E-TUX: Case Study - Configuring Tuxedo Jolt to use SSL encryption (Doc ID 2546466.1)

In this Document

APPLIES TO:

PeopleSoft Enterprise PT PeopleTools - Version 8.56 and later
Information in this document applies to any platform.

GOAL

Case study for configuring Jolt SSL with a new wallet.

SOLUTION

This example was performed on Oracle Linux 6 and PeopleTools 8.57 using openssl and where the Web Server and Application Server resided on the same host.

A) Create a new wallet for use on the Tuxedo Server. In this example the wallet name is 'server'.

Change directory to PS_CFG_HOME for the target Tuxedo Domain.

```
>> mkdir wallet.server

>> cd wallet.server

>> openssl genrsa -out server.key 4096
Generating RSA private key, 4096 bit long modulus
..++
.........++
e is 65537 (0x10001)

>> openssl req -new -key server.key -out server.csr -subj '/C=CN/CN=psft'

>> ls
server.csr  server.key

>> openssl genrsa -out caCert.key 4096
Generating RSA private key, 4096 bit long modulus
.........................................++
.............................................++
e is 65537 (0x10001)


>> ls
caCert.key  server.csr  server.key

>> openssl req -new -x509 -days 1826 -key caCert.key -out caCert.crt -subj '/C=US/OU=Class 2 Public Primary
Certification Authority/O=VeriSign'

>> ls
caCert.crt  caCert.key  server.csr  server.key

>> openssl x509 -req -days 730 -in server.csr -CA caCert.crt -CAkey caCert.key -set_serial 01 -out server.crt
Signature ok
subject=/C=CN/CN=psft
Getting CA Private Key
```

```
>> ls
caCert.crt  caCert.key  server.crt  server.csr  server.key

>> openssl pkcs12 -export -out ewallet.p12 -inkey server.key -in server.crt -chain -CAfile caCert.crt -passout
pass:password
```

B) Add the server's certificate to the PIA Web Server trust store. Note that access to 'wallet.server' directory will be needed.

On PIA Web Server host, logon as the ID that boots the PIA Web Server

```
>> keytool -import -file /home/psadm2/wallet.server/caCert.crt -alias srvcert -keystore /home/psadm2/psft/pt
/8.57/webserv/peoplesoft/piaconfig/keystore/pskey -storepass password -noprompt
Picked up _JAVA_OPTIONS: -Djava.security.egd=file:/dev/./urandom
Certificate was added to keystore
```

C) Setup Tuxedo Domain Server side. Note that in this example, a new 'wallet.server' directory was created/used. The delivered wallet/directory is named 'psft'.

For troubleshooting, if needed, you can set the following two environment variables to log additional SSL debug messages (the Domain will need to be reconfigured for these to be picked up).

Edit the psappsrv.ubx file and at the bottom add the following under the *PS_ENVFILE heading.

TUXNZTRACE=8191 (when this parameter is set as shown, when SSL negotiation occurs a debug file, 'Trace.12345 (12345 is a pid number), will be generated within the Tuxedo Domain directory where psappsrv.cfg resides)
ULOG_SSLINFO=Y

(! remember to unset these after you have Jolt SSL working ok)

D) Set the appropriate values for SSL within the Application Server psappsrv.cfg file

SEC_PRINCIPAL_LOCATION=/path/to/security (this is the path to the directory containing the 'wallet.server' directory whcih contains the SSL certs)
SEC_PRINCIPAL_NAME=server (this is name of the wallet, which is part of the directory name eg: wallet.server)
SEC_PRINCIPAL_PASSWORD=password (this is the wallet password, this will be encrypted by psadmin when the Domain is configured)

Under the Jolt Listener section set both of these. Other bit choices can cause issues for SSL

JSL Min Encryption=256
JSL Max Encryption=256

The Tuxedo Domain will need to be reconfigured to pick up these changes.

E) Set the appropriate Jolt SSL values within the PIA Web Server configuration.properties file under the PORTAL.war tree.

Set 'psserver' variable to use the SSL port defined in the psappsrv.cfg file under the Jolt Listener section, for example: Hostname:SSLport

Next use PATHTO/webserv/peoplesoft/piabin/pscipher to encrypt the password used for the Weblogic pskey store (PT 8.57 default 'password' is used in this example).

```
>> PSCipher.sh password
Encrypted text: {V2.1}1dGN94//cQFmeDH62drvu8fAgo1FMSwb
```

Edit the PORTAL.war configuration.properties file and set the variable 'KeyStorePwd' to be the pscipher encrypted 'password' value from above.

NOTE: the KeyStorePwd variable is the password used for the Weblogic pskey store as opposed to the Tuxedo Server side password (these can be the same though depending on how they were configured).

The PIA Web Server will need to be restarted to pick up these changes.