Configuring Oracle HTTP Server to use SSL in Fusion Middleware 11g (11.1.1.X)

There are two major steps needed to configure SSL in Fusion Middleware 11g (11.1.1.X)

I. Create an Oracle Wallet which contains an SSL Certificate.
II. Configure ssl.conf directives to enable SSL with OHS.

Step I: Creating an Oracle Wallet

As outlined in some of the referenced notes, there are several ways to create an Oracle Wallet in Fusion Middleware 11g. To summarize the methods are as follows:

Fusion Middleware Control
Oracle Wallet Manager
ORAPKI
WLST

The one you choose to use depends on your circumstances. Please read Note 1218603.1 Understanding Wallets and Keystores in Fusion Middleware 11g

Generally speaking the recommendation is to use FMW Control, however remember that FMW Control can ***only*** be used if your Webtier is associated with a WLS domain. For OHS standalone, use OWM or ORAPKI.

Choose whichever method suits and follow the relevant "*How to Create a Wallet Via ....*" Note in Note 1218695.1 Master Note for SSL Configuration in Fusion Middleware 11g, Section II: Wallets and Keystores in FMW 11g.

When the Wallet is complete and contains a valid certificate move to Step II.

Step II: Configuring HTTP Server for SSL

OHS can be configured using either FMW Control or by editing the configuration manually. The method chosen comes down to preference, and depends on whether your OHS is standalone or whether associated with a WLS domain. For OHS standalone follow the Manual Configuration steps.

Configuring SSL via Fusion Middleware Control

The OHS out of the box install creates an SSL Virtual Host for you, which is configured to use a dummy certificate. The steps below will show how to edit the existing SSL Virtual Host. If you choose to create a new Virtual Host see the later section.

Editing an Existing SSL Virtual Host

1. Follow Steps 1-8 in Section 6.4.3.1 Enable SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using Fusion Middleware Control with the following cavaets:

- Ignore Step 2
- At Step 5 for "*Server Wallet Name*" select the Wallet you created in Step I.
  Note if you created your Wallet via OWM or ORAPKI, then you need to import it into FMW Control by following 7.4.4.9 Importing a Wallet Using Fusion Middleware Control
- At Step 5 for "*SSL Authentication*" select "*Server Authentication*". It is not recommended to set "*No Authentication*" for security reasons, and "*Mutual*" and "*Optional Client Authentication*" are used if client certificates are required.
  See Note 1228083.1 Configuring SSL Client Authentication with Oracle HTTP Server in Fusion Middleware 11g (11.1.1.X)
- At Step 5 select the "*CipherSuites*" you wish to use, or leave All as the default.
- At Step 5 select the "*SSL Protocol*" version you wish to use. In FMW 11g, "*v1*" refers to *SSL V3.0*, *v3_v2Hello* refers to *SSLV3 with SSLv2 Client Hello*, and "*v3*" refers to to *TLS 1.0*

2. Test you can connect from a browser to your Virtual Host: via https://host.domain:port e.g https://host.uk.oracle.com:4443

To Create A New Virtual Host
1. Select "Web Tier" -> "ohs1" -> Right click "Administration" -> Virtual Hosts
2. Click the "Create" button
3. In the Virtual Host Name add a new listen address, for example: *:4449

If you are creating an SSL port on any port <1024, please see Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 (UNIX Only)

4. Set "Type" as "IP-based". SSL does not support Name Based Virtual hosts hence why IP-based is required.
5. Fill in any of the other parameters as required and hit OK
6. Highlight the new Virtual Host and select "Configure" -> "SSL Configuration"
7. Follow the Steps 4-8 from 6.4.3.1 Enable SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using Fusion Middleware Control with the same caveats outlined in the "*Editing an existing SSL Virtual Host*" section
8. Test you can connect from a browser to your Virtual Host: via https://host.domain:port e.g https://host.uk.oracle.com:4443

Configuring SSL Via Manual Configuration

If using OHS standalone i.e without a WLS domain, it is necessary to configure SSL manually. You can also do it this way if you prefer not to use FMW Control

As mentioned above, out of the box OHS ships with a default SSL VirtualHost. The easiest way to get SSL up and running quickly is to modify this VirtualHost.

1. Backup the $ORACLE_INSTANCE/config/OHS/ohs1/ssl.conf
2. Edit the ssl.conf and locate the VirtualHost section:

```
<VirtualHost *:4448>
<IfModule ossl_module>
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Client Authentication (Type):
# Client certificate verification type and depth. Types are
# none, optional and require.
SSLVerifyClient None

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
SSLCipherSuite
SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_S
HA,SSL_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256
_CBC_SHA

# SSL Certificate Revocation List Check
# Valid values are On and Off
SSLCRLCheck Off

#Path to the wallet
SSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/defa
ult"

<FilesMatch "\.(cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>

<Directory
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/cgi-bin">
SSLOptions +StdEnvVars
</Directory>

BrowserMatch ".*MSIE.*" \
nokeepalive ssl-unclean-shutdown \
downgrade-1.0 force-response-1.0

</IfModule>
</VirtualHost>
```

3. Change the SSLWallet directive to point at the Wallet created in Step I e.g:

```
SSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/neww
allet
```

4. Save the file and restart HTTP Server:

```
$ORACLE_INSTANCE/bin/opmnctl restartproc process-type=OHS
```

5. Test you can connect from a browser to your Virtual Host:
https://host.domain:port e.g https://host.uk.oracle.com:4448