

How to Configure Open SSL for SAP HANA Studio to SAP HANA Server

To Secure Communication Between SAP HANA Studio and SAP HANA Server

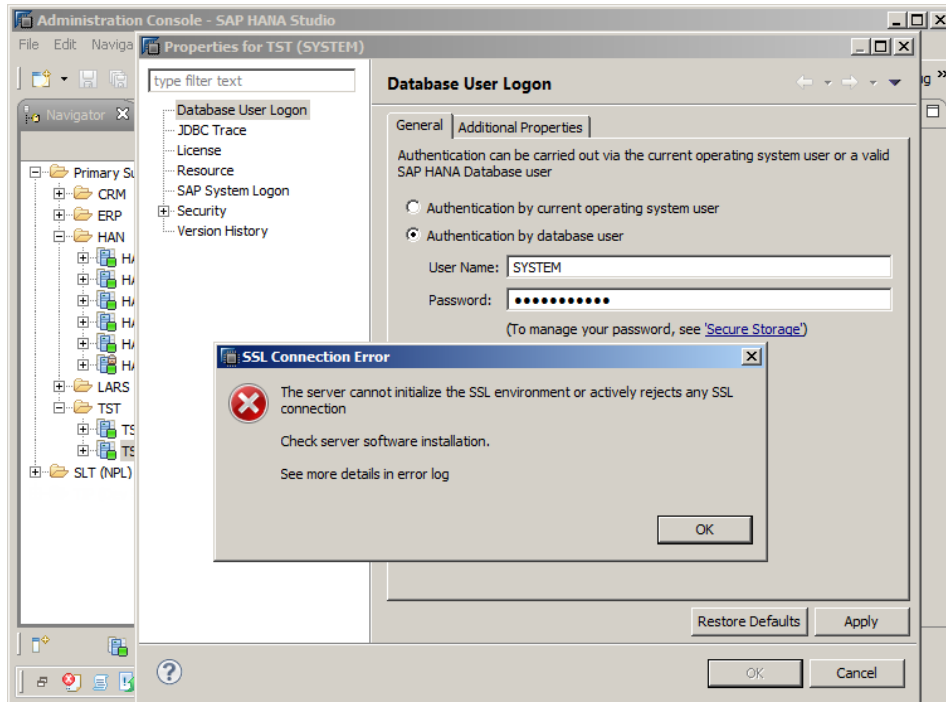
TABLE OF CONTENTS

	SYMPTOM WHEN SSL IS NOT CONFIGURED	3
1	CONFIGURE SAP HANA SERVER TO SUPPORT SSL.....	4
1.1	Create the Root Certificate	4
1.2	Create the Server Certificate	5
1.3	Sign the Server Certificate.....	6
1.4	Chain the Certificate.....	7
1.5	Copy the Certificate to Trust.pem.....	7
2	RESTART HANA SERVER.....	9
3	CONFIGURE SAP HANA CLIENT TO SUPPORT SSL.....	10
3.1	Import 'trust.pem' into the Java keystore on the client.....	10
3.2	Enable SSL Communication within HANA Studio.....	12

SAP HANA Server and SAP HANA Studio are not delivered by hardware vendors with secure socket layer (SSL) communication enabled. As an added layer of security SAP HANA Administrators are encouraged to enable SSL communication between SAP HANA server nodes, between SAP HANA clients, as well as between SAP HANA Studio and SAP HANA Server. SAP HANA supports use of either the SAPCrypto libraries or OpenSSL to secure communication. This guide walks through the steps required to configure and enable OpenSSL communication between SAP HANA Studio and SAP HANA Server.

SYMPTOM WHEN SSL IS NOT CONFIGURED

Following is a screenshot of the error received when attempting to enable SSL communication between HANA Studio and HANA server when SSL has not been properly configured.



