

---

# Kousec Server Certificate Manager

## Installing SSL Server Certificates to Oracle WebLogic Server

---

Copyright 2009 Kousec Software, Inc. All rights reserved.

Kousec and Kousec Server Certificate Manager are trademarks of Kousec Software, Inc.  
WebLogic and BEA WebLogic Server are registered trademarks of BEA Systems, Inc, a  
subsidiary of Oracle Corporation.

All company names and product names are trademarks of their respective holders.

r7

---

---

## Table of Contents

1. Introduction.....	4
1.1. Product Versions.....	4
2. Operations in Certificate Enrollment and Obtaining .....	5
3. Operations in Certificate Deployment.....	5
3.1. (A) Newly Installing the Certificate.....	6
Preparation on the server computer .....	6
Operations on CertMgr.....	6
Install the certificate on the server computer .....	7
Modifying Keystores and SSL Settings on WebLogic Server.....	8
3.2. (B) Updating the Certificate .....	9
Operations on CertMgr.....	9
Procedure for WebLogic Server 9 or Later Versions .....	9
Procedure for Versions prior to WebLogic Server 9 .....	10
4. Start Managing Existing WebLogic Server Certificate .....	11
4.1. Importing the Existing Keystore File .....	11
4.2. Importing Certificate in another Format.....	12
4.3. Daily Operations after the Import.....	12
5. Installing an SSL Server Certificate on Node Manager .....	13
5.1. Obtaining SSL Certificate for Node Manager .....	13
5.2. Installing SSL Certificate on to Node Manager.....	13
5.3. Configuration on WebLogic Administration Server.....	14
6. Summary .....	17

---

## 1. Introduction

In a WebLogic Server installation, the standard way of obtaining an SSL certificate begins with generating a key pair and CSR within a keystore file on the WebLogic Server computer.

When using Kousec Server Certificate Manager, the key pairs and CSRs are generated within the Kousec Server Certificate Manager computer and will be managed centrally there. Then, the WebLogic server administrator imports both the certificate and the corresponding private key to the keystore on the WebLogic Server instance. Therefore there is no need to generate a CSR on the WebLogic Server computer. When applying for an SSL certificate to the CA, specify the certificate format of Apache2. Then obtain the certificate and register it in Kousec Server Certificate Manager.

This document explains the procedure to install the certificate and private key registered in a Kousec Server Certificate Manager computer onto a WebLogic Server computer.

You can also use Kousec Server Certificate Manager as a tool to convert Apache-style or IIS-style SSL certificate and key to a format suitable for WebLogic Server, equipped with an automatic certificate installer.

In this document, Kousec Server Certificate Manager will be referred to as either “Kousec CertMgr” or just “CertMgr”.

### 1.1. Product Versions

Kousec Server Certificate Manager RC-1

Oracle WebLogic Server (formerly known as BEA WebLogic Server)

This document lists specific instructions when using the following product:

BEA WebLogic Server® 9.2 (for Windows)

Large part of the content is also applicable to the following products:

BEA WebLogic Server® 9.2 (for other platforms)

BEA WebLogic Server® 8.1

Oracle WebLogic Server® 10.3.1

---

---

## 2. Operations in Certificate Enrollment and Obtaining

Obtain an SSL certificate for WebLogic Server by following standard Kousec Certmgr operations. Always specify “**Apache 2**” as the software type to the CA, not WebLogic or a Java application server. Kousec CertMgr will convert the Apache-type certificate and package it in a format suitable for JKS based Server (e.g., WebLogic Server).

Information on the target server of the certificate install can be entered either in Certificate Definition creation time or during the certificate deployment process.

During the certificate definition creation, select “**Java(generic)**” as the server software type. As for the server software options, see “Operations in Certificate Deployment” in the next section.

## 3. Operations in Certificate Deployment

### New Install and Update of SSL Certificates

Two cases will be considered.

A) You are using Demo Identity JKS now. Or, you are using a certificate from a commercial CA now, but with introduction of Kousec CertMgr, you want to change the naming rule of ID keystore file, or the keystore password is lost.

B) You are using a certificate from a commercial CA now and its filename is “server.jks”. You want to keep unchanged the filename of JKS, key alias and keystore password when introducing Kousec CertMgr.

In this document A) is referred to as New Install of certificate and B) is referred to as Update of certificate.

In case A), SSL configuration of the target WebLogic server is necessary.

1. Using the certificate package from CertMgr, newly create an ID keystore (JKS file)
  2. On the target WebLogic server, configure Keystores and SSL
  3. Reboot the target WebLogic server
-

---

In case B), SSL configuration of the target WebLogic server is not necessary.

1. Stop the target WebLogic server
2. Using the certificate package from CertMgr, update the ID keystore (JKS file)
3. Start the target WebLogic server

You must know the key alias, keystore password and key password for the existing JKS file.

