2589081 - How to configure Corba SSL using self-signed certificate for SAP BI 4.2 pre-SP05

Version	6	**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/2589081**

Symptom

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

Environment

- SAP BusinessObjects Business Intelligence Platform 4.2, Support Package 04 (and its Patches) 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:

- 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. Please refer to the Admin guide for further instructions to configure a CA signed certificate. For third party certificate, follow the commands from this step from the SP4 Administrators guide.
- As the commands are similar in any OS, we advise users to update the folders according to the install locations and OS level convention.
- The CA certificate (cacert.der) and its corresponding private key (cakey.pem) must be generated only once per deployment. All machines in the same deployment share the same CA certificates. All other certificates must be signed by the private key of any CA certificate.
- Note: The certificates created for versions lower than BI 4.2 SP4 are not supported. You have to create new certificates for BI 4.2 SP4, as the minimum certificate key strength is now increased to 2048. For a complete list of security enhancements in BI 4.2 SP04, please see SAP Note 2433337.

Steps to configure BI Server for SSL:

1. **Setup the server:**

    1. Open Windows CMD in elevated mode (Run as Administrator)

    2. Create the following directory structure
       MKDIR C:\SSL
       MKDIR C:\SSL\private
       MKDIR C:\SSL\newcerts

    3. Set SECUDIR environment variable
       set SECUDIR=.

    4. Navigate to Win64_x64 folder:
       CD "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64"

    5. Configure the SSLC.cnf file:
       Start Notepad and open the following file:
       “C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sslc.cnf”

       Change the following lines and save the changes. If it is not already done, modify the first two lines of sslc.cnf file to
       RANDFILE = .rnd
       #oid_file = $ENV::HOME/.oid
       dir = C:/SSL

2. **Generating the Root certificate (cacert.pem)** :

   To create Root certificate you need 2 files

   - cacert.req – This is the certificate request which is used to generate a Root certificate.
   - privkey.pem – This is the private key that will be used to self-sign the Root certificate.
   - sslc.exe and sslc .cnf files will be used from \InstallDir\SAP BusinessObjects Enterprise XI 4.0\win64_x64 folder.Use the SSLC tool which is installed with your BI platform software. (Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64).

   i. Generate CA certificate request
      sslc req -config sslc.cnf -new -out cacert.req
      - Enter all details as prompted (passphrase, country, state, city, name etc)

      - This command creates following files,
      cacert.req - a Certificate Authority (CA) certificate request
      privkey.pem - a private key
      .rnd - a random file

   ii. Next, the private key needs to be decrypted
      sslc rsa -in privkey.pem -out cakey.pem
      - Enter the same password that was entered before

      - This command creates the decrypted key file
      cakey.pem - decrypted key

   iii. To obtain Root certificate, we are Self-Signing the CA Certificate.

sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
- Choose the number of days that suits your security needs.

- This command creates
cacert.pem - a self-signed certificate that expires after 365 days.

iv. Copy the files created from above steps to C:\SSL folder structure as below:

COPY **cacert.pem to C:\SSL**
COPY **cakey.pem to C:\SSL\private**
Create the following empty text file (database index file): **C:\SSL\index.txt**
Create another text file **C:\SSL\serial** (without extension), with the following value saved in it: **11111111111111111111111111111111**

3. **Generating the Digital certificate (servercert.pem)** :

we follow same steps as above to create 2 files (*servercert.req & privkey.pem*) after which the digital certificate will be signed by the root certificate created in earlier step.

i. Generate the server certificate request
sslc req -config sslc.cnf -new -out servercert.req
- Enter all details as prompted (passphrase, country, state, city, name etc).
- The Following files are created or modified -
servercert.req - digital certificate request is created
.rnd & privkey.pem - these are modified

ii. Decrypt the private key :
sslc rsa -in privkey.pem -out server.key
- Enter the same password that was entered before

- This command creates the decrypted key file
server.key - decrypted server key

iii. Run the below command to sign server certificate with root certificate
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
- Choose the number of days that suits your security needs.

