2634052 - How to configure Corba SSL using self-signed certificate for SAP BI 4.2 SP05+

Version	14	**Type**	SAP Knowledge Base Article
Language	English	**Master Language**	English
Release Status	Released to Customer	**Category**	How To
Component	BI-BIP-SRV (CMS / Auditing issues (excl. 3rd Party Authentication))	**Released On**	12.05.2020

Please find the original document at **https://launchpad.support.sap.com/#/notes/2634052**

Symptom

- How to configure Corba SSL
- How to enable server-side SSL in SAP BI 4.2, SP05 and later versions
- What are the high-level steps or commands used to configure Corba SSL?

Environment

- SAP BusinessObjects Business Intelligence Platform 4.2, Support Package 05 and newer
- Windows Server platform
- NOTE: Windows is used as reference but the equivalent commands should work in any supported OS, although the file locations may differ.

Reproducing the Issue

- Configure CORBA SSL based on product documentation on the Help portal.

Resolution

Assumptions & Prerequisites:

- Starting BI 4.2 SP05, certificates generated by the **SSLC tool will no longer** enable corba SSL, so you will need to use the **new GenPSE tool to re-generate x.509 certificates**.
- In BI 4.2 SP05, **GenPSE**(Based on SAP CCL) is the **new tool** created to generate x.509 certificate and PSE files, used for enabling SSL.
- **GenPSE** can **also generates CSR for 3rd party CA** to sign
- BI Server is on a supported Windows OS. Please refer to the Administration guide more details on this configuration or for other Operating systems.
- Installed on default location: "C:\Program Files (x86)\SAP BusinessObjects".
- Instructions for generating a self-signed certificate are given as reference. For third party CA certificate, follow commands from this step from the SP5 Administrators guide.
- All machines in the same deployment share the same CA certificates.

Steps to configure BI Server for SSL:

1. **Setup the server:**

i. Open Windows CMD in elevated mode (Run as Administrator), or a terminal session as the BI user for Linux / Unix
ii. Create the following directory structure
Windows
MKDIR C:\ssl
Linux
<PATHTOFOLDER>/ssl
iii. Navigate to the folder containing genpse:
Windows
CD "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64"
Linux
cd <PATHTOINSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64

iv. Create a new text file called **ssl.cnf** [make sure the extension is changed to .cnf and not .txt]
v. Open the SSL.cnf file for editing and provide some default values as shown below - then save the file.

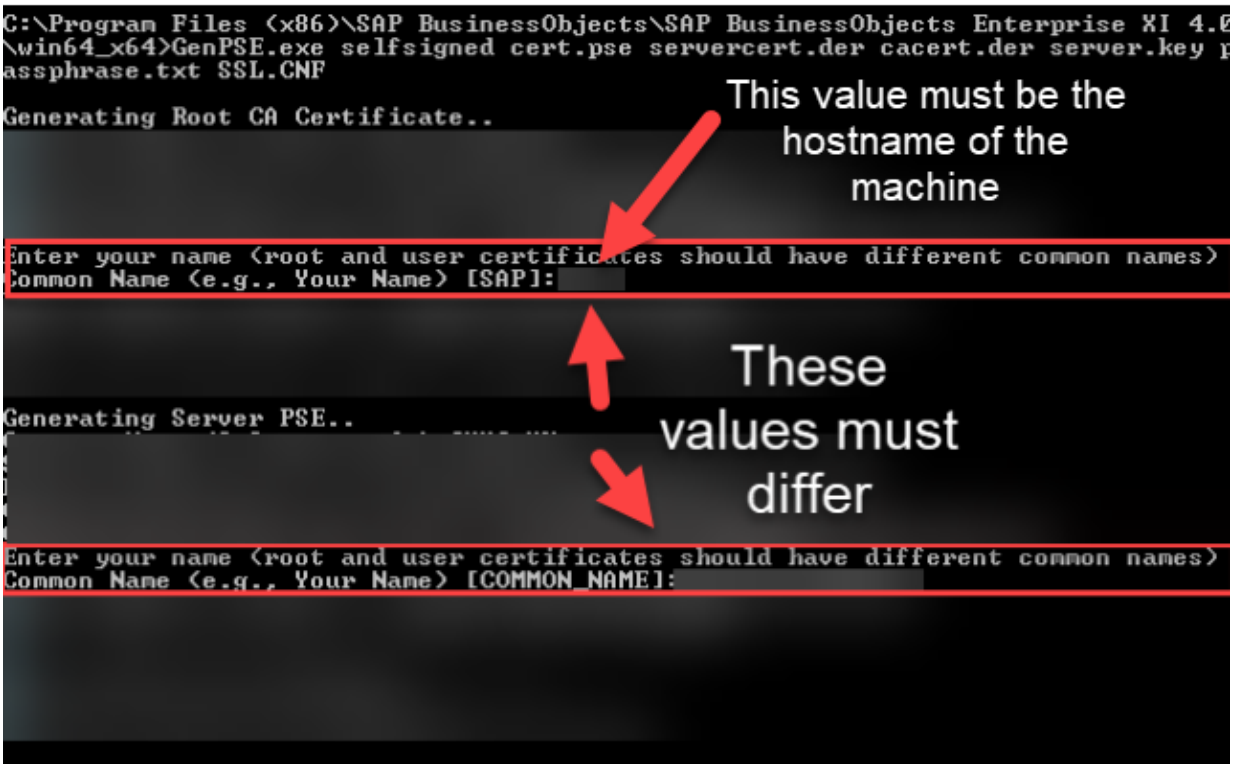
CA_Common_Name = SAP Company
CA_Country = US
CA_State = GA
CA_Locality = APH
CA_Email = xyz@sap.com
CA_Unit = Product Support
CA_Expiration[YYMMDD] = 201231
User_Expiration[YYMMDD] = 201231
User_Country = US
User_State = GA
User_Locality = APH
User_Organization = DBS
User_Unit = PS
User_Common_Name = UserName
NOTE: ssl.cnf is a default configuration file which provides you with default options so you dont have type them everytime you try generating the keys.

