



## 10gAS SSL / Certificate Based Authentication Configuration

---

### I. Overview

This document covers the processes required to create a self-signed certificate or to import a 3<sup>rd</sup> party certificate using the Oracle Certificate Authority. In addition, the steps to configure the App Server for SSL and Certificate Base Authentication are included.

### II. SSL Certificate Creation

An SSL certificate is required in order to enable encryption between the web server and client. Oracle's Application Server is delivered with a Server Certificate that is meant only for testing. This section of the document explains how to use Oracle's Certificate Authority (OCA) to create a Certificate Signing Request (CSR) and then use that CSR to create a real Server Certificate. This CSR can also be used to obtain a Server Certificate from a Trusted Authority like Verisign.

Because the Server Certificate will be created and "signed" by OCA, a standard browser will not recognize it as a "trusted" certificate. Trusted Certificates are pre-loaded in the browser and are available at all times. So if you request a Server Certificate from Verisign, your browser already recognized it as being trusted. You can, however, load the OCA created certificate in your browser permanently and effectively "trust" it. From that point on, the browser will not display a trust warning when you connect to a site that uses the OCA certificate.

#### A. Certificate Creation

The default wallet directory should be named : `/etc/ORACLE/WALLETS/<user>`

By default, a directory called `/etc/oracle` may already exist and will likely be owned by root so the ownership of the directories must be changed to oracle. The name of the directory must be changed to `/etc/ORACLE` before doing anything else.

Once the name has been changed, add the following subdirectories :

`/WALLETS/<user that installed the app server>`

The finished directory should look like this:

`/etc/ORACLE/WALLETS/oracle`

Change to the `/etc` directory and modify the owner/group of `/etc/ORACLE/WALLETS/oracle` to `oracle/dba` using the following command:

`chown oracle:dba ORACLE`



## 10gAS SSL / Certificate Based Authentication Configuration

---

### B. Run the Oracle Wallet Manager (owm) from <ORACLE\_HOME>/bin

If the process in step 1 is not done correctly, owm will tell you that the default wallets directory does not exist and asks if you would like to create it. If any of the directories under /etc/ORACLE are still owned by root, this will also fail. If everything works correctly, the “New Wallet” window will appear asking for a password for the new wallet.

1. Click the <Wallet> menu and then <New>
2. Enter the password : enk1tec1

Passwords must be at least 8 chars and contain both alpha and numeric characters.

2. Leave the wallet type set to <Standard>
3. The next popup asks if you want to create a new Certificate Signing Request (CSR). Answer <Yes>.
4. For the parameters of the CSR, use the following values

Common Name : specify the name or alias of the site that will be configured for HTTPS support. (**bart.enkitec.com**)  
Organizational Unit : IT  
Organization : enkitec  
Locality / City : grapevine  
State / Province : TX  
Country : US  
Key Size : 2048

3. Click <Ok>

If the CSR (Certificate Signing Request) was created correctly, a window will pop up telling you that it was created successfully.

4. Click <Ok>



## 10gAS SSL / Certificate Based Authentication Configuration

---

### C. Creating a Certificate Signing Request (CSR)

Once the CSR has been created, a certificate can be created either by using Oracle Certificate Authority (OCA) or by sending the CSR to another Certificate Authority (CA) like Verisign or Thawte. If using a public CA, skip the next section which describes how to use OCA to create the certificate.

1. Check the status of the OCA. Run the following command on the machine where the infrastructure is installed:

```
<$ORACLE_HOME>/oca/bin/ocactl status
```

You will be prompted for the OCA password (enk1tecoca)

If it shows that the OCA is not running, start it using the following command:

```
<$ORACLE_HOME>/oca/bin/ocactl start
```

You will be prompted for the OCA password (enk1tecoca)

2. Run the OCA Administration Interface

**Note** - Don't try this with FireFox. Use IE here.

The OCA Administrator requires that you get the Administrator Certificate before you can use any of the tools. This is done the first time you log in. This cert is used to encrypt the traffic between you and the OCA administration interface.

