

Oracle HTTP Server 11g R1 Configuration for FLEXCUBE

Oracle FLEXCUBE Investor Servicing

Release 12.3.0.0.0

[September] [2016]



## Table of Contents

<b>1. PURPOSE .....</b>	<b>4</b>
<b>2. INTRODUCTION TO ORACLE HTTP SERVER (OHS).....</b>	<b>5</b>
2.1 HTTP LISTENER .....	5
2.2 MODULES (MODS) .....	5
<b>3. INSTALLATION OF OHS 11G .....</b>	<b>6</b>
<b>4. CONFIGURE ORACLE HTTP SERVER INFRONT OF WEBLOGIC SERVER .....</b>	<b>14</b>
4.1 FOR WEBLOGIC IN SINGLE INSTANCE .....	14
4.2 FOR WEBLOGIC INSTANCES IN CLUSTER .....	15
<b>5. ENABLE “WEBLOGIC PLUG-IN ENABLED” FLAG IN WEBLOGIC.....</b>	<b>17</b>
<b>6. COMPRESSION RULE SETTING .....</b>	<b>18</b>
6.1 LOADING MOD_DEFLATE .....	18
6.2 CONFIGURING FILE TYPES.....	18
6.3 HTTPD.CONF FILE CHANGES .....	19
<b>7. CONFIGURING SSL FOR ORACLE HTTP SERVER .....</b>	<b>20</b>
7.1 SSL CONFIGURATION FOR INBOUND REQUEST TO ORACLE HTTP SERVER .....	20
7.1.1 Create a new Wallet and import Certificate .....	20
7.1.2 Configuring Wallet in ssl.conf file.....	24
7.2 CONFIGURING SSL BETWEEN ORACLE HTTP SERVER AND ORACLE WEBLOGIC SERVER .....	25
7.2.1 Turn off KeepAliveEnabled.....	25
7.2.2 To enable one-way SSL.....	25
7.2.3 To enable two-way SSL .....	27
<b>8. SAMPLE CONFIGURATION FILES .....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>9. STARTING, STOPPING, AND RESTARTING ORACLE HTTP SERVER .....</b>	<b>29</b>
9.1 START .....	29
9.2 STOP .....	29
9.3 RESTART .....	29

<b>10.</b>	<b>TEST THE APPLICATION .....</b>	<b>30</b>
<b>11.</b>	<b>SERVER LOGS LOCATION .....</b>	<b>31</b>
<b>12.</b>	<b>REFERENCES .....</b>	<b>32</b>

## 1. Purpose

The objective of this document is to explain the installation and configuration of Oracle HTTP Server 11g R1 (11.1.1.9.0). This includes setting up of server details, configuration of compression rules and enabling SSL.

## 2. Introduction to Oracle HTTP Server (OHS)

Oracle HTTP Server is the Web server component for Oracle Fusion Middleware. It is based on Apache web server, and includes all base Apache modules and modules developed specifically by Oracle. It provides a HTTP listener for Oracle WebLogic Server and the framework for hosting static pages, dynamic pages, and applications over the Web. Key aspects of Oracle HTTP Server are its technology, its serving of both static and dynamic content and its integration with both Oracle and non-Oracle products.

Oracle HTTP Server consists of several components that run within the same process. These components provide the extensive list of features that Oracle HTTP Server offers when handling client requests.

Following are the major components:

### 2.1 HTTP Listener

Oracle HTTP Server is based on an Apache HTTP listener to serve client requests. An HTTP server listener handles incoming requests and routes them to the appropriate processing utility.

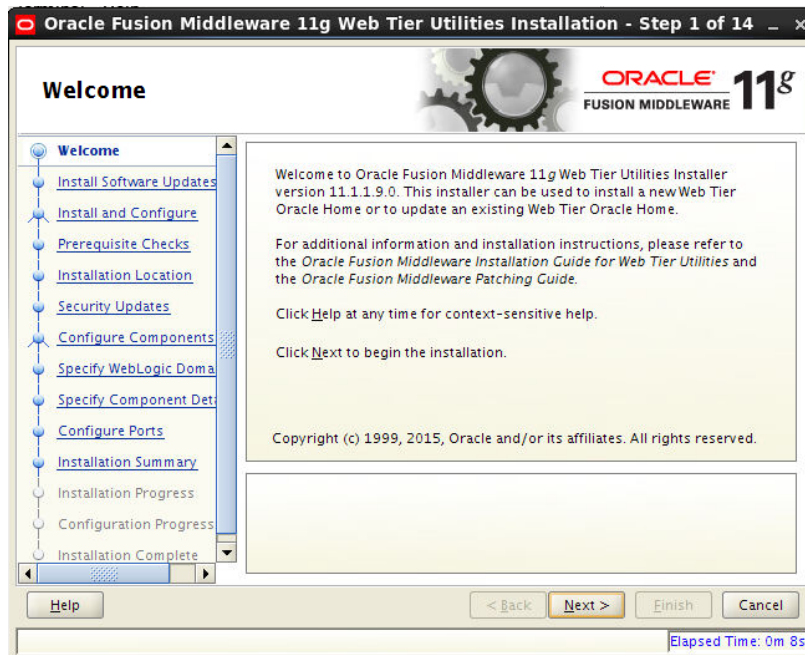
### 2.2 Modules (mods)

Modules extend the basic functionality of Oracle HTTP Server, and support integration between Oracle HTTP Server and other Oracle Fusion Middleware components. There are modules developed specifically by Oracle for Oracle HTTP Server. Ex: `mod_wl_ohs`, `mod_plsql`

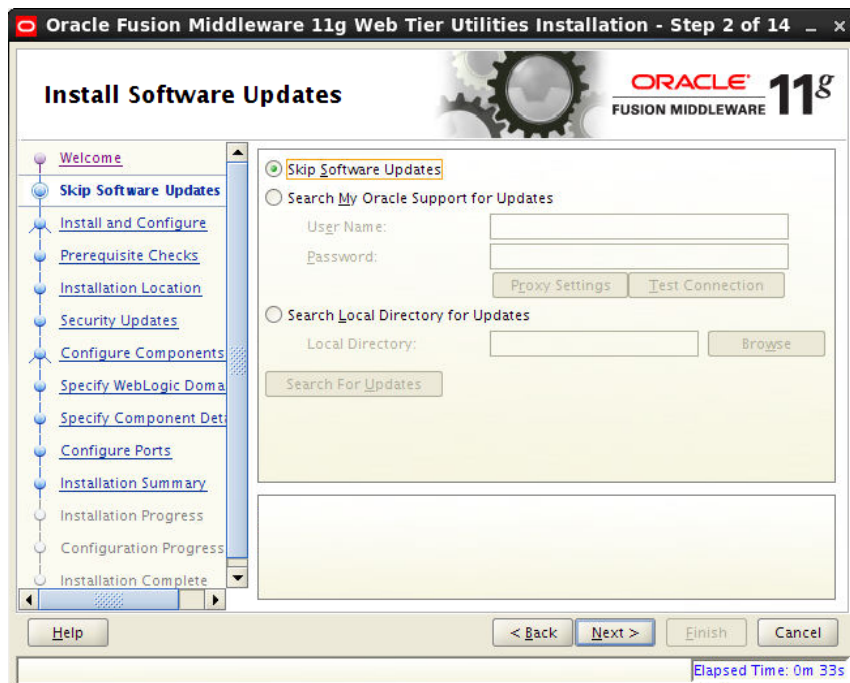
Oracle HTTP Server also includes the base Apache and third-party modules out-of-the-box. These modules are not developed by Oracle. Ex: `mod_proxy`, `mod_perl`