Details in the error log can be found in the IndexServer_alert_*.trc diagnostics file in HANA Studio's Administrative perspective, and shows the following:

```
[3747]{0}{0} 2013-03-12 12:14:06.921974 e SQLSession sm_handler.cc(00242) : (sockfd:135, part:<not assigned>) Cannot create SSL context: $ErrorText$
```

1 CONFIGURE SAP HANA SERVER TO SUPPORT SSL

As user 'root', check for existence of libssl.so, if the file does not exist create a symbolic link to libssl.so.0.9.8:

```
vanp9lnxc25b6:/ # ls -l /usr/lib64 |grep ssl

-rwxr-xr-x 1 root root 267160 2012-04-25 15:10 libssl3.so
-r-xr-xr-x 1 root root 343040 2012-05-03 09:02 libssl.so.0.9.8
-rw-r--r-- 1 root root 65 2012-05-03 09:03 .libssl.so.0.9.8.hmac

vanp9lnxc25b6:/ # ln -s /usr/lib64/libssl.so.0.9.8 /usr/lib64/libssl.so

vanp9lnxc25b6:/ # ls -l /usr/lib64 |grep ssl

-rwxr-xr-x 1 root root 267160 2012-04-25 15:10 libssl3.so
lrwxrwxrwx 1 root root 26 2013-03-11 17:55 libssl.so -> /usr/lib64/libssl.so.0.9.8 <-
-r-xr-xr-x 1 root root 343040 2012-05-03 09:02 libssl.so.0.9.8
-rw-r--r-- 1 root root 65 2012-05-03 09:03 .libssl.so.0.9.8.hmac
```

1.1 Create the Root Certificate

As user '<sid>adm' create the root certificate, as follows:

```
vanp9lnxc25b6:/usr/home > cd /usr/sap/<sid>/home

vanp9lnxc25b6:~> pwd

/usr/sap/HAN/home

vanp9lnxc25b6:~>

vanp9lnxc25b6:~> mkdir .ssl

vanp9lnxc25b6:~> cd .ssl

vanp9lnxc25b6:~/./ssl> openssl req -new -x509 -newkey rsa:2048 -days 3650 -sha1 -keyout CA_Key.pem -
out CA_Cert.pem -extensions v3_ca

Generating a 2048 bit RSA private key
.....+++
.....+++

writing new private key to 'CA_Key.pem'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

-----

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:CA

State or Province Name (full name) [Some-State]:British Columbia

Locality Name (eg, city) []:Vancouver

Organization Name (eg, company) [Internet Widgits Pty Ltd]:SAP

Organizational Unit Name (eg, section) []:AGS

Common Name (eg, YOUR name) []:HANA Server HAN

Email Address []:

vanp9lnxc25b6:~/./ssl>

vanp9lnxc25b6:~/./ssl> ls -l *.pem

-rw-r--r-- 1 <sid>adm sapsys 1533 2013-03-11 18:03 CA_Cert.pem

-rw-r--r-- 1 <sid>adm sapsys 1743 2013-03-11 18:03 CA_Key.pem
```

1.2 Create the Server Certificate

As user <sid>adm create the server certificate as follows:

```
vanp9lnxc25b6:~/./ssl> cd /usr/sap/<sid>/home/ssl

vanp9lnxc25b6:~/./ssl> openssl req -newkey rsa:2048 -days 365 -sha1 -keyout Server_Key.pem -out
Server_Req.pem -nodes

Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'Server_Key.pem'

-----

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----
```

```
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:British Columbia
Locality Name (eg, city) []:Vancouver
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SAP
Organizational Unit Name (eg, section) []:AGS
Common Name (eg, YOUR name) []:vanpglncx25b6.pgdev.sap.corp
Email Address []:.
```

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

```
vanpglncx25b6:~/.ssl> ls -l *.pem
-rw-r--r-- 1 hanadm sapsys 1533 2013-03-11 18:03 CA_Cert.pem
-rw-r--r-- 1 hanadm sapsys 1743 2013-03-11 18:03 CA_Key.pem
-rw-r--r-- 1 hanadm sapsys 1675 2013-03-11 18:13 Server_Key.pem
-rw-r--r-- 1 hanadm sapsys 1037 2013-03-11 18:13 Server_Req.pem
```

