Renewing SSL Certificates in an Oracle WebLogic Server Environment

In order to renew an SSL certificate for an Oracle WebLogic Server environment, create a new certificate signing request, submit it to a CA, and import the signed server certificate into the server identity keystore.

If there is no change to the root certificate, and it has not expired, you should not have to re-import the root certificate or import certificates into client browsers.

You must delete the key pair in the keystore first; otherwise, you will get an error stating that the certificate alias already exists. If possible, use the same alias for the new certificate.

Procedure

1. Log on to each server as a user with administrative privileges.
2. Delete the current certificate using Java keytool.

   ```
   Keytool –delete –alias <certificate_name> -keystore <keystore_name>
   ```

   To get a list of certificates:

   ```
   Keytool -list -keystore <keystore_name>
   ```

3. Create the Certificate Signing Request (CSR) using Java keytool to create the key pair and a Certificate Signing Request (CSR) file.
4. Submit the request to the Certification Authority (CA).
   a. Submit the CSR to your Certification Authority (CA) to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.

   b. Download the approved CA certificates to a local directory. Make sure the certificates are named to distinguish them.

   Note: The CA can also be the root CA. Sometimes certificates are chained so you can have multiple. If you have multiple they all need to be imported from root down in sequence into the trusted keystore
5. Import the renewed server certificate into each application server by performing the following tasks:
   a. Log on to each OpenPages server as a user with administrative privileges.

   b. Launch a Command Prompt window (using the Run as Administrator option).

c. Navigate to the OpenPagesDomain directory in <OP_Home>.

By default, /opt/hint_108/user_projects/domains

d. Use the Keytool command within the OpenPagesDomain directory to import the server certificate (.cer) or certificate chain (.p7b) using the following command:

```
keytool -importcert -alias <certificate_name> -trustcacerts -file
<file_name> -keystore <keystore_name>
```

where

1. `import` imports the certificate.
2. `alias` is the name of the certificate.
3. `file` specifies the name of the file to store the certificate. The command may require the full path name.
4. `keystore` is the keystore associated with the certificate.
5. `trustcacerts` imports the certificate as a trusted certificate.

Note: You only need `-trustcacerts` if you are using Java Truststore.

Tip: Use different keystores for identity and trust, using the configuration setting "Custom Identity and Java Standard Trust" (Oracle WebLogic Server Administrative Console). The identity is coming from the custom keystore you created, and the trust is coming from the standard Java cacerts file (where you imported the trusted CA and intermediate CA as well).

The example imports the `servercert` certificate into the `opkeystore` file.

```
keytool -importcert

-alias opkeystore

-trustcacerts

-file hint.cer

-keystore hintstore.jks
```

e. Enter the password for the keystore.

f. Enter `Yes` to trust the certificate.

6. Update Oracle WebLogic server.