### 3. Installation of OHS 11g

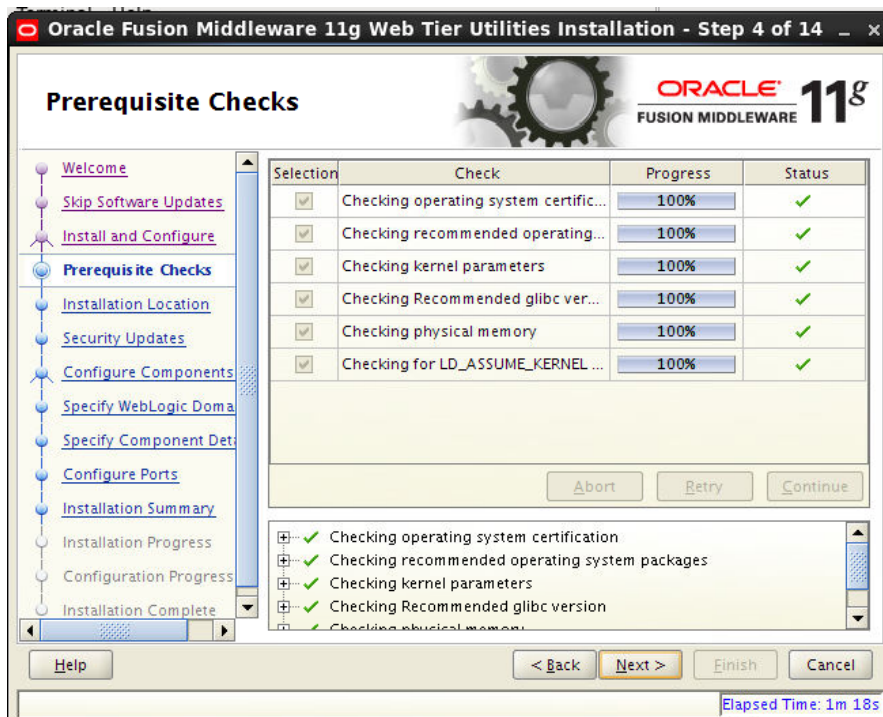
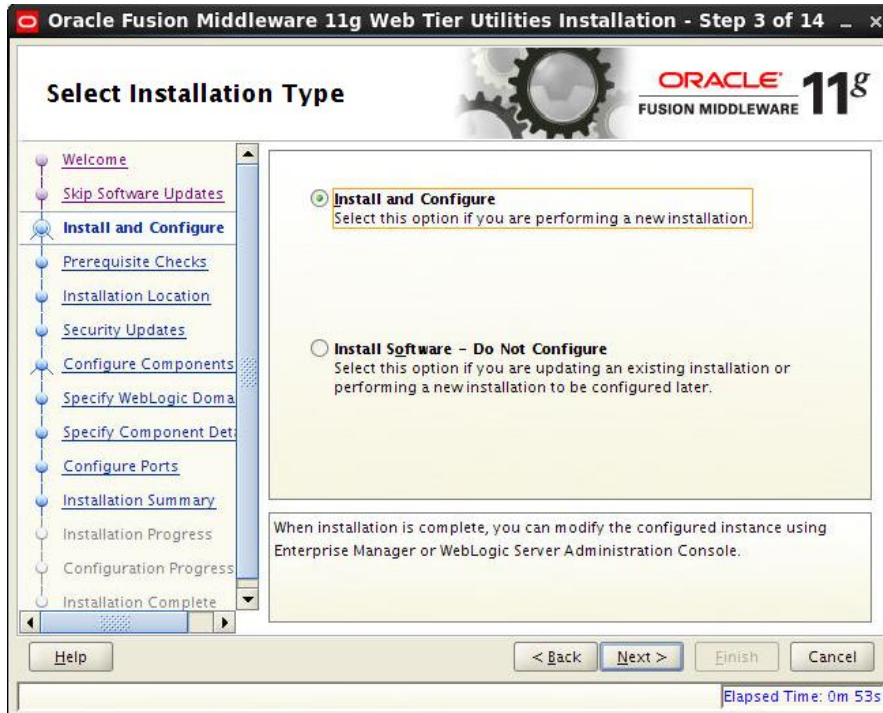
Invoke the setup exe to start the installation

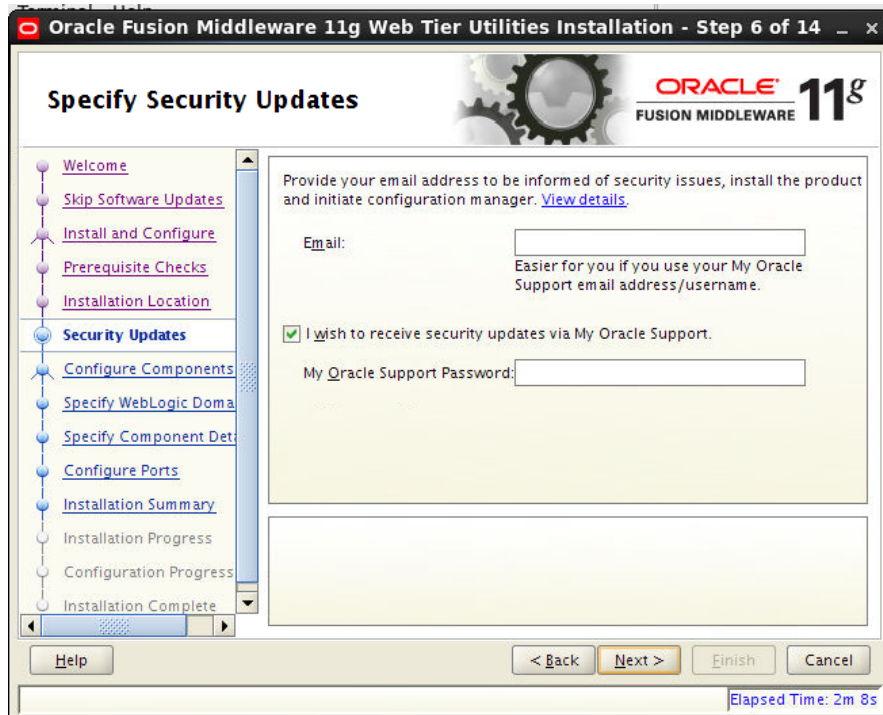
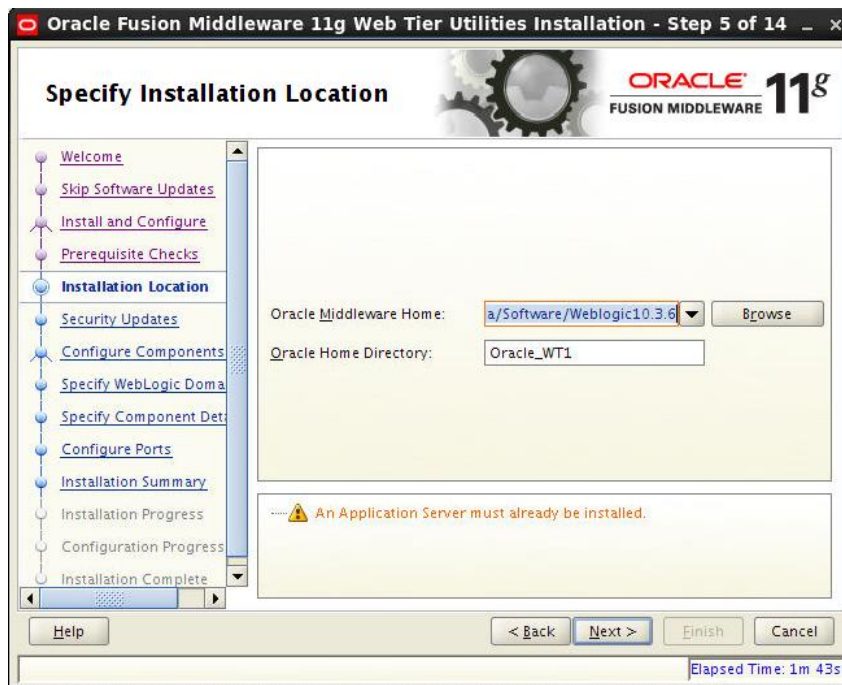