1.3 Sign the Server Certificate

As user <sid>adm, sign the certificate:

```
vanpglncx25b6:~/.ssl> cd /usr/sap/<sid>/home/.ssl
vanpglncx25b6:~/.ssl> openssl x509 -req -days 365 -in Server_Req.pem -sha1 -extfile
/etc/ssl/openssl.cnf -extensions usr_cert -CA CA_Cert.pem -CAkey CA_Key.pem -CAcreateserial -out
Server_Cert.pem
Signature ok
subject=/C=CA/ST=British Columbia/L=Vancouver/O=SAP/OU=AGS/CN=vanpglncx25b6.pgdev.sap.corp
Getting CA Private Key
Enter pass phrase for CA_Key.pem: Secret123!      <- Use a secure password
```

Confirm creation of Server_Cert.pem and CA_Cert.srl:

```
vanpglncx25b6:~/.ssl> ls -l
total 24
-rw-r--r-- 1 hanadm sapsys 1533 2013-03-11 18:03 CA_Cert.pem
-rw-r--r-- 1 hanadm sapsys 17 2013-03-11 18:19 CA_Cert.srl      <
```

```
-rw-r--r-- 1 hanadm sapsys 1743 2013-03-11 18:03 CA_Key.pem
-rw-r--r-- 1 hanadm sapsys 1424 2013-03-11 18:19 Server_Cert.pem ←
-rw-r--r-- 1 hanadm sapsys 1675 2013-03-11 18:13 Server_Key.pem
-rw-r--r-- 1 hanadm sapsys 1037 2013-03-11 18:13 Server_Req.pem
```

1.4 Chain the Certificate

As user <sid>adm chain the certificate:

```
vanp9lnxc25b6:~/ssl> cd /usr/sap/<sid>/home/ssl
vanp9lnxc25b6:~/ssl> cat Server_Cert.pem Server_Key.pem CA_Cert.pem > key.pem
vanp9lnxc25b6:~/ssl> ls -l
total 32
-rw-r--r-- 1 hanadm sapsys 1533 2013-03-11 18:03 CA_Cert.pem
-rw-r--r-- 1 hanadm sapsys 17 2013-03-11 18:19 CA_Cert.srl
-rw-r--r-- 1 hanadm sapsys 1743 2013-03-11 18:03 CA_Key.pem
-rw-r--r-- 1 hanadm sapsys 4632 2013-03-11 18:26 key.pem ←
-rw-r--r-- 1 hanadm sapsys 1424 2013-03-11 18:19 Server_Cert.pem
-rw-r--r-- 1 hanadm sapsys 1675 2013-03-11 18:13 Server_Key.pem
-rw-r--r-- 1 hanadm sapsys 1037 2013-03-11 18:13 Server_Req.pem
vanp9lnxc25b6:~/ssl> cat key.pem
-----BEGIN CERTIFICATE-----
<Certificate content not displayed for this How To Guide>
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
<Certificate content not displayed for this How To Guide>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Certificate content not displayed for this How To Guide>
-----END CERTIFICATE-----
```

1.5 Copy the Certificate to Trust.pem

As user <sid>adm copy the certificate:

```
vanp9lnxc25b6:~/ssl> cd /usr/sap/<sid>/home/ssl
```

```
vanp9lnxc25b6:~/ssl> cp CA_Cert.pem trust.pem  
  
vanp9lnxc25b6:~/ssl> ls -l  
  
total 36  
  
-rw-r--r-- 1 hanadm sapsys 1533 2013-03-11 18:03 CA_Cert.pem  
-rw-r--r-- 1 hanadm sapsys  17 2013-03-11 18:19 CA_Cert.srl  
-rw-r--r-- 1 hanadm sapsys 1743 2013-03-11 18:03 CA_Key.pem  
-rw-r--r-- 1 hanadm sapsys 4632 2013-03-11 18:26 key.pem  
-rw-r--r-- 1 hanadm sapsys 1424 2013-03-11 18:19 Server_Cert.pem  
-rw-r--r-- 1 hanadm sapsys 1675 2013-03-11 18:13 Server_Key.pem  
-rw-r--r-- 1 hanadm sapsys 1037 2013-03-11 18:13 Server_Req.pem  
-rw-r--r-- 1 hanadm sapsys 1533 2013-03-11 18:33 trust.pem ←  
  
vanp9lnxc25b6:~/ssl>
```