The OCA Admin page is accessed via URL. The port number used in this URL is listed in portlist.ini as the following:

Oracle Certificate Authority SSL Server Authentication port = 6600

Check ../install/portlist.ini for the actual port for oca

The URL is as follows:

```
https://<host>.enkitec.com:<port>/oca/admin
```

When the page is displayed, click the "Click Here" link to fill out the enrollment form. Fill in the fields of this form as follows:



## 10gAS SSL / Certificate Based Authentication Configuration

---

Common name	The name that you want on the certificate <b>bart.enkitec.com</b>
Email address	Email address of the administrator <b>oca_admin@enkitec.com</b>
Organization unit belongs	Name of the organization unit or division to which the administrator belongs <b>IT</b>
Organization belongs	Name of the company or organization to which the administrator belongs <b>enkitec</b>
Location	The city location of the administrator <b>grapevine</b>
State	The state or province of the administrator <b>TX</b>
Country	Two-letter code for the administrator's country <b>US</b>
Password	Password for the oca_admin account. This must be the same password assigned during the install of OCA. <b>enk1tecoca</b>

### D. Signing the CSR and Creating a Certificate

Now that the CSR has been created and stored in the Wallet Manager on the server, it can be used to create an actual certificate. To do this, the CSR needs to be exported from the Wallet Manager and imported into the OCA using the OCA Web Interface.

To Export the CSR from the Wallet Manager and import it into the OCA Admin tool, do the following:

1. Open the Wallet Manager on the Server. `$INFRA_HOME/bin/owm`



## 10gAS SSL / Certificate Based Authentication Configuration

---

2. Highlight the CSR and click <Operations><Export> from the menu
3. Name and Save the CSR. Give it a recognizable name and “.csr” extension
4. Open the file and copy the entire contents into the clip board
5. Nav to the OCA Web Interface. <https://host:port/oca/user>
6. If this is the first time this interface is accessed, do the following:
  1. Click on **“click here to install the certificate authority certificate into your browser”**

Follow the prompts to install the cert in your browser. This will install the admin cert in your browser. You should export this cert from your browser to a file immediately since you only have one chance to obtain the cert (don't know how OCA knows you have been here before).
  2. Click on **“click here to save the certificate authority certificate to your file system”**
7. Once the Certificate Authority Certificate is loaded, click on the <Server / SubCA Certificates> tab
8. In the <PKCS#10 Request> field, paste in the CSR from the Wallet Manager (obtained in steps 1-4).
9. Supply a Name / eMail address / phone number. These are required but are not tied to anything in the Certificate.
10. Approve the CSR by going to <https://host:port/oca/admin>
11. Click the <

The OCA administration interface can now be used to accept CSR's and create certificates.

2. Send the CSR to OCA to create the new Server Certificate

Either copy the text of the CSR into the clipboard or write it to a file. Depending on the XWindows system being used, you may or may not be able to copy the text so that it can be pasted later.

Use the following URL to access the User page of the OCA:

<https://bart.enkitec.com:6600/oca/user>



## 10gAS SSL / Certificate Based Authentication Configuration

---

Click the **Server/SubCA certificates** tab to access the certificate request form.

Press the **Request Certificate** button to import the certificate request that you created with the Oracle Wallet Manager.

Copy the content stored in the clipboard to the **Certificate Request** field in the OCA form. Enter the information required on this page and press the **Submit** button.

### 3. Approve the CSR

Open the OCA administration page with a browser that has the OCA Administrator Certificate installed and click the **Certificate Management** tab.

The Certificate Management tab shows a list of all pending certificate requests. Press the **View Details** button to approve or reject the selected certificate request. To approve a request, press the **Approve** button.

This creates the server certificate that must be imported into the Oracle Wallet Manager. In addition, because OCA is not a commercial certificate authority, you need to download the root certificate of the OCA instance and add it to the list of trusted root certificates in Oracle Wallet Manager. This however is the job of the certificate requestor, which in the Oracle Forms Services case is not necessarily the same person administering OCA.

### 4. Obtaining the Root Certificate from OCA

In order to be able to use the certificate that was just created, the root certificate from OCA must be imported into the wallet. If you don't have this root certificate in the wallet, it will not allow you to import the server certificate that was just created since OCA is not a "trusted certificate authority" like Verisign or Entrust (the wallet comes with root certs from GTE, Entrust, and others).

To download the OCA root certificate, select the [click here](#) link below the *Oracle Wallet Manager or Web server administrators* headline.



## 10gAS SSL / Certificate Based Authentication Configuration

---

5. Importing the root certificate
6. Importing the server certificate
7. Saving the Wallet

Note - Make sure to check the “Auto Login” checkbox under the <Wallet> menu or you will not be able to assign this wallet to the web cache.

### III. Convert Infrastructure to SSL

In order to configure the Infrastructure Layer to SSL, the SSLConfigTool can be used. This only works in release 10.1.2 or later. In addition, the Infrastructure layer must be set up for SSL in order to use Certificate Based Authentication.