Select Skip Software Updates



## Select Install and Configure

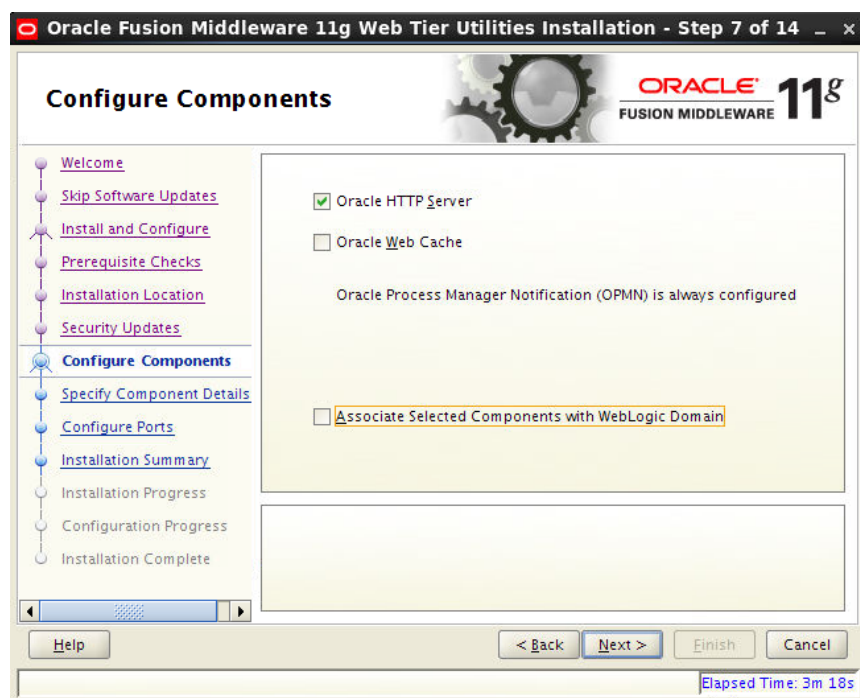








Select only Oracle HTTP Server



Enter the required OHS instance and component names

Oracle Fusion Middleware 11g Web Tier Utilities Installation - Step 8 of 13

### Specify Component Details

Welcome

Skip Software Updates

Install and Configure

Prerequisite Checks

Installation Location

Security Updates

Configure Components

**Specify Component Detail**

Configure Ports

Installation Summary

Installation Progress

Configuration Progress

Installation Complete

Instance Home Location:  Browse

Instance Name:

QHS Component Name:

Help < Back Next > Finish Cancel

Elapsed Time: 4m 18s

Oracle Fusion Middleware 11g Web Tier Utilities Installation - Step 9 of 13

### Configure Ports

Welcome

Skip Software Updates

Install and Configure

Prerequisite Checks

Installation Location

Security Updates

Configure Components

Specify Component Details

**Configure Ports**

Installation Summary

Installation Progress

Configuration Progress

Installation Complete

☒ Auto Port Configuration

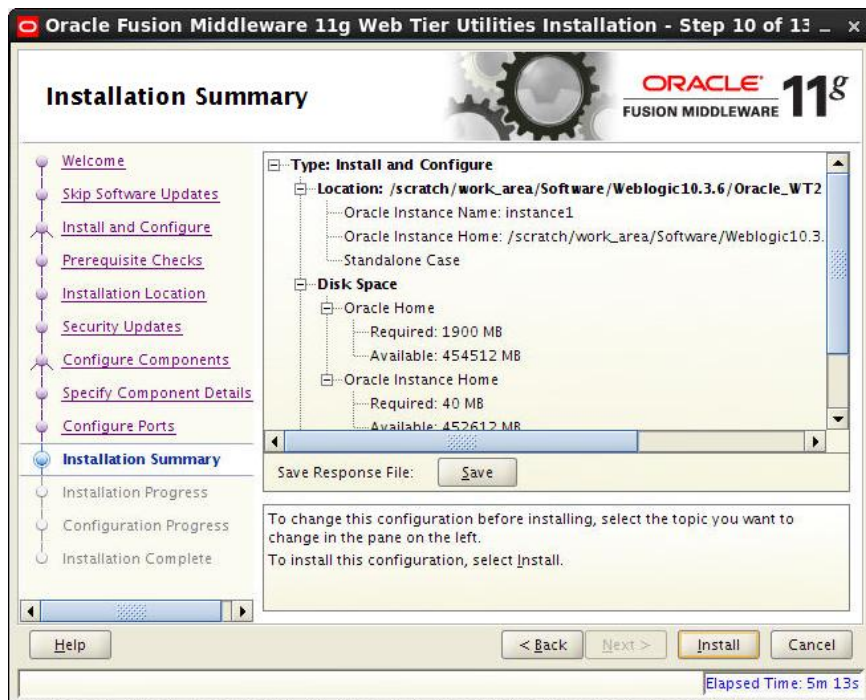
☐ Specify Ports using Configuration file

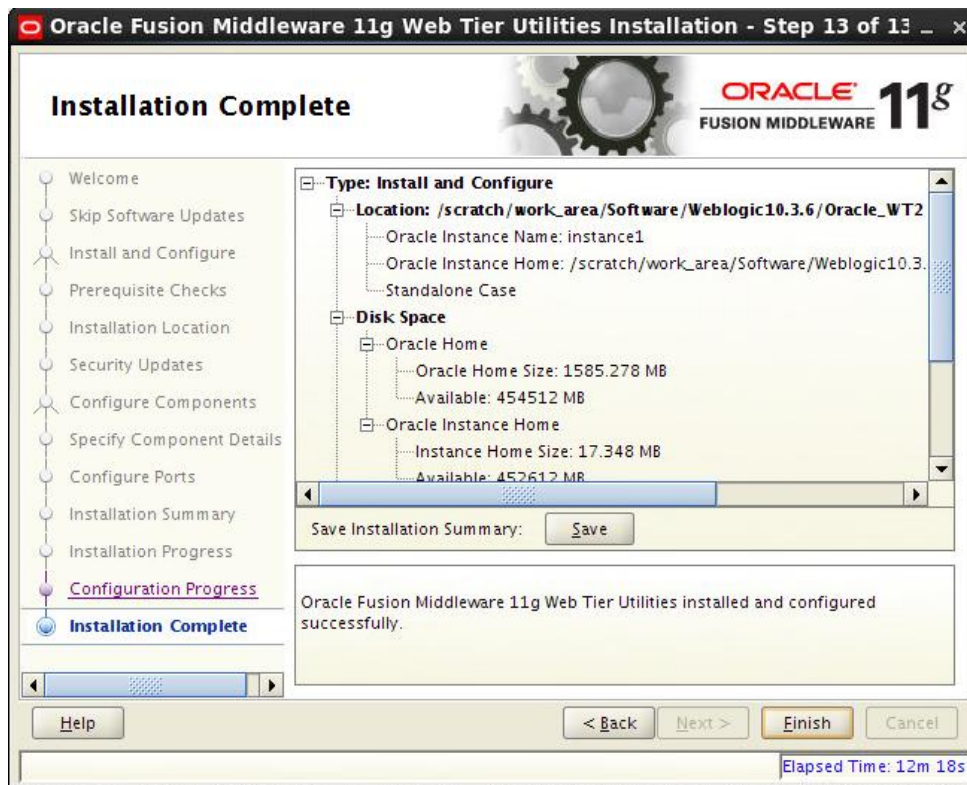
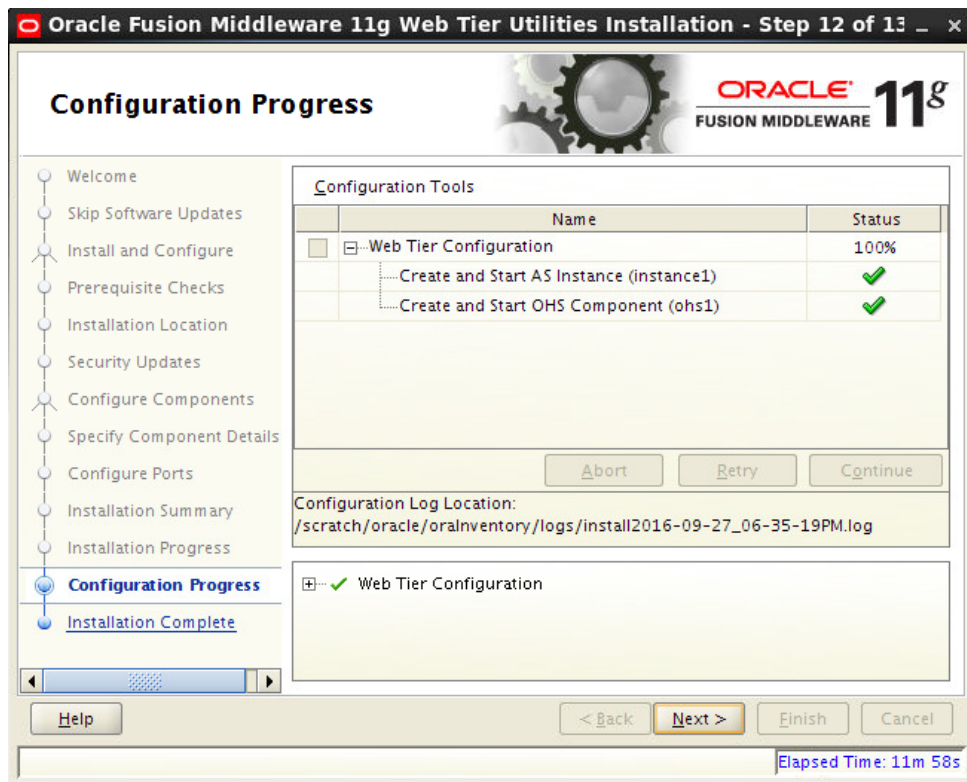
File name:  Browse