2 RESTART HANA SERVER

As user <sid>adm, stop and start the SAP HANA Server:

```
vanp9lnxc25b6:~> cd /usr/sap/<sid>/HDB<inst#>

vanp9lnxc25b6:/usr/sap/HAN/HDB00> ./HDB stop

hdbdaemon will wait maximal 300 seconds for NewDB services finishing.

Stopping instance using: /usr/sap/HAN/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function
StopWait 400 2

11.03.2013 18:37:49

Stop

OK

11.03.2013 18:38:45

StopWait

OK

hdbdaemon is stopped.

vanp9lnxc25b6:/usr/sap/HAN/HDB00> ./HDB start

StartService

OK

OK

Starting instance using: /usr/sap/HAN/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function
StartWait 2700 2

11.03.2013 18:39:25

Start

OK

11.03.2013 18:41:41

StartWait

OK

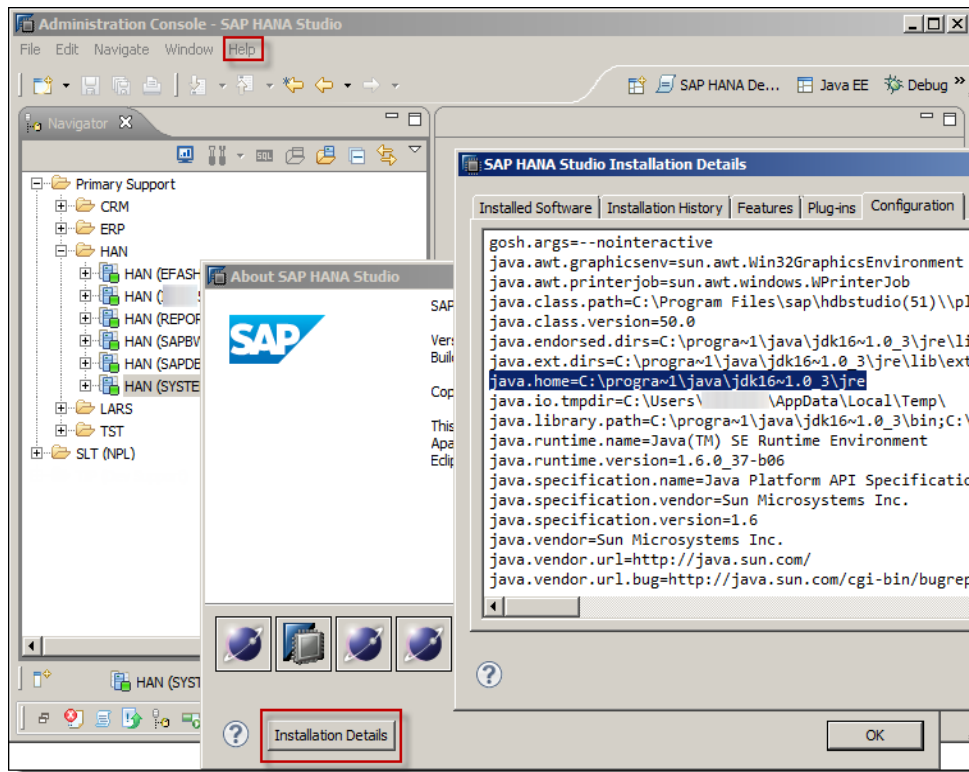
vanp9lnxc25b6:/usr/sap/HAN/HDB00>
```

3 CONFIGURE SAP HANA CLIENT TO SUPPORT SSL

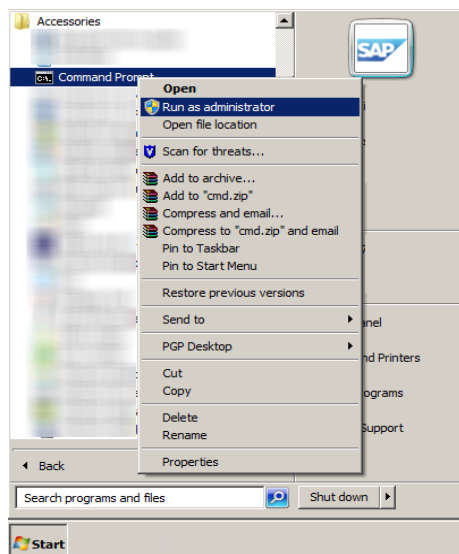
Using WinSCP or a different FTP tool, transfer trust.pem to the client machine (following screenshots show Microsoft Windows client operating system). Copy trust.pem, in TEXT mode, from the HANA Server to the client (i.e. c:\temp\).