#### A. Automatic SSL Configuration

This section describes how to set up the Infrastructure component of the App Server 10gR2 to respond to SSL requests. The automated method using a tool called **SSLConfigTool**



## 10gAS SSL / Certificate Based Authentication Configuration

---

1. Set ORACLE\_HOME to the Infrastructure home
2. \$ORACLE\_HOME/bin/SSLConfigTool -config\_w\_prompt -opwd **enk1tec**
3. Do you want to configure your site to accept browser requests using SSL protocol?  
[y]: **y**
4. What is the virtual host name for your site? [marge.enkitec.com]: login.enkitec.com  
Note – this is a virtual name for this machine. If you have more than one SSL based App Server on a machine, this name must be unique.
5. What is the virtual port number for your site? [4444]: **4444**
6. Does your site have an external load balancer (LBR)?  
Note: Do NOT include OracleAS Web Cache as LBR here. [y]: **n**
7. Does your site have OracleAS Web Cache? [y]: **n**
8. Do you want to supply your own wallet location for OHS? [n]: **n**
9. You have supplied all the information. Are you ready to continue? [y]: **y**  
Note : Several scripts will now be run. This can take several minutes to complete. Be patient.
10. Run the following command to re-register the Portal with Single Sign On  
`<mid_tier_home>/portal/conf/ptlconfig -dad portal -site -wc -em`

### B. Testing the SSL Configuration

Check the \$ORACLE\_HOME/install/portlist.ini to get the SSL port for the Infrastructure layer to get the HTTPS listen port. It will look something like this:

Oracle HTTP Server Listen (SSL) port = 4444

To test the configuration, access the Portal using the HTTP Server Port. This is the second port listed in the portlist.ini file named "HTTP Server Listen Port = 9999".



## 10gAS SSL / Certificate Based Authentication Configuration

---

<http://server.domain.com:9999/pls/portal>

You should be redirected to the SSL based SSO server. You will know this worked if the browser asks you to accept or view the server's certificate. Accept the certificate **temporarily** and then log in as the "Portal" user. Notice that the Portal pages are not HTTPS (SSL) pages, only the SSO server is encrypting content at this point.

### C. Creating New Users

After converting the OSSO server to SSL, the Create User function in the Portal no longer works. This issue can be avoided using the one of the following two methods:

#### Use OIDDAS directly to create users

1. Navigate to [https://server:ssl\\_port/oiddas](https://server:ssl_port/oiddas)
2. Click on the <Directory> tab
3. Click on <Create> above the user list
4. Fill in the required fields and click <Submit>
5. Verify that the user was created by clicking on the <Go> button next to "Advanced Search"

#### Fix the Portal

Steps TBD

## IV. Configuring the SSO Server for Certificate Based Authentication

Certificate Based Authentication allows a user who has a "Client Certificate" pass the SSO Server without providing a username / password. This section will describe how to set up the SSO Server for this type of authentication along with how to generate Client Certificates.

These steps are taken almost directly from Appendix E of the Oracle Certificate Authority Administration guide.

### A. Enabling Certificate Base Authentication for SSO

1. The process of requesting a User Certificate requires authenticating to the OCA via browser. By default, OCA expects the user to already have a user certificate. This step



## 10gAS SSL / Certificate Based Authentication Configuration

---

negates that requirement and allows the user to request a certificate using their Single Sign-On id.

Edit `$ORACLE_HOME/sso/conf/policy.properties`

Add or Edit the following lines:

```
DefaultAuthLevel = MediumHighSecurity
MediumHighSecurity_AuthPlugin =
oracle.security.sso.server.auth.SSOX509CertAuth
MediumSecurity_AuthPlugin =
oracle.security.sso.server.auth.SSOServerAuth
Oca_hostname\:port = MediumSecurity
```

### 2. Restart the SSO Server

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
$ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

## B. Changing the OCA Wallet Password

```
Stop oca
ocactl setpasswd -type CASSL <Enter>
Start oca
```

## C. Update the ssl.conf file

SSLWallet

The location, or path, of the server wallet. The default location is

`ORACLE_HOME/Oracle/Oracle/conf/ssl.wlt/default`.

Note: The actual location of the Oracle home must be substituted for the variable.

If OracleAS Certificate Authority is installed in the same Oracle home as OracleAS Single Sign-On, and you want to use this CA to issue certificates, the wallet location is

`ORACLE_HOME/oca/wallet/ssl`. See ["Choosing a Certificate Authority"](#) for details.

SSLWalletPassword

Password for the server wallet

SSLVerifyClient

The verification type for client certificates. These are the three types:



## 10gAS SSL / Certificate Based Authentication Configuration

---

- `none`—SSL without certificates
- `optional`—server certificate and optionally client certificate
- `require`—server and client certificates

You must choose either `optional` or `require`.

3.