2. **Generating all the required key and certificate files for the BI system**:
Compared to earlier versions, this step has been drastically simplified in SP5 to a 1-step process for self-signed certificates.
You now generate the certificates using the SAP GENPSE tool, a command-line tool for executing numerous tasks related to Public Key Infrastructure.
The SAP GENPSE tool is used to generate X.509 certificates, certificate signing requests, and PSE files that are used in the CORBA SSL workflow.
It is based on SAP's cryptographic library CommonCryptoLib and supports SHA-2 hashing mechanism.
Generating self-signed certificates and keys using sap genpse:
GenPSE selfsigned cert.pse servercert.der cacert.der server.key passphrase.txt ssl.cnf

On Linux, it may be necessary to first source in the env.sh before running GenPSE with below command (including **.**)
. /PATHTOINSTALLDIR/sap_bobj/setup/env.sh

Note: When generating the information, bear in mind that the ROOT CA Certificate Common

Name (CN) and Server PSE Common name must be different (they must not match), and the ROOT CA certificate should be the hostname of the machine, as below:



- Fill all the requested information
- Choose certificate type S for Server
- Dates are in YYMMDD format [you can choose upto year 2049]
- provide a password when prompted.
- Ensure the CA certificate and pse file name are different.

The PSE file and the certificates are generated and stored in the win64_x64 or linux_x64 folders
This step creates the following files:

cacert.der - Truststed CA certificate file
servercert.der - server certificate file
server.key - server private key file
cert.pse - server pse file
passphrase.txt - passphrase for decrypting server private key

3. *Copy all the files created in the above step to the SSL folder in step 1.ii*

Windows
COPY cacert.der C:\ssl
COPY servercert.der C:\ssl
COPY server.key C:\ssl
COPY cert.pse C:\ssl
COPY passphrase.txt C:\ssl

Linux
cp -p cacert.der <PATHTOFOLDER>/ssl
cp -p servercert.der <PATHTOFOLDER>/ssl
cp -p server.key <PATHTOFOLDER>/ssl
cp -p cert.pse <PATHTOFOLDER>/ssl
cp -p passphrase.txt <PATHTOFOLDER>/ssl

4. **Configuring SSL Protocol for the BI Server:**

Windows

i. In CCM, Stop Server Intelligence Agent (SIA), right-click and choose Properties.
ii. In the Properties dialog box, click the Protocol tab.
iii. Make sure Enable SSL is selected.
iv. Provide the file path for the directory where you stored the key and certificate files.*Server SSL Certificate File - server SSL certificate (C:\ssl\servercert.der)*
SSL Trusted Certificates File - SSL trusted certificate (C:\ssl\cacert.der)
SSL Private Key File - SSL private key file used to access the certificate. (C:\ssl\server.key)
SSL Private Key Passphrase File - passphrase used to access the private key. (C:\ssl\passphrase.txt)
SSL Pse Certificate File - pse file that contains information about the trusted and server certificates. (C:\ssl\cert.pse)
v. Start the SIA.Note: Although your server is configured with SSL, you may still get an error when trying to login to CMS using the CCM tool.
Example error: *Transport error: Insufficient resources. (FWM 00002).*
This is because the thick clients have not yet been configured to use SSL communication with the BI server.

Linux

i. Stop the servers
ii. Go to <installdir>/sap_bobj
iii. Start ./serverconfig.sh
iv. Select 3 - Modify a Node
v. Select the node to be configured for Corba SSL
vi. Select 1 - Modify Server Intelligence Agent SSL configuration.
vii. Select ssl.
viii. When prompted, specify each of the SSL certificate locations.
ix. Start the servers
NOTE: The -fips parameter must be present on the SIA command line in the ccm.config, otherwise CORBA SSL will not be functional and some servers will fail to start. For more info see:
2476061 - In BI 4.2 SP04 for non-windows platforms, if you want to configure SSL in SIA (CORBA), make sure your servers are running in fips mode.

