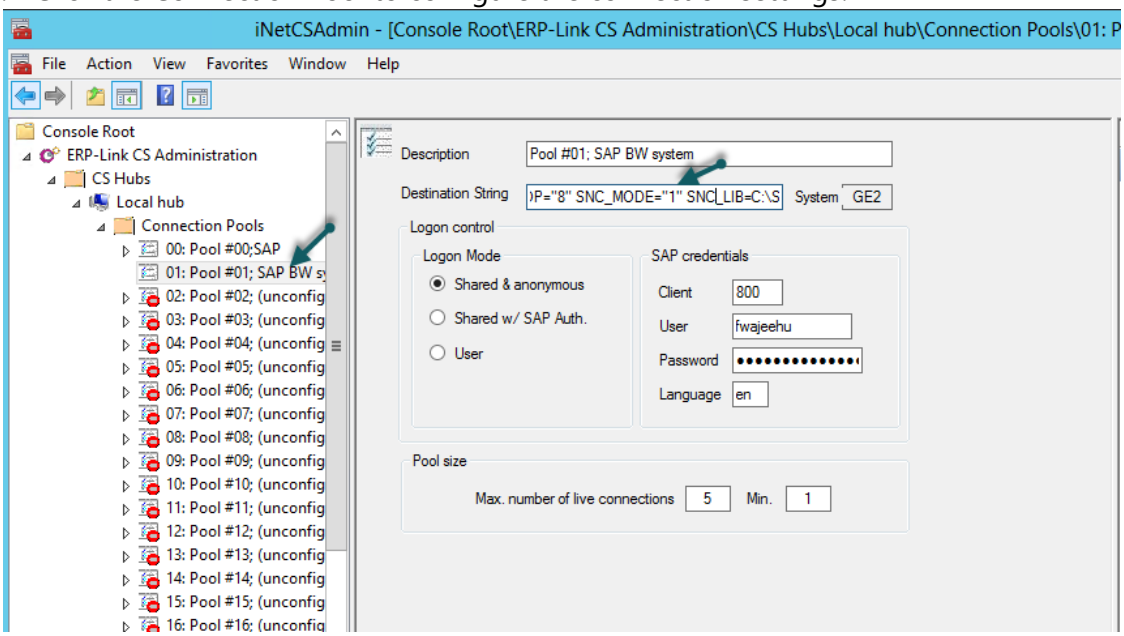


Figure 1-32 Selecting the Connection Pool

3. To configure SNC settings to be used by iNet CS, provide this information:

```
Destination string: ASHOST=housapbw01v SYSNR=00 SNC_PARTNERNAME="p: CN=sap00.housap-
bw01v, OU=IT, O=GE2, C=US" SNC_MYNAME="p: CN=RFC, OU=IT, O=GE, C=US" SNC_QOP="8"
SNC_MODE="1" SNC_LIB=C:\SAPCrypto\sapcrypto.dll
```

Note:

`SNC_MODE =1` means that SNC is enabled

---

4. Select and enter all the other settings on the screen, such as **Logon mode** and the **SAP credentials**.

5. After completing all the configuration details, click **Validate**.

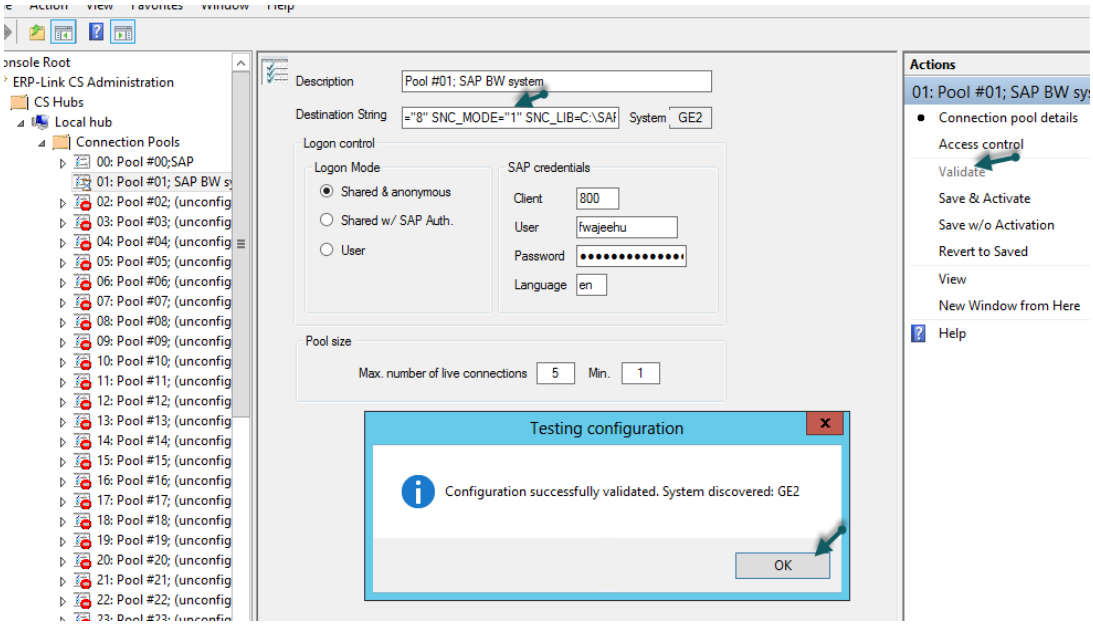


Figure 1-33 Validating the Connection

6. If the SNC is properly configured, you should see the message *Configuration successfully validated. System GE2*. Click **OK**.
7. **Save** and then **Activate** to save the configuration.