View/Edit File

Help < Back Next > Finish Cancel

Elapsed Time: 4m 38s

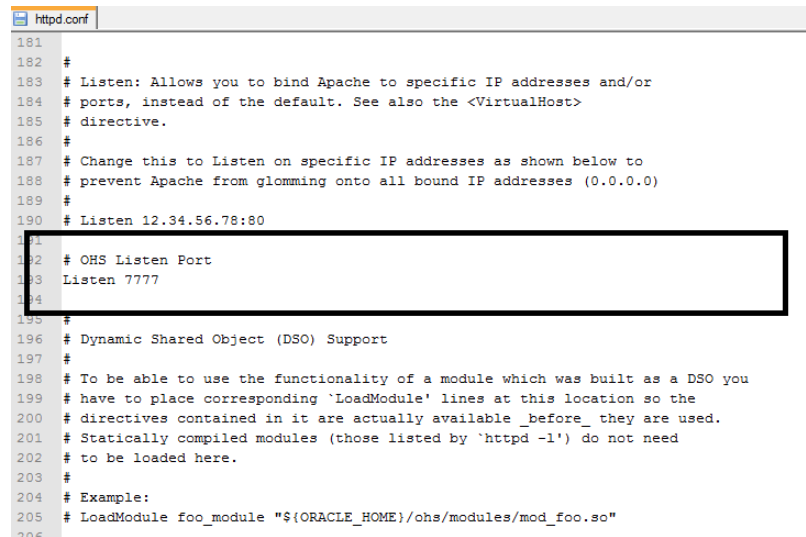




This completes the installation of Oracle HTTP Server with <Instance> and <component>. Example: Instance is instance1 and component is ohs1.

If you would like to change the port after the installation (OHS Listen Port) edit \$ORACLE\_INSTANCE/config/OHS/<component\_name>/httpd.conf and change the listen port.

NOTE: This port is for http protocol and not for https.



```
181
182 #
183 # Listen: Allows you to bind Apache to specific IP addresses and/or
184 # ports, instead of the default. See also the <VirtualHost>
185 # directive.
186 #
187 # Change this to Listen on specific IP addresses as shown below to
188 # prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
189 #
190 # Listen 12.34.56.78:80
191 #
192 # OHS Listen Port
193 Listen 7777
194 #
195 #
196 # Dynamic Shared Object (DSO) Support
197 #
198 # To be able to use the functionality of a module which was built as a DSO you
199 # have to place corresponding 'LoadModule' lines at this location so the
200 # directives contained in it are actually available _before_ they are used.
201 # Statically compiled modules (those listed by 'httpd -l') do not need
202 # to be loaded here.
203 #
204 # Example:
205 # LoadModule foo_module "${ORACLE_HOME}/ohs/modules/mod_foo.so"
206 #
```

## 4. Configure Oracle HTTP Server in front of Weblogic Server

In Oracle HTTP Server requests from Oracle HTTP Server to Weblogic server are proxied using mod\_wl\_ohs module. This configuration file needs to be modified to include the Weblogic server and port details.

mod\_wl\_ohs.conf file is located at

`${ORACLE_INSTANCE}/config/OHS/{COMPONENT_NAME}/mod_wl_ohs.conf`

Add the below directives to mod\_wl\_ohs.conf file.

### 4.1 For WebLogic in single instance

```
<Location /<<context/url>> >
```

```
    SetHandler weblogic-handler
```

```
    WebLogicHost <<server name>>
```

```
    WeblogicPort <<port>>
```

```
</Location>
```

Example:

```
<Location /FCISNeoWeb>
```

```
    SetHandler weblogic-handler
```

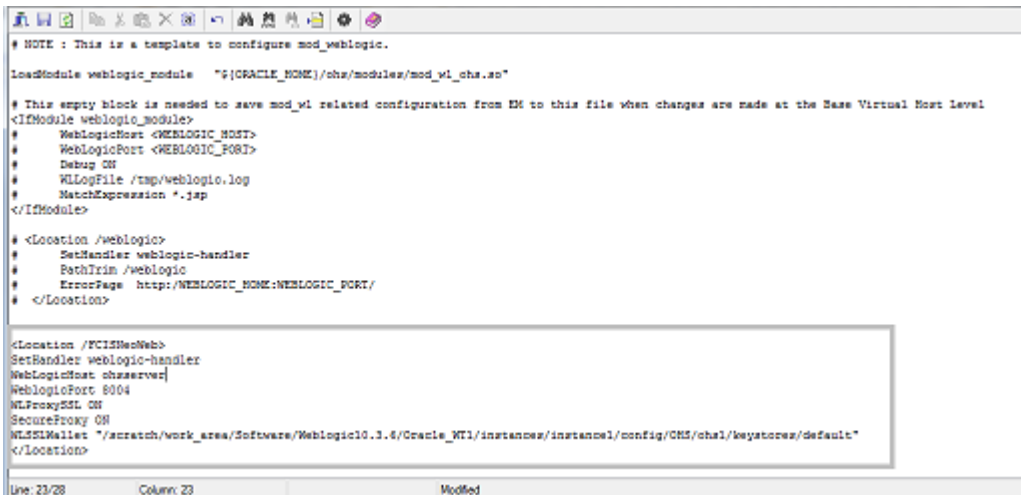
```
    WebLogicHost wlserver1
```

```
    WeblogicPort 7707
```

```
</Location>
```

