Configuring Web Cache with SSL in Fusion Middleware 11g (11.1.1.X)

Step I: Configure the HTTP Server so it can be accessed by Web Cache in SSL mode

1. To configure HTTP Server to run in SSL mode, see [Note 1226933.1 Configuring Oracle HTTP Server to use SSL in Fusion Middleware 11g (11.1.1.X)]
2. After this is configured make sure HTTP Server can be accessed in SSL mode e.g: https://ohs.uk.oracle.com:4444 where 4444 is the SSL port configured for the OHS.

Step II: Configure the WebCache Wallet

If WebCache and HTTP Server exist on the same server then this section can be ignored as the same Wallet can be used for both WebCache and the HTTP Server.

If WebCache and the HTTP Server are on different machines, then create a Wallet for Webcache. 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].

If on Windows, then make sure you perform the following steps or you will hit the issue outlined in [Note 1283744.1 Oracle HTTP Server and/or WebCache Fails to Start after Configuring SSL in FMW 11g on Windows]:

1. Open Windows Explorer and navigate to the <wallet_location>\cwallet.sso file.
2. Right Click on the cwallet.sso file, select Properties, and navigate to the Security tab. In the "Group or user names" security box, select "Add", and enter "SYSTEM" and click OK.

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

Step III: Configure the WebCache to listen in SSL Mode

The steps to follow depend on whether your Webtier is associated with a WebLogic Server domain, or whether it is a standalone Webtier. Follow the relevant section below for your circumstances:

WebCache associated with WLS Domain

1. In Step I, if you created a new Wallet for Webcache via FMW Control or WLST ignore this and continue at 2. If you created a new Wallet for Webcache via OWM or orapki, OR Webcache and OHS are on the same machine and you want to use the same Wallet as you did for OHS, then you need to import the Wallet into the WebCache configuration. Copy the Wallet (ftp in binary) from it's existing location on the server to the browser machine where FMW Control is
running. Then follow 7.4.4.9 Importing a Wallet Using Fusion Middleware Control, to import
the Wallet to the 'Wallet' section of WebCache

2. Create a new SSL listening port:

- Select 'Webcache' -> 'Administration' -> 'Ports Configuration'
- Select 'Create' and enter the relevant information:
  - Port Type: Norm
  - IP address: ANY
  - Port: 4443 (make sure this is not used by another process)
  - Select OK and this will take you back to the Ports screen.
  - Select the Port you just added e.g 4443 and select 'Edit'
  - Check 'Enable SSL'
  - Select the Wallet created in Step II.
  - In Advanced Settings leave the defaults.
  - Click OK

If you plan on using a port <1024 on UNIX, then follow Configuring Root Privilege for
Privileged Ports and More than 1,024 File Descriptors

3. Create an Origin Server:

- Select 'Webcache' -> 'Administration' -> 'Origin Servers'
- Select 'Create' and enter the relevant information:
  - Host: <OHS host.domain> e.g ohs.uk.oracle.com
  - Port: <OHS HTTP Port> e.g: 4444
  - Protocol : HTTPS
  - Leave all the rest as default

4. Create a new Site:

- Select 'Webcache' -> 'Administration' -> 'Sites'
- Select 'Create' and enter the relevant information:
  - Host: <webcache host.domain> e.g webcache.uk.oracle.com
  - Port <port> e.g 4443
  - Click OK and this will return you to the Sites page

5. Create a Site to Server Mapping:

- Select 'Create' and enter the relevant information:
  - Host Pattern: <webcache host.domain> e.g webcache.uk.oracle.com
  - Port Pattern: 4443
  - Select the Origin Server created earlier e.g: ohs.uk.oracle.com:4444 and
    select the 'Move' button.
  - Click OK
6. Import the Trusted Root CA Certificate into the Origin Server Wallet:

- Navigate to 'Webcache' -> 'Security' -> 'SSL Configuration'
- In 'SSL Communication Between Web Cache and Oracle HTTP Server (OHS)' select 'Change Wallet'
- Select the Client Wallet that you created in Step II
- If Webcache and OHS are on the same server and you are using the same wallet for OHS and Webcache move to 7.
- If Webcache and OHS are on the same or different servers and the certificate for OHS was signed by a different CA to the Webcache certificate, you need to import the Trusted Root CA certificate that signed the OHS certificate, into the Webcache Wallet selected above. How to import a Trusted Certificate into a Wallet has already been covered in earlier sections/notes.