3.1 Import 'trust.pem' into the Java keystore on the client

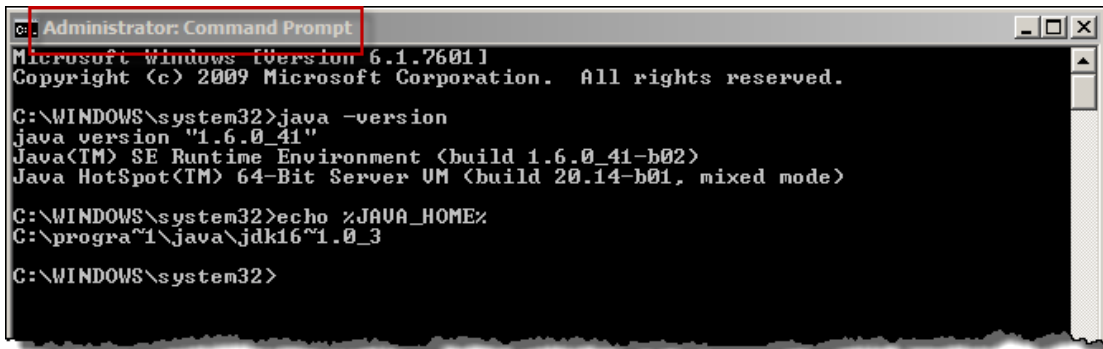
As user 'Administrator', or with administrative access, import trust.pem into Java's keystore. Confirm that the Microsoft Window's environment variable %JAVA_HOME% matches the version of Java in the OS path, as well as matches that shown in HANA Studio's Help | About | Installation Details.



Open Microsoft Windows Command Prompt as Administrator:



Command prompt will open in Administrator mode:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>java -version
java version "1.6.0_41"
Java(TM) SE Runtime Environment (build 1.6.0_41-b02)
Java HotSpot(TM) 64-Bit Server VM (build 20.14-b01, mixed mode)

C:\WINDOWS\system32>echo %JAVA_HOME%
C:\progra~1\java\jdk16~1.0_3

C:\WINDOWS\system32>
```

Change to the Java binary directory...

```
C:\WINDOWS\system32> cd \progra~1\java\jdk16~1.0_3\bin
```

Execute the following command, ensure that `..\jre\lib\security\cacerts` file exists prior to executing the keytool command. Note only a single prompt for password should occur.

```
C:\PROGRA~1\Java\JDK16~1.0_3\bin>keytool.exe -importcert -keystore
..\jre\lib\security\cacerts -alias HANServer -file c:\temp\trust.pem

Enter keystore password: ← The default password for the Java keystore is "changeit"

Owner: CN=HANA Server HAN, OU=AGS, O=SAP, L=Vancouver, ST=British Columbia, C=CA

Issuer: CN=HANA Server HAN, OU=AGS, O=SAP, L=Vancouver, ST=British Columbia, C=CA

Serial number: da51f183316af49f

Valid from: Mon Mar 11 18:03:59 PDT 2013 until: Thu Mar 09 17:03:59 PST 2023

Certificate fingerprints:

[ Object information removed for brevity ]

[CN=HANA Server HAN, OU=AGS, O=SAP, L=Vancouver, ST=British Columbia, C=CA]
SerialNumber: [ da51f183 316af49f]