This will forward /FCISNeoWeb from HTTP server to /FCISNeoWeb on WebLogic Server wlserver1: 7707





```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module    "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level
<IfModule weblogic_module>
#
# WebLogicHost <WEBLOGIC_HOST>
#
# WebLogicPort <WEBLOGIC_PORT>
#
# Debug ON
#
# WlLogFile /tmp/weblogic.log
#
# MatchExpression *.jsp
</IfModule>

#
# <Location /weblogic>
#
#     SetHandler weblogic-handler
#     PathTrim /weblogic
#     ErrorPage http://WEBLOGIC_HOST:WEBLOGIC_PORT/
#
# </Location>

<Location /FCISNeoWeb>
SetHandler weblogic-handler
WebLogicHost wlsserver1
WebLogicPort 8004
WlProxySSL ON
SecureProxy ON
WlSSLWallet "/scratch/work_area/Software/Weblogic10.3.6/Oracle_WT1/instances/instance1/config/OHS/ohs1/keystore/default"
</Location>
```

## 4.2 For Weblogic instances in cluster

<Location /<<context/url>> >

SetHandler weblogic-handler

WebLogicCluster <server1>:<port1>,<server2>:<port2>

</Location>

Example

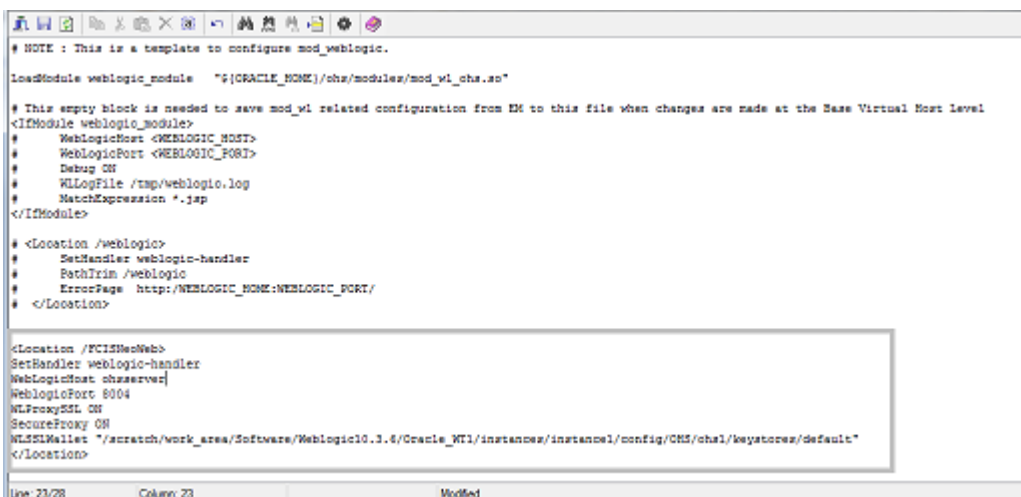
<Location / FCISNeoWeb >

SetHandler weblogic-handler

WebLogicCluster wlsserver1:7010, wlsserver2:7010

</Location>

This will forward /FCISNeoWeb from HTTP server to /FCISNeoWeb on WebLogic Cluster wlsserver1:7010 and wlsserver2:7010



```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module    "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level
<IfModule weblogic_module>
#   WebLogicHost <WEBLOGIC_HOST>
#   WebLogicPort <WEBLOGIC_PORT>
#   Debug ON
#   WLLogFile /tmp/weblogic.log
#   MatchExpression *.jsp
</IfModule>

# <Location /weblogic>
#   SetHandler weblogic-handler
#   PathTrim /weblogic
#   ErrorPage  http://WEBLOGIC_HOST:WEBLOGIC_PORT/
# </Location>

<Location /FCISWeb>
SetHandler weblogic-handler
WebLogicHost ohsserver
WebLogicPort 8004
WLProxySSL ON
SecureProxy ON
WLSSEMaillet "/scratch/work_area/Software/Weblogic10.3.6/Oracle_WT1/instances/instance1/config/ONS/ohs1/keystore/default"
</Location>
```

Line: 23/28      Column: 23      Modified



## 5. Enable “WebLogic Plug-In Enabled” flag in weblogic

This flag needs to be enabled in weblogic if it is accessed through proxy plugins. When the WebLogic plugin is enabled, a call to `getRemoteAddr` will return the address of the browser client from the proprietary `WL-Proxy-Client-IP` header instead of the web server.

a. Plugin flag at managed server level

- i. Click on 'Environment' -> 'Servers' -> '<ManagedServer>' -> 'General' -> 'Advanced'
- ii. Check the 'WebLogic Plug-In Enabled' box.
- iii. Click 'Save'
- iv. Restart the Server.

b. Plugin flag at domain level

- v. Click on <Domain> -> 'Web Applications'
- vi. Check the 'WebLogic Plug-In Enabled' box.
- vii. Click 'Save'
- viii. Restart the server.

## 6. Compression rule setting

Content compression in Oracle HTTP Server is done using mod\_deflate. This can compress HTML, text or XML files to approx. 20 - 30% of their original sizes, thus saving on server traffic. However, compressing files causes a slightly higher load on the server, but clients' connection times to server is reduced.

### 6.1 Loading mod\_deflate

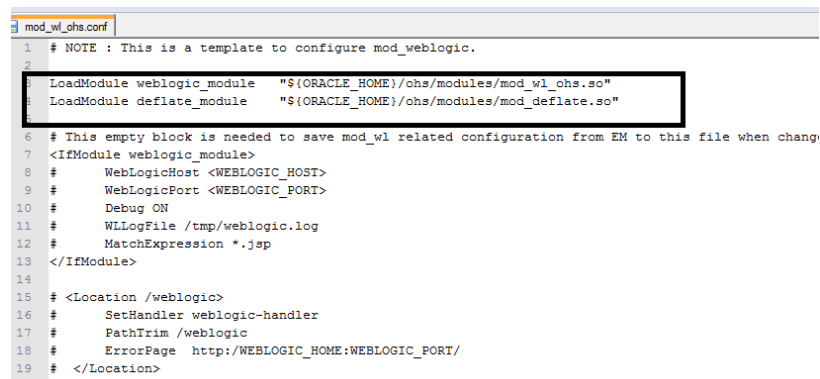
mod\_deflate is used for compression in OHS and this is installed in Oracle HTTP Server under location

"\${ORACLE\_HOME}/OHS/modules/mod\_deflate.so"

But it might not be loaded.

To load the file add the below directive in mod\_wl\_ohs.conf file

LoadModule deflate\_module "\${ORACLE\_HOME}/OHS/modules/mod\_deflate.so"



```
1 # NOTE : This is a template to configure mod_weblogic.
2
3 LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"
4 LoadModule deflate_module "${ORACLE_HOME}/ohs/modules/mod_deflate.so"
5
6 # This empty block is needed to save mod_wl related configuration from EM to this file when chang
7 <IfModule weblogic_module>
8 #     WebLogicHost <WEBLOGIC_HOST>
9 #     WebLogicPort <WEBLOGIC_PORT>
10 #     Debug ON
11 #     WLLogFile /tmp/weblogic.log
12 #     MatchExpression *.jsp
13 </IfModule>
14
15 # <Location /weblogic>
16 #     SetHandler weblogic-handler
17 #     PathTrim /weblogic
18 #     ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
19 # </Location>
```

### 6.2 Configuring file types

mod\_deflate also requires to specify which type files are going to be compressed.

In the LOCATION section of mod\_wl\_ohs.conf file add the below entries.