7. Restart WebCache:

- Select 'WebCache' -> 'Control' -> 'Restart''

8. Move to Step IV: Test you can access Web Cache in SSL mode

**Webcache Standalone Not Associated with a WLS Domain**

1. Access the WebCache Administration page e.g: http://webcache.uk.oracle.com:<admin_port>. To find your Webcache Administration port run:

   $ORACLE_INSTANCE/bin/opmnctl status -l

   For example:

   ```
   ./opmnctl status -l
   Processes in Instance: wtdomain
   ----------------------------------------------------------+-------------------+-----------+----------+--
   ias-component | process-type | pid | status | uid | memused | uptime | ports
   ----------------------------------------------------------+-------------------+-----------+----------+--
   webcache1 | WebCache-admin | 11281 | Alive | 118425894 | 48540 | 0:32:26 | http_admin:7786
   In this case the admin port is 7786.
   2. Create a new SSL listening port:

   - Select 'Listen Ports'
   - Select the top entry in the list
   - Select 'Insert Above' and enter the relevant information:
     - Enter IP Address: ANY
Enter Port Number: 4443 (make sure this is not used by another process)
Protocol: HTTPS
Wallet : <wallet_location_created_in_Step_II>
Client Certificate: Not Required
Click 'Submit'

3. Create an Origin Server:
   - Select 'Origin Servers'
   - Click 'Add' and enter the relevant information:
     - Host Name: <OHS host.domain> ohs.uk.oracle.com
     - Port: <OHS SSL Port> e.g 4444
     - Protocol: HTTPS
     - Capacity: 100
     - Failover Threshold: 5
     - Ping URL: /
     - Ping Interval (seconds): 10
     - Click OK

4. Create a new Site:
   - Select 'Sites'.
   - Click 'Add' and enter the relevant information:
     - Host Name : <Webcache_host.domain> e.g webcache.uk.oracle.com
     - Port Number: <Webcache_SSL_port> e.g 4443
     - Leave the rest of the entries as default
     - Click Submit

5. Create a Site to Server Mapping:
   - Select 'Site to Server Mapping'
   - Select the top entry and Insert Above
   - Check 'Select a Defined Site' and select the Site you added from the drop down list
   - Select the correct Origin Server from 'Available Origin Servers' e.g: ohs.uk.oracle.com:4444
   - Select 'Submit'

6. Set the Origin Server Wallet:
   - Select 'Origin Server Wallet'
   - Select the Wallet and 'Edit Selected'
   - Change the path to the Wallet you created in Step II
   - If Webcache and OHS are on the same server and you are using the same wallet for OHS and Webcache move to 7.
If Webcache and OHS are on same or different servers and the certificate for OHS was signed by a different CA to the Webcache certificate you need to import the Trusted Root CA certificate that signed the OHS certificate, into the Webcache Wallet selected above. How to import a Trusted Certificate into a Wallet has already been covered in earlier sections/notes.

7. Restart Webcache:

- Select 'Cache Operations'
- Select 'Apply Changes'
- Select 'Restart'

**Step IV: Test you can access Web Cache in SSL mode**

1. Test you can access Webcache via SSL e.g: https://webcache.uk.oracle.com:4443

**Configuration II: HTTPS between Browser/Web Cache and HTTP between Web Cache/HTTP Server**

This section will show how to set up WebCache so the configuration is as follows:

Browser --> https --> WebCache --> http --> Oracle HTTP Server

There are several steps to configure WebCache for SSL on UNIX:

Step I: Configure Web Cache Wallet
Step II: Configure the Web Cache to listen in SSL Mode
Step III: Configure HTTP Server to use Mod_certheaders
Step IV: Test you can access Web Cache in SSL mode

**Step I: Configure the WebCache 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 WebCache 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: Configure the WebCache to listen in SSL Mode**

The steps to follow here depend on whether your Webtier is associated with a WebLogic Server domain, or whether it is a standalone Webtier. Follow the relevant section below for your circumstances:

**WebCache associated with WLS Domain**

1. In Step I, if you created a new Wallet for Webcache via FMW Control or WLST ignore this step and move to 2. If you created a new Wallet for Webcache via OWM or orapki, OR Webcache and OHS are on the same machine and you want to use the same Wallet as you did for OHS, then you need to import the Wallet into the WebCache configuration. Copy the Wallet (ftp in binary) from it's existing location on the server to the browser machine where FMW Control is running. Then follow 7.4.4.9 Importing a Wallet Using Fusion Middleware Control, to import the Wallet to the Webcache -> Wallets section.
2. Create a new SSL listening port:
   - Select 'Webcache' -> 'Administration' -> 'Ports Configuration'