5. **Configuring thick clients (including .NET or JAVA SDK applications) for server-side SSL communication:**

To configure thick clients for SSL, you use the **sslconfig.exe (boe_sslconfig on Linux).**

i. On the machine where the thick client is:
For **64-bit** clients (Eg. Central Configuration Manager/CCM) use the **win64_x64 (for Linux: linux_x64)** directory:
Windows
CD "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64"
Linux
cd <PATHTOINSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64
For **32-bit** clients (Eg. Web Intelligence Rich Client, Crystal Reports etc), use the **win32_x86 (for Linux: linux_x86)** directory:
Windows
Note: Command Prompt must be opened in 'Run as Administrator' mode

CD "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86"
Linux
cd <PATHTOINSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86

ii. Run the following command:
Windows
sslconfig.exe -dir C:\SSL -mycert servercert.der -rootcert cacert.der -mykey server.key -passphrase passphrase.txt -psecert cert.pse -protocol ssl
Linux
. <PATHTOINSTALLDIR>/sap_bobj/setup/env.sh
./boe_sslconfig -dir <SSLDIR> -mycert servercert.der -rootcert cacert.der -mykey server.key -passphrase passphrase.txt -psecert cert.pse -protocol ssl

iii. This will confirm that the communication protocol has been set to SSL.

iv. After this step, you should be able to test a login to the CMS from the CCM tool.
Note: For UNIX/LINUX systems, SSL parameters for the thick client (ccm.sh) need to be configured within the registry.
Refer to KBA 1533801 - ERROR: Couldnt logon to CMS (STU00152) while running ccm.sh with SSL

6. **Configuring other clients for SSL communication:**
   - KBA 2478707 - Problems connecting to BI Platform Support Tool 2.0.8 when CORBA SSL is configured
   - KBA 1722634 - How to configure SSL for Information Design Tool (IDT) and Translation Management Tool (TMT)
   - KBA 2042632 - Can applications like Promotion management communicate between Corba SSL servers and Non-Corba SSL servers in BI 4.X ?
   - KBA 1978655 - ERROR -"Transport error: Insufficient resources" when trying to login to Web Intelligence Rich Client , Universe Design Tool after SSL configuration
   - KBA 2439703 - Lumira 1.31.4 support for BI platform secured with CORBA SSL and WACS HTTPS
7. **Configuring J2EE webapp server (Tomcat) to communicate with SSL-enabled BI Server:**

To configure a J2EE web application server (Eg: Apache Tomcat) to communicate with a Corba SSL-enabled BI Server,
you need to run the Java environment with the following options set in the comman-line.
Example: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=c:/ssl -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt
To configure an Apache Tomcat server running on a Windows BI Server deployment:

i. Navigate to “Start | All Programs | Tomcat | Tomcat configuration | Java” and add the following entries at the end of “Java Options”

ii. Enter the following values for these standard Java command-line options into the "java options" text box [Ensure that there are no preceding/trailing spaces]
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=cert.pse

iii. Click OK to save these options and restart Tomcat.
For non-default / non-Windows environments, just do the equivalent to ensure these values are on the Java web application server's command-line.

Example (*<sap_bobj location>/tomcat/bin/setenv.sh*):

JAVA_OPTS="$JAVA_OPTS -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<folderpath>/ssl -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse"
export JAVA_OPTS

See Also

BI Server SSL Resources	General links
BI 4.2 SP5 Administrator guide (Windows) Configuring Third-party Certificate Autority (CA) managed SSL certificate SAP Community Blogs : Configure SIA to use SSL Certificate in BI 4.2 SP5 SAP Note 2433337 - Security enhancements in SAP BI 4.2 SP04 SAP KBA 1642329 - How to: Configure Corba SSL SAP KBA 1920033 - How to: Disable CORBA SSL Guided answers tree Pattern Books	SAP BI Platform Featured Content (links to most useful resources) How to find TOP KBAs for SAP BI Platform in Guided Answers decision trees SAP Help portal SAP Community (Questions & Answers / Direct Link to ask question / Blogs) SAP Community WIKI Enhancement Requests on SAP Customer Influence portal Product tutorials Training SAP Analytics Customer Handbook Roadmap

Your feedback is important to help us improve our knowledge base.
Please rate how useful you found this article by using the star rating feature at the beginning of this article. See KBA 1850330.

Keywords

sapbi 4.2 SP5 SP05 sp 5 05 corba ssl server side sslc sslconfig sapgenpse bobj bidep biserver business objects bi platform deploy sslpsecertificate sslkey pse 42 4x corbassl ccm.sh setenv.sh genpse psg-16703

Products

SAP BusinessObjects Business Intelligence platform 4.2

This document refers to

SAP Note/KBA	Title
2042632	Can applications like Promotion management communicate between Corba SSL servers and Non-Corba SSL servers in BI 4.X ?
1978655	ERROR -"Transport error: Insufficient resources" when trying to login to Web Intelligence Rich Client , Universe Design Tool after SSL configuration
1722634	How to configure Corba SSL for Information Design Tool (IDT) and Translation Management Tool (TMT)
1533801	ERROR: "Couldn't logon to CMS (STU00152)" while running ccm.sh with SSL

	BI 4.2 SP05 Administrator Guide