AddOutputFilterByType DEFLATE text/plain

AddOutputFilterByType DEFLATE text/xml

AddOutputFilterByType DEFLATE application/xhtml+xml

AddOutputFilterByType DEFLATE text/css

AddOutputFilterByType DEFLATE application/xml

AddOutputFilterByType DEFLATE application/x-javascript

AddOutputFilterByType DEFLATE text/html

SetOutputFilter DEFLATE

Images are supposed to be in a compressed format, and therefore are bypassed by mod\_deflate.

```

21      <Location /FCJNeoWeb>
22          SetHandler weblogic-handler
23          WebLogicHost wlserver1
24          WebLogicPort 7707
25
26          AddOutputFilterByType DEFLATE text/plain
27          AddOutputFilterByType DEFLATE text/xml
28          AddOutputFilterByType DEFLATE application/xhtml+xml
29          AddOutputFilterByType DEFLATE text/css
30          AddOutputFilterByType DEFLATE application/xml
31          AddOutputFilterByType DEFLATE application/x-javascript
32          AddOutputFilterByType DEFLATE text/html
33          SetOutputFilter DEFLATE

```

### 6.3 httpd.conf file changes

This is a server configuration file which typically contains directives that affect how the server runs, such as user and group IDs it should use, and location of other files. Cross check the existence of mod\_wl\_ohs.conf include in httpd.conf file.

httpd.conf file is present under location

"\${ORACLE\_INSTANCE}/config/OHS/{COMPONENT\_NAME}/httpd.conf"

In this file cross check for the below entry

include "\${ORACLE\_INSTANCE}/config/OHS/\${COMPONENT\_NAME}/mod\_wl\_ohs.conf"

If above include entry is not present, then add the above include section.

```

013 #Directives to setup logging via OUL
014 OraLogDir "${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_NAME}"
015 OraLogMode odl-text
016 OraLogSeverity WARNING:32
017 OraLogRotationParams S 10:70
018
019
020 # Set it to On to enable Audit Logs
021 OraAuditEnable On
022
023 # Include the configuration files needed for mod_weblogic
024 include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/mod_wl_ohs.conf"
025
026 # Include the SSL definitions and Virtual Host container
027 include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/ssl.conf"
028
029 # Include the admin virtual host (Proxy Virtual Host) related configuration
030 include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/admin.conf"
031
032 include "moduleconf/*.conf"
033

```

## 7. Configuring SSL for Oracle HTTP Server

Secure Sockets Layer (SSL) is required to run any Web site securely. Secure Sockets Layer (SSL) is an encrypted communication protocol that is designed to securely send messages across the Internet.

Reading of “**SSL\_Configuration on Weblogic**” document provided as part of FCIS installation is recommended before proceeding with further setup.

In Oracle HTTP server, SSL configuration can be done between

1. Browser to Oracle HTTP Server (Mandatory)
2. Oracle HTTP Server to Oracle Weblogic Server(If required)

### 7.1 SSL configuration for Inbound Request to Oracle HTTP Server

Perform these tasks to enable and configure SSL between browser and Oracle HTTP Server.

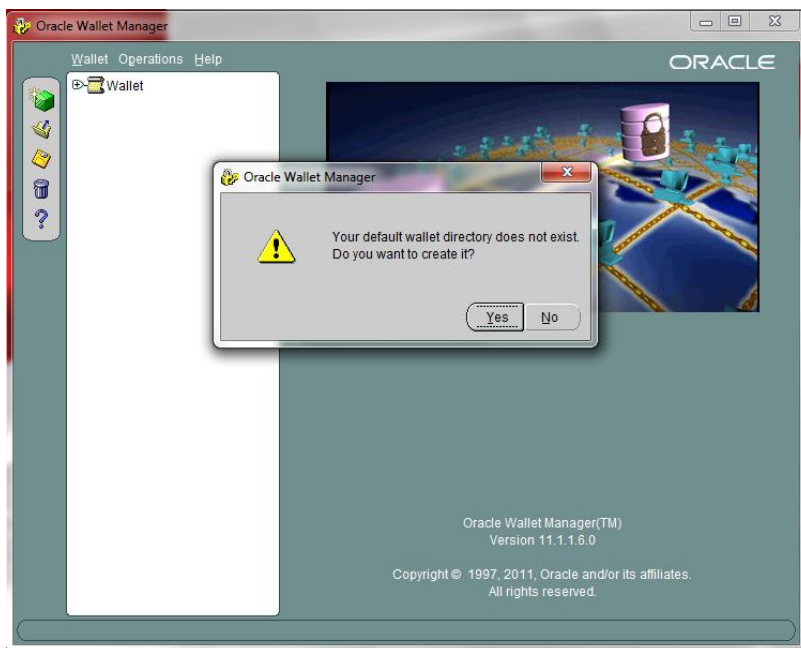
1. Obtain a certificate from CA or create a self signed certificate.
2. Create an Oracle Wallet which contains the above SSL Certificate. The default wallet that is automatically installed with Oracle HTTP Server is for testing purposes only. The default wallet is located in  
"`${ORACLE_INSTANCE}/config/OHS/${COMPONENT_NAME}/keystores/default`"
3. Configuring Wallet in ssl.conf file

#### 7.1.1 Create a new Wallet and import Certificate

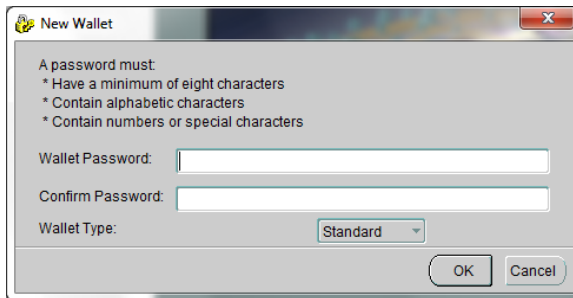
1. Go to the `\Oracle_WT1\bin\launch.exe`, this will launch your wallet manager



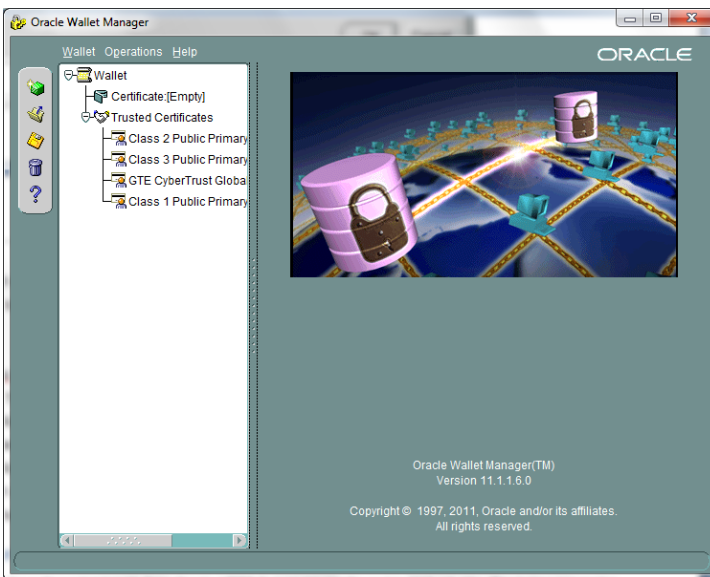
2. Click on Create new and then click no option.



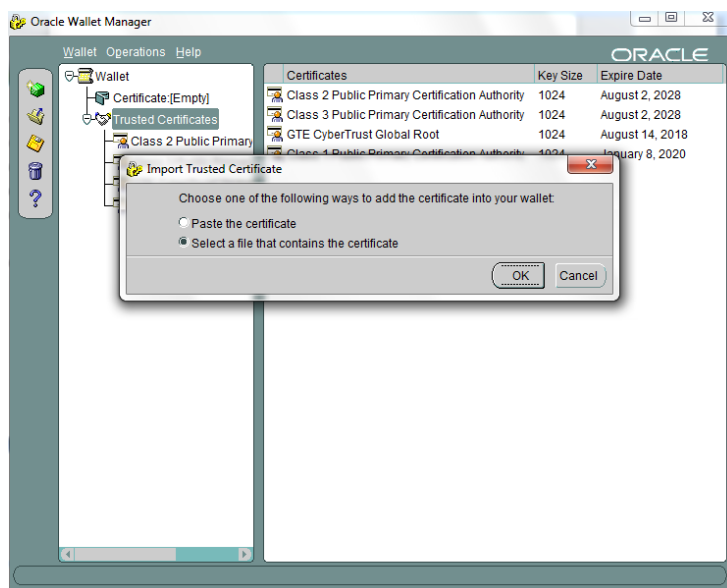
3. Enter the wallet password and click on OK, this will create a new wallet.