- This command creates or modifies following files,
servercert.pem *- created in Win64_X64 folder and contains the signed digital certificate.*
11111111111111111111111111111111.pem - is created in “C:\SSL\newcerts”
(“index.txt.old”) - a backup of index.txt created in "C:\SSL"
index.txt - is updated in "C:\SSL"
serial.old - a Backup of “serial” is created in "C:\SSL"
serial - is updated in "C:\SSL"

4. **DER encode both certificates**
Run following commands to encode both certificates to DER

sslc x509 -in cacert.pem -out cacert.der -outform DER
- This command creates
cacert.der - Trusted CA certificate file

sslc x509 -in servercert.pem -out servercert.der -outform DER
- This command creates
servercert.der - Generated server certificate file

5. **Copy all files to C:\SSL folder**

   i. Copy “cacert.der”, “servercert.der” TO "C:\SSL\"
   ii. Create a file called passphrase.txt in "C:\SSL\" which contains only the plain text passphrase which was used in earlier steps to encode private key.
   iii. Copy the following files in a secure location; for example, C:\SSL.
   cacert.der - the trusted certificate file
   servercert.der - the generated server certificate file
   server.key - the server key file
   passphrase.txt - the passphrase file

6. **Generate a PSE file**

   i. Run following command:
   sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key
   - When prompted, provide an empty password (just press enter)
   - This creates a cert.pse file in "C:\SSL" folder.

   ii. Add user credentials to the created pse file -

   - if the user running BI 4x (SIA) is a LocalSystem Administrator you need to execute following command
   sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM
   - If the user is a service, then run the below command -
   sapgenpse seclogin -p C:\SSL\cert.pse -O ntdomain\ntuser

Configuring SSL Protocol on BI Server:

1. In CCM, Stop Server Intelligence Agent (SIA), right-click and choose Properties.
2. In the Properties dialog box, click the Protocol tab.
3. Make sure Enable SSL is selected.
4. 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)
5. 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.

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.**

1. On the server where the thick client is, go to <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64.
   CD "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64"
2. Run the following command:
   sslconfig.exe -dir C:\SSL -mycert servercert.der -rootcert cacert.der -mykey server.key -passphrase passphrase.txt -psecert cert.pse -protocol ssl
3. This will confirm that the communication protocol has been set to SSL.
4. After this step, you should be able to test a login to the CMS from the CCM tool.

Configuring other clients for SSL communication:

- SAP KBA 2478707 - Problems connecting to BI Platform Support Tool 2.0.8 when CORBA SSL is configured
- SAP KBA 1722634 How to configure SSL for Information Design Tool (IDT) and Translation Management Tool (TMT)
- SAP KBA 2042632 Can applications like Promotion management communicate between Corba SSL servers and Non-Corba SSL servers in BI 4.X ?
- SAP KBA 2439703 - Lumira 1.31.4 support for BI platform secured with CORBA SSL and WACS HTTPS

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:

1. Navigate to “Start | All Programs | Tomcat | Tomcat configuration | Java” and add the following entries at the end of “Java Options”
2. 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
3. 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.

See Also

BI Server SSL Resources	General links
BI 4.2 SP4 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 SP4 Automatic CORBA SSL Self Signed Certificate Generator for SAP Business Intelligence	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

4.0/4.1 SAP Note 2433337 - Security enhancements in SAP BusinessObjects BI Platform 4.2 SP04 SAP KBA 1642329 - How to: Configure Corba SSL SAP KBA 1920033 - How to: Disable CORBA SSL Guided answers tree Pattern Books	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 sp4 sp04 4 04 sp5 sp05 5 05 corba, ssl, server, side, sslc, sslconfig, sapgenpse, bobj, bidep, biserver, business, objects, bi, platform, deploy

Products

SAP BusinessObjects Business Intelligence platform 4.2