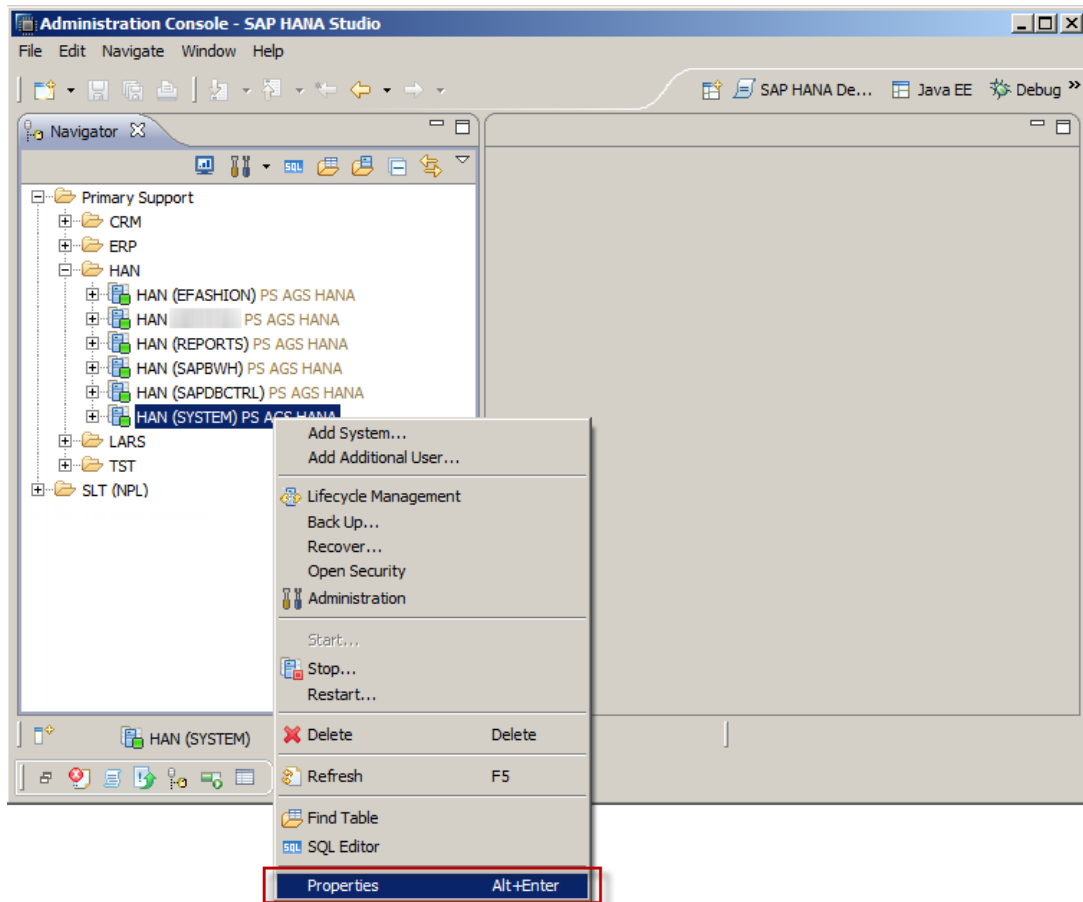
]