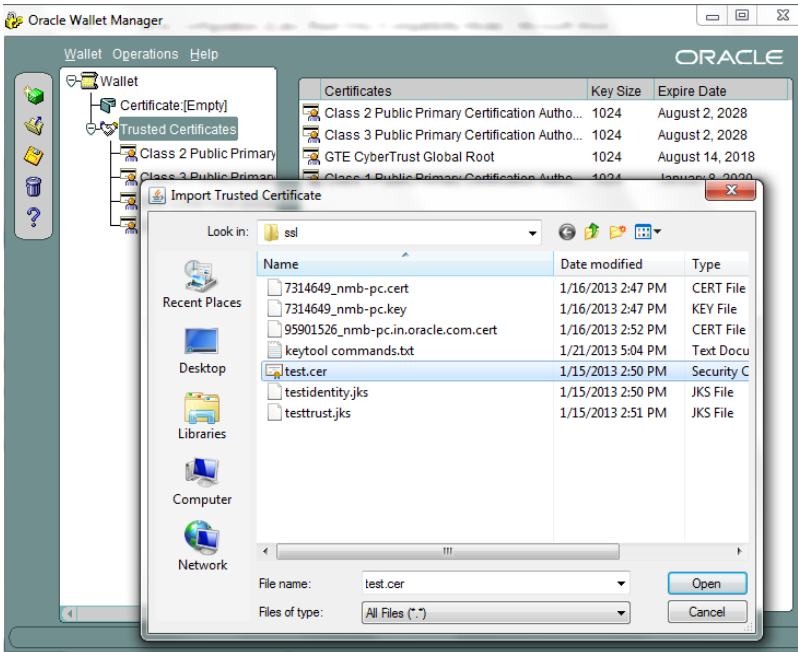
4. Not it will ask for certificate request creation, Click on NO to proceed



5. Right click on trusted certificates and then import trusted certificate.

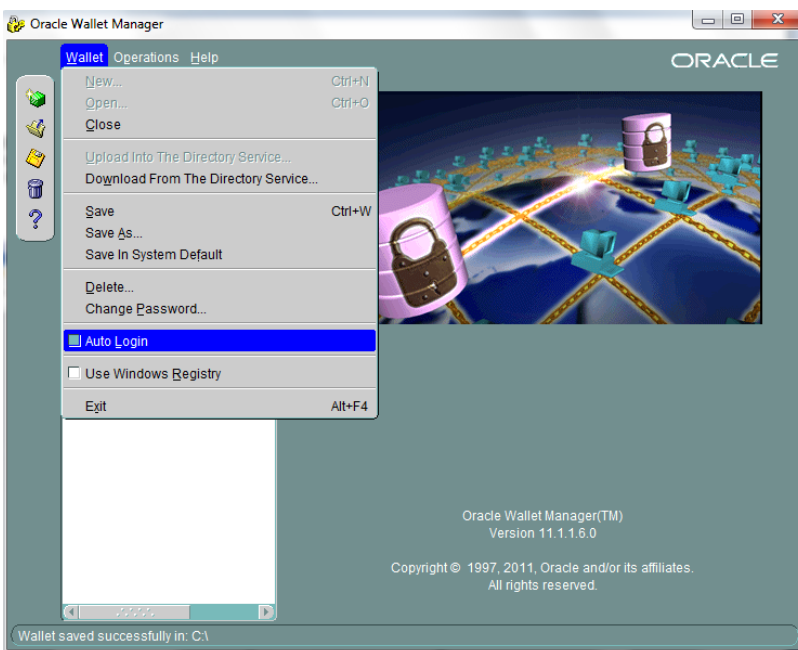


6. Browse to the folder where certificate is stored and click on Open



7. Click on Save Wallet button on the left side navigation and save the wallet either to default location("`{ORACLE_INSTANCE}/config/OHS/{COMPONENT_NAME}/keystores/default`") or folder of your choice.

8. Click on Wallet tab and enable Auto Login



### 7.1.2 Configuring Wallet in ssl.conf file

In ssl.conf file the newly created wallet need to updated. This file is located under folder

"\${ORACLE\_INSTANCE}/config/OHS/\${COMPONENT\_NAME}/

1. Change the SSLWallet directive to point to the location of new wallet created.

SSLWallet "\${ORACLE\_INSTANCE}/config/\${COMPONENT\_TYPE}/\${COMPONENT\_NAME}/keystores/"

```

1  # Allow the cipher suites that the client is permitted to negotiate.
2  SSLCipherSuite
3  SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_DES_CBC_SHA,
4  AES_256_CBC_SHA
5
6  # SSL Certificate Revocation List Check
7  # Valid values are On and Off
8  SSLCRLCheck Off
9
10 #Path to the wallet
11 SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/"
12
13 <FilesMatch "\.(cgi|shtml|phtml|php)$">
14     SSLOptions +StdEnvVars
15 </FilesMatch>
16
17 <Directory "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/cgi-bin">
18     SSLOptions +StdEnvVars
19 </Directory>
20
21 BrowserMatch ".MSIE.*" \
22     nokeepalive ssl-unclean-shutdown \
23     downgrade-1.0 force-response-1.0
24
25 </IfModule>
26 </VirtualHost>
27
28 </IfModule>

```

2. Change the Listen port number in ssl.conf file to the SSL enabled port, by default the value is 4443

```

1  #####
2  # Oracle HTTP Server mod_oss1 configuration file: ssl.conf      #
3  #####
4
5
6  # OHS Listen Port
7  Listen 4443
8
9  <IfModule oss1_module>
10  ##
11  ##  SSL Global Context
12  ##
13  ##  All SSL configuration in this context applies both to
14  ##  the main server and all SSL-enabled virtual hosts.
15  ##
16
17  #
18  #  Some MIME-types for downloading Certificates and CRLs
19  AddType application/x-x509-ca-cert .crt
20  AddType application/x-pkcs7-crl    .crl
21
22  #  Pass Phrase Dialog:

```



## 7.2 Configuring SSL between Oracle HTTP Server and Oracle Weblogic Server

SSL for outbound requests from Oracle HTTP Server are configured in mod\_wl\_ohs.

Refer to “**SSL\_Configuration on Weblogic**” document for weblogic server setting mentioned in below section.

### 7.2.1 Turn off KeepAliveEnabled

The below parameter in mod\_wl\_ohs should be turned off, by default it is on. Add the below directive under LOCATION section of mod\_wl\_ohs file

KeepAliveEnabled OFF

```

6      AddOutputFilterByType DEFLATE text/plain
7      AddOutputFilterByType DEFLATE text/xml
8      AddOutputFilterByType DEFLATE application/xhtml+xml
9      AddOutputFilterByType DEFLATE text/css
0      AddOutputFilterByType DEFLATE application/xml
1      AddOutputFilterByType DEFLATE application/x-javascript
2      AddOutputFilterByType DEFLATE text/html
3      SetOutputFilter DEFLATE
4
5      KeepAliveEnabled OFF
6
7      WlSSLWallet "D:\misc\ssl\"
8  </Location>
9

```

### 7.2.2 To enable one-way SSL

1. Generate a custom keystore identity.jks for Weblogic Server containing a certificate.
2. At Identity section in Keystores tab in weblogic Admin Console for server set
  - a. The custom trust store with the identity.jks file location
  - b. The keystore type as JKS
  - c. The passphrase used to created the keystore

Home > base\_domain > Summary of Environment > Summary of Servers > AdminServer

Messages

- Changes to your Keystore configuration may require you to update your SSL Configuration. Please review your settings on the SSL tab.
- All changes have been activated. No restarts are necessary.
- Settings updated successfully.