   - Select Create and enter the relevant information:
     - Port Type: Norm
     - IP address: ANY
     - Port: 4443 (make sure this is not used by another process)
     - Select OK and this will take you back to the Ports screen.
     - Select the Port you just added e.g 4443 and select Edit
     - Check 'Enable SSL'
     - Select the Wallet created in Step I
     - In Advanced Settings leave the defaults.
     - Click OK
3. Create an Origin Server:
   - Select 'Webcache' -> 'Administration' -> 'Origin Servers'
• Select 'Create' and enter the relevant information:
  o Host: <OHS host.domain> e.g ohs.uk.oracle.com
  o Port: <OHS HTTP Port> e.g: 7779
  o Protocol: HTTP
  o Leave all the rest as default
  o Click OK

4. Create a new Site:

• Select 'Webcache' ->'Administration' ->'Sites'
• Select 'Create' and enter the relevant information:
  o Host: <Webcache_host.domain> e.g webcache.uk.oracle.com
  o Port <SSL_port> e.g 4443
  o Click OK and this will return you to the Sites page

5. Create a Site to Server Mapping:

• Select 'Create' and enter the relevant information
  o Host Pattern: <Webcache_host.domain> e.g webcache.uk.oracle.com
  o Port Pattern: 4443
  o Select the Origin Server created earlier e.g: ohs.uk.oracle.com:7779 and select the 'Move' button.
  o Click OK

6. Restart WebCache:

• Select 'WebCache' -> 'Control' -> 'Restart'

7. Move to Step III: Configure HTTP Server to use Mod_certheaders

Standalone WebCache not associated with WLS Domain

1. Access the WebCache Administration page e.g: http://webcache.uk.oracle.com:<admin_port>.
To find your Webcache Administration port run:

$ORACLE_INSTANCE/bin/opmnctl status -l

For example:

./opmnctl status -l

Processes in Instance: wtdomain
-------------------------------------------------------------------------------------------
---+-----------------+-----------+---------+----------+---------+--------+------------+---------+---
---+-----------------+-----------+---------+----------+---------+--------+------------+---------+---
ias-component | process-type | pid | status | uid | memused | uptime | ports
-------------------------------------------------------------------------------------------
---+-----------------+-----------+---------+----------+---------+--------+------------+---------+---
webcache1 | WebCache-admin | 11281 | Alive | 118425894 | 48540 | 0:32:26 | http_admin:7786
In this case the admin port is 7786.

2. Create a new SSL listening port:
   - Select 'Listen Ports'
   - Select the top entry in the list and select 'Insert Above'
   - Enter the relevant information as follows:
     - IP Address: ANY
     - Port Number: 4443
     - Protocol: HTTPS
     - Wallet: <wallet_location_created_in_Step_I>
     - Client Certificate: Not Required
     - Click 'Submit'

3. Create an Origin Server:
   - Select 'Origin Servers'
   - Click 'Add' and enter the relevant information:
     - Host Name: <OHS host.domain> ohs.uk.oracle.com
     - Port: <OHS Port> e.g 7779
     - Protocol: HTTP
     - Capacity: 100
     - Failover Threshold: 5
     - Ping URL: /
     - Ping Interval (seconds): 10
     - Click OK

4. Create a new Site:
   - Select 'Sites'
   - Click 'Add' and enter the relevant information:
     - Host Name: <Webcache_host.domain> e.g webcache.uk.oracle.com
     - Port Number: <Webcache_SSL_port> e.g 4443
     - Leave the rest of the entries as default
     - Click 'Submit'

5. Create a Site to Server Mapping:
   - Select 'Site to Server Mapping'
   - Select the top entry and 'Insert Above'
   - Check 'Select a Defined Site' and select the Site you added from the drop down list
   - Select the correct Origin Server from 'Available Origin Servers'
     e.g: ohs.uk.oracle.com:7779
   - Select 'Submit'
6. Restart Web Cache:

- Select 'Cache Operations'
- Select 'Apply Changes'
- Select 'Restart'

**Step III: Configure HTTP Server to use Mod_certheaders**

This step is necessary to configure HTTP server so it knows the originating request to Webcache was via HTTPS. To do this HTTP Server needs to be configured to use mod_certheaders.

1. For OHS associated with a WLS domain:
   In FMW Control select -> 'ohs1' -> 'Administration' -> 'Advanced Configuration' -> Select file: *httpd.conf*
   
   For Standalone OHS:
   Edit $ORACLE_INSTANCE/config/OHS/ohs1/httpd.conf

2. Add the certheaders_module by adding the following at the end of the LoadModule section:
   LoadModule certheaders_module "${ORACLE_HOME}/ohs/modules/mod_certheaders.so"

3. At the end of the httpd.conf add:
   AddCertHeader HTTPS
   SimulateHttps On

4. Restart HTTP Server

**Step IV: Test you can access Web Cache in SSL mode**

1. Test you can access Webcache via SSL e.g: https://webcache.uk.oracle.com:4443