Configuring Connector 5.0 for SNC

1. Display the Admin console settings,
2. Make sure the `RFC.PSE` and the `cred_v2` files are copied to:

   `C:\Windows\System32\config\systemprofile\AppData\Local\sec` – If the directories do not exist, they need to be created.

1.8.2 Testing SNC Using the Gimmal Connection Service

Follow these steps to test if SNC is correctly set up.

1. Run the transaction **RZ10**.

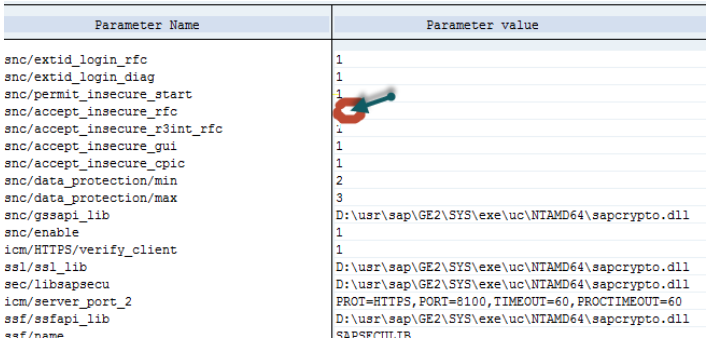


Figure 1-34 Running the RZ10 Transaction

2. Make sure the parameter `snc/accept_insecure_rfc` is set to 0 (zero), which means *do not accept any insecure connections*.
3. From the iNetCs administration console, set the SNC_MODE =1 to disable SNC.
4. Now attempt to validate a connection. A message similar to the following displays:

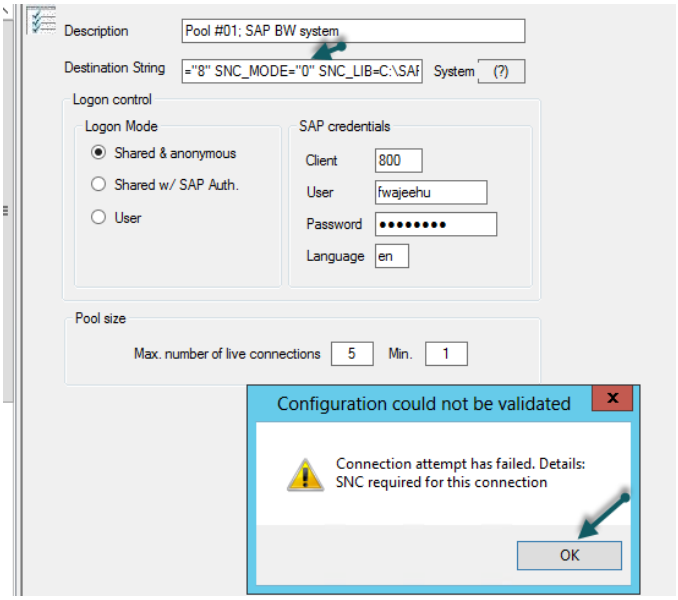


Figure 1-35 Validating the Connection

This message indicates that SNC must be active on the RFC client, and in this case, iNet CS service can make a connection to SAP.

5. Click **OK**.

6. When you enable the SNC on iNet Cs service, the connection should be successful.

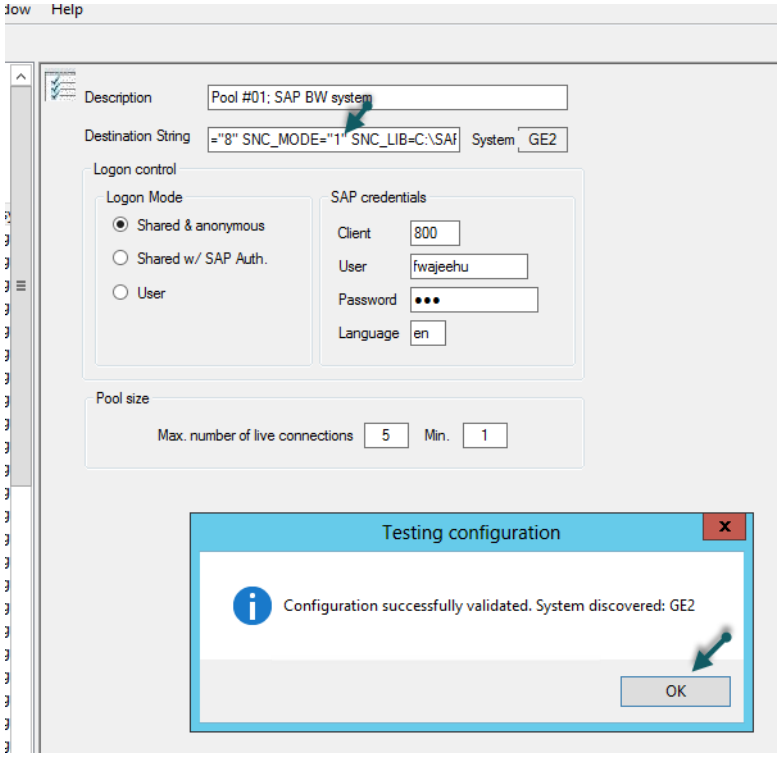


Figure 1-36 Successful Connection Message