Settings for AdminServer

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations to manage the security of message transmissions.

Keystores:	Custom Identity and Custom Trust: Change	Which configuration rules should be used for... More Info...
<b>Identity</b>		
Custom Identity Keystore:	D:\misc\testidentity.jks	The path and file name of the identity keystore.
Custom Identity Keystore Type:	JKS	The type of the keystore. Generally, this is JKS.
Custom Identity Keystore Passphrase:	*****	The encrypted custom identity keystore's passphrase. If the keystore is opened without a passphrase, it will be opened without a passphrase.
Confirm Custom Identity Keystore Passphrase:	*****	
<b>Trust</b>		
Custom Trust Keystore:	D:\misc\testtrust.jks	The path and file name of the custom trust keystore.
Custom Trust Keystore Type:	JKS	The type of the keystore. Generally, this is JKS.
Custom Trust Keystore Passphrase:	*****	The custom trust keystore's passphrase. If the keystore is opened without a passphrase, it will be opened without a passphrase. More Info
Confirm Custom Trust Keystore Passphrase:	*****	

- Copy the certificate to Oracle HTTP Server and import the new certificate into OHS wallet as a trusted certificate.
- Add following new directive in mod\_wl\_ohs.conf to point to the wallet location

WISSLWallet "\${ORACLE\_INSTANCE}/config/OHS/{COMPONENT\_NAME}/keystores/default"

- Change the port in mod\_wl\_ohs file to point to SSL port of Weblogic server.

```

20
21 <Location /FCJNeoWeb>
22   <SetHandler weblogic-handler>
23     WebLogicHost wlsserver1
24     WebLogicPort 443
25
26     AddOutputFilterByType DEFLATE text/plain
27     AddOutputFilterByType DEFLATE text/xml
28     AddOutputFilterByType DEFLATE application/xhtml+xml
29     AddOutputFilterByType DEFLATE text/css
30     AddOutputFilterByType DEFLATE application/xml
31     AddOutputFilterByType DEFLATE application/x-javascript
32     AddOutputFilterByType DEFLATE text/html
33     SetOutputFilter DEFLATE
34
35     KeepAliveEnabled OFF
36
37     WISSLWallet "${ORACLE_INSTANCE}/config/OHS/{COMPONENT_NAME}/keystores/"
38 </Location>
39
40

```

- Restart both Weblogic Server and Oracle HTTP Server

### 7.2.3 To enable two-way SSL

1. Perform one-way SSL configuration steps
2. Generate a new trust store, trust.jks for Weblogic server
3. Keystore created for one-way SSL could be used, but it is recommended to create a separate truststore
4. Export the user certificate from Oracle HTTP Server wallet, and import it into truststore created above
5. At Trust section in Keystores tab in Weblogic Admin Console for the server set
  - a. The custom trust store with the trust.jks file location
  - b. The keystore type as JKS
  - c. The passphrase used to created the keystore

Messages

⚠ Changes to your Keystore configuration may require you to update your SSL Configuration. Please review your settings on the SSL tab.

✓ All changes have been activated. No restarts are necessary.

✓ Settings updated successfully.

Settings for AdminServer

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystores to manage the security of message transmissions.

**Keystores:** Custom Identity and Custom Trust [Change](#) Which configuration rules should be used for trust keystores? [More Info...](#)

**Identity**

**Custom Identity Keystore:** D:\misc\testidentity.jks The path and file name of the identity keystore.

**Custom Identity Keystore Type:** JKS The type of the keystore. Generally, this is JKS.

**Custom Identity Keystore Passphrase:** ..... The encrypted custom identity keystore's passphrase. If the keystore will be opened without a passphrase, leave this field blank.

**Confirm Custom Identity Keystore Passphrase:** .....

**Trust**

**Custom Trust Keystore:** D:\misc\testtrust.jks The path and file name of the custom trust keystore.

**Custom Trust Keystore Type:** JKS The type of the keystore. Generally, this is JKS.

**Custom Trust Keystore Passphrase:** ..... The custom trust keystore's passphrase. If the keystore will be opened without a passphrase, leave this field blank.

**Confirm Custom Trust Keystore Passphrase:** .....

6. Under the SSL tab

Ensure trusted CA is set as from Custom Trust Keystore.

Home Log Out Preferences Record Help

Home > base\_domain > Summary of Environment > Summary of Servers > AdminServer

**Settings for AdminServer**

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores **SSL** Federation Services Deployment Migration Tuning Overload Health Monitoring S

Configuration - Services- Tab

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security c

**Identity and Trust Locations:** Keystores  Indicates where SSL should find (key) as well as the server's tru

**Identity**

**Private Key Location:** from Custom Identity Keystore The keystore attribute that def Info...

**Private Key Alias:** selfcert The keystore attribute that def the server's private key. More

**Private Key Passphrase:** ..... The keystore attribute that def server's private key. More Int

**Confirm Private Key Passphrase:** ..... More Info...

**Certificate Location:** from Custom Identity Keystore The keystore attribute that def certificate. More Info...

**Trust**

**Trusted Certificate Authorities:** from Custom Trust Keystore The keystore attribute that def authorities. More Info...

**Advanced**

## 7. Restart Weblogic Server

## 8. Starting, Stopping, and Restarting Oracle HTTP Server

Navigate to the below location in command prompt `${ORACLE_INSTANCE}/bin/` and run below commands

### 8.1 Start

```
opmnctl startproc ias-component={COMPONENT_NAME}
```

Example: `opmnctl startproc ias-component=ohs1`

### 8.2 Stop

```
opmnctl stopproc ias-component={COMPONENT_NAME}
```

Example: `opmnctl stopproc ias-component=ohs1`

### 8.3 Restart

```
opmnctl restartproc ias-component={COMPONENT_NAME}
```

Example: `opmnctl restartproc ias-component=ohs1`

## 9. Test the application

Test the application deployed on Weblogic using Oracle HTTP Server after restarting both the oracle http server and weblogic server

`https://ohs_servername:ohs_https_port/<<context/url>>`

`http://ohs_servername:ohs_http_port/<<context/url>>`

ohs\_servername: server on which OHS is deployed

ohs\_https\_port: port number mentioned against LISTEN directive in SSL.conf file

ohs\_http\_port: port number mentioned against LISTEN directive in httpd.conf file

Example:

`https://localhost:4443/FCJNeoWeb/welcome.jsp`

Or

`http://localhost:7777/FCJNeoWeb/welcome.jsp`

## 10. Server Logs Location

Oracle HTTP Server Logs are generated under folder

`${ORACLE_INSTANCE}/diagnostics/logs/OHS/{COMPONENT_NAME}/`

## 11. References

SSL\_Configuration.doc for Weblogic provided as part of FCIS installation.

[http://docs.oracle.com/cd/E16764\\_01/web.1111/e10144/under\\_mods.htm](http://docs.oracle.com/cd/E16764_01/web.1111/e10144/under_mods.htm)

[http://docs.oracle.com/cd/E25054\\_01/core.1111/e10105/sslconfig.htm](http://docs.oracle.com/cd/E25054_01/core.1111/e10105/sslconfig.htm)





Oracle\_HTTP\_Server\_Configuration

[September] [2016]

Version 12.3.0.0.0

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

[www.oracle.com/financialservices/](http://www.oracle.com/financialservices/)

Copyright © 2007, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.