### D. Restart everything on both tiers

### E. Request a user certificate

Here are my revised notes:

- Brian

MARGE

=====

Infrastructure:

-----

From [http://download-west.oracle.com/docs/cd/B14099\\_19/core.1012/b13995/ssl\\_config\\_tool.htm#BABIAHEB](http://download-west.oracle.com/docs/cd/B14099_19/core.1012/b13995/ssl_config_tool.htm#BABIAHEB):

- 1) Set ORACLE\_HOME to the Infrastructure home
- 2) \$ORACLE\_HOME/bin/SSLConfigTool -config\_w\_prompt -opwd enk1tec
- 3) Do you want to configure your site to accept browser requests using SSL protocol? [y]: y
- 4) What is the virtual host name for your site? [marge.enkitec.com]: login.enkitec.com
- 5) What is the virtual port number for your site? [4444]: 4444 \*\*\*I recommend using the Oracle HTTP Server Listen (SSL) port from \$OH/install/portlist.ini!!!\*\*\*
- 6) Does your site have an external load balancer (LBR)?  
Note: Do NOT include OracleAS Web Cache as LBR here. [y]: n



## 10gAS SSL / Certificate Based Authentication Configuration

---

- 7) Does your site have OracleAS Web Cache? [y]: n
- 8) Do you want to supply your own wallet location for OHS? [n]: n
- 9) You have supplied all the information. Are you ready to continue? [y]: y

NOTE: This will cause Enterprise Manager to indicate that the "Single Sign-On:orasso" component is down. Need to import the root CA certificate into the EM wallet.

\*\*\*

If this causes HTTP-403 "Forbidden" "You don't have permission to access /sso/auth on this server" when trying to login to Portal, see MetaLink Note:334172.1

\*\*\*

Middle Tier:

-----

From [http://download-west.oracle.com/docs/cd/B14099\\_19/portal.1014/b19305/cg\\_secur.htm#CHDEAJAC](http://download-west.oracle.com/docs/cd/B14099_19/portal.1014/b19305/cg_secur.htm#CHDEAJAC):

When choosing the SSL port #, I recommend using the Oracle HTTP Server Listen (SSL) port from \$OH/install/portlist.ini! Otherwise, you will have to change the listen port in Apache (and maybe other places).

- 1) Web Cache
  - a) From Web Cache Admin, add a port: IP Address=\*, Port=4446, Protocol=HTTPS, Require Client-Side Certificates for HTTPS=Not Required, Wallet for HTTPS=/opt/oracle/product/oas/10.1.2/mid/Apache/Apache/conf/ssl.wlt/default
  - b) From Web Cache Admin:
    - 1) Add a site: Host=portal.enkitec.com, Port=4446, Prefix=<blank>, Selected Origins Servers=marge.enkitec.com:7782
    - 2) Click "OK"
    - 3) Select the new site and click "Set as Default Site"
  - c) Restart Web Cache

- 2) PPE
  - a) Backup and edit \$ORACLE\_HOME/j2ee/OC4J\_Portal/applications/portal/portal/WEB-INF/web.xml
  - b) Add the following lines to the section for the "page" servlet:

```
<init-param>
  <param-name>useScheme</param-name>
  <param-value>http</param-value>
</init-param>
<init-param>
  <param-name>usePort</param-name>
  <param-value>7781</param-value>
</init-param>
<init-param>
  <param-name>httpsports</param-name>
  <param-value>4446</param-value>
</init-param>
```

- c) Save and exit

- 3) Re-Register HTTP Server Partner Application



## 10gAS SSL / Certificate Based Authentication Configuration

---

a) Execute:

```
$ORACLE_HOME/sso/bin/ssoreg.sh -oracle_home_path $ORACLE_HOME -site_name portal.enkitec.com  
-config_mod_osso TRUE  
-mod_osso_url https://portal.enkitec.com:4446 -config_file  
$ORACLE_HOME/Apache/Apache/conf/osso/osso.conf -admin_info cn=orcladmin
```

4) Specify the OracleAS Portal Published Address and Protocol

- a) From EM console, click "Portal:portal"
- b) Click "Portal Web Cache Settings" in the Administration section
- c) Change Listening Port to "4446"
- d) Change Listening Port SSL Enabled to "Yes"
- e) Click "Apply"
- f) Edit httpd.conf
- g) Add the following lines to the bottom of the file:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

```
NameVirtualHost 192.168.10.58:7782
```

```
<VirtualHost 192.168.10.58:7782>  
  ServerName portal.enkitec.com  
  Port 4446  
  SimulateHttps On  
  RewriteEngine On  
  RewriteOptions inherit  
</VirtualHost>
```

- h) Apply the changes and restart the HTTPS Server
- i) `$ORACLE_HOME/opmn/bin/opmnctl stopall`
- j) `$ORACLE_HOME/opmn/bin/opmnctl startall`