Trust this certificate? [no]: yes

Certificate was added to keystore
```

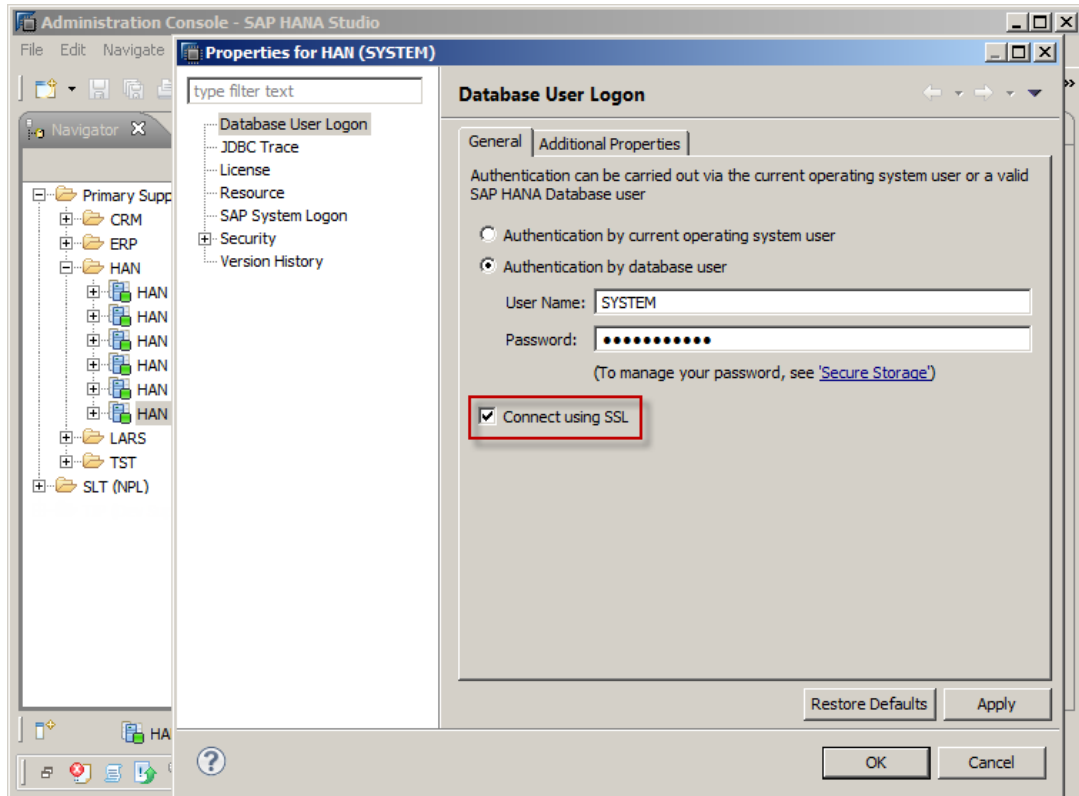
3.2 Enable SSL Communication within HANA Studio

Start SAP HANA Studio, from the Administrator's perspective, right click on the HANA system (or right click and add a new SAP HANA system) to bring up the properties dialog.

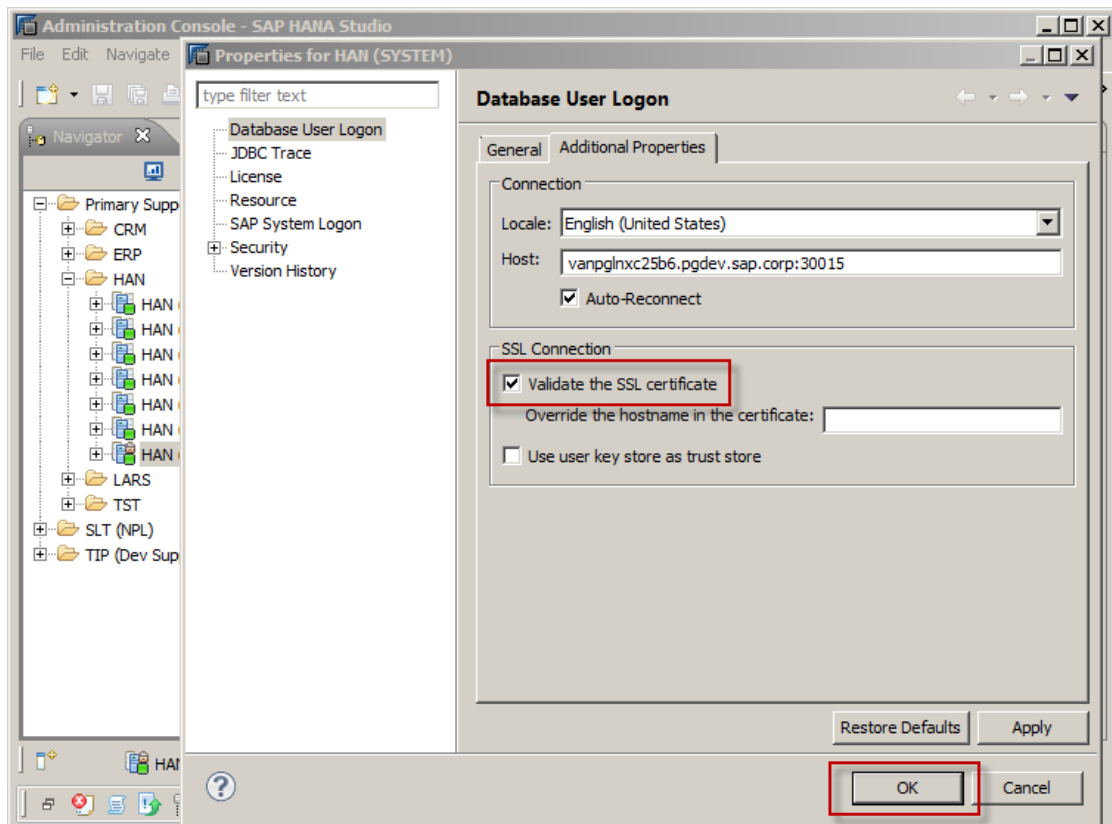


On the Properties dialog, check the 'Connect using SSL' option.

How to Configure Open SSL for SAP HANA Studio to SAP HANA Server

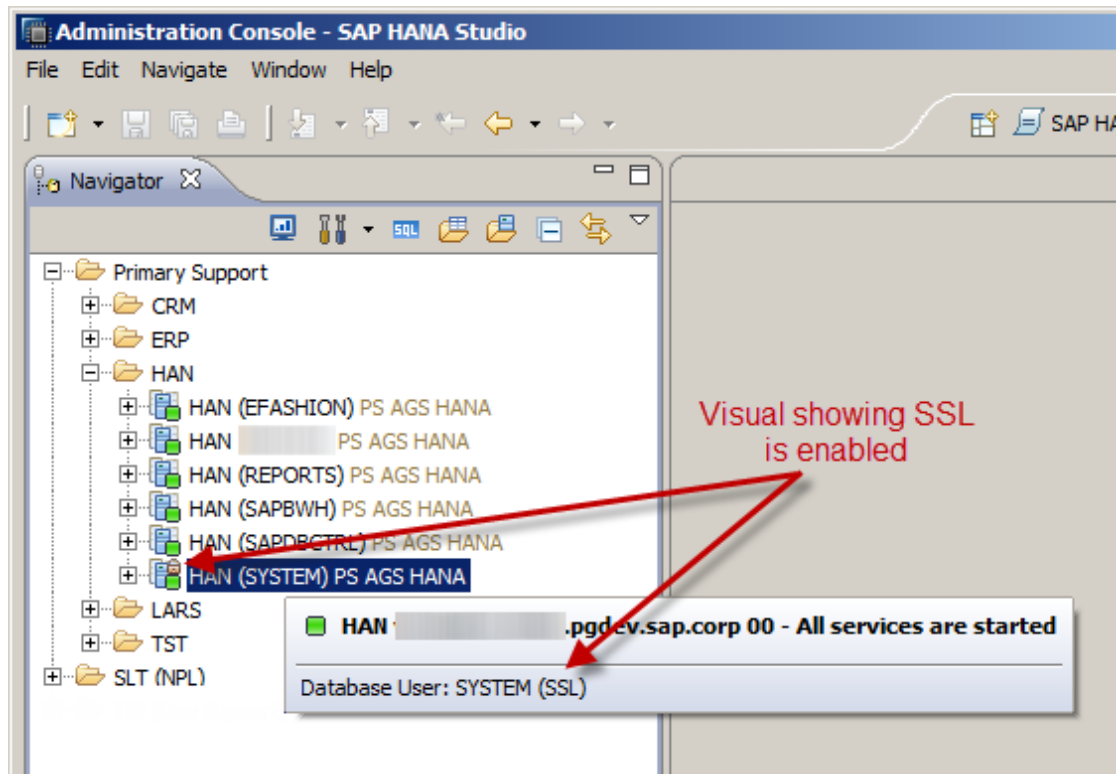


On the Additional Properties tab, check the 'Validate the SSL certificate' option.



How to Configure Open SSL for SAP HANA Studio to SAP HANA Server

Confirm that HANA Studio will now communicate using SSL, the hover tooltip should now show SSL, and the system node icon should show a small lock.



© 2013 SAP AG. All rights reserved.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase Inc. Sybase is an SAP company.

Crossgate, m@gic EDDY, B2B 360°, and B2B 360° Services are registered trademarks of Crossgate AG in Germany and other countries. Crossgate is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