In WebLogic Server 9 or later versions, there is no need to reboot the target WebLogic server. You can restart SSL subsystem only. In that case, the procedure is as follows:

1. Using the certificate package from CertMgr, update the ID keystore (JKS file)
2. From the WebLogic Administration Console, select the target server and restart SSL.

### 3.1. (A) Newly Installing the Certificate

#### Preparation on the server computer

We will place the ID keystore in ssl-private directory under WL\_HOME\server. Create the directory ssl-private beforehand.

Start a command prompt and make the directory for server certificates:

```
>cd C:\bea\weblogic92\server  
>mkdir ssl-private
```

#### Operations on CertMgr

We name JKS files with <Common-Name>.jks. If the common name of the certificate to be deployed is www2.example.com, we name it as www2.example.com.jks.

In “Enter Deployment Information” screen, select **JKS(generic)** in the Server Software Type list box. Enter the hostname of the target WebLogic server in the **Server Name** text box.

Enter the following in the **Server Software Options** tab.

JKS File Path: **C:\bea\weblogic92\server\ssl-private\www2.example.com.jks**

---

---

Alias in Keystore: **wlserver** (arbitrary)  
Keystore Password: **changeit** (arbitrary)

Lastly click the Set button.

### **Install the certificate on the server computer**

Unzip the certificate install package (cert.zip) and run jks\_inst.bat in the archive.

```
C:\work\cert\cert>jks_inst.bat
Kousec Certmgr Cert Installer for JKS 0.1.5a
successfully read parameter file
Creating new keyStore file : C:\bea\weblogic92\server\ssl-private\www2.example.com.jks
Certificate chain length: 2
Subject: CN=www2.example.com
Validity Period: 2009/10/08 22:53:39 to 2010/10/08 22:53:39
Intermediate CA Certificates
Subject: CN=Kousec CertMgr Auto-Generated CA 20090715215939
SUCCESS:A new key store with private key and certificate is created.
Alias and key password are set as follows:
    Alias:wlserver Password:changeit
You can change them using one of the commands below:
keytool -keypasswd -alias wlserver -keystore
"C:\bea\weblogic92\server\ssl-private\www2.example.com.jks"
keytool -changealias -alias wlserver -keystore
"C:\bea\weblogic92\server\ssl-private\www2.example.com.jks"
Enter 'y' or 'n' to end this program(y/n)y
Press any key to continue . . .
```

Now, a new ID keystore file, www2.example.com.jks, has been created in the directory C:\bea\weblogic92\server\ssl-private.

---

## Modifying Keystores and SSL Settings on WebLogic Server

Next, configure the WebLogic server to use this ID keystore file.

Here we illustrate the procedure for WebLogic Server 9.2.

- Log in to the Administration Console.
- Go to **Environment > Servers** and select target server, and open the Configuration tab.
- Open the **Configuration - Keystores** tab.
- In the Keystores listbox, Demo Identity and Demo Trust is selected by default. We recommend saving the screenshot of this screen as we are going to change the ID keystore and trust keystore.
- In the Keystores listbox, select Custom Identity and Java Standard Trust, and enter the following:

Custom Identity Keystore: **C:\bea\weblogic92\server\ssl-private\www2.example.com.jks**

Custom Identity Keystore Type: **jks**

Custom Identity Keystore Passphrase: **changeit**

Confirm Custom Identity Keystore Passphrase: **changeit**

Do not modify settings for Java Standard Trust Keystore.

- Click the [Save] button to store the settings.
- Open the Configuration - SSL tab.
- In the v Identity and Trust Locations listbox, make sure that **Keystores** is selected.
- Enter the following:

Private Key Location: **from Custom Identity Keystore** (make sure this value is shown)

Private Key Alias: **wlserver**

Private Key Passphrase: **changeit**

Confirm Private Key Passphrase: **changeit**

Certificate Location: **from Custom Identity Keystore** (make sure this value is shown)

Trusted Certificate Authorities: **from Java Standard Trust Keystore** (make sure this value is shown)

- Click the [Save] button to store the settings.

---

- Finally, by clicking the [Activate Changes], the SSL certificate will be enabled on the target server.

When using WebLogic Server 8.1, the procedure is very similar, except that you must restart the target WebLogic server to put the new ID keystore into effect.

### 3.2. (B) Updating the Certificate

#### Operations on CertMgr

Configure the certificate install package so as to match the ID keystore currently used on the WebLogic server.

#### Example

JKS File Path: C:\bea\weblogic92\server\lib\server.jks

Alias in Keystore: wl\_server

Keystore Password: Something

Lastly click the Set button.

Note: in the current version of Kousec CertMgr, the keystore password and key password must be identical.

#### Procedure for WebLogic Server 9 or Later Versions

- Run the certificate install package on the server computer:

unzip cert.zip and start jks\_inst.bat.

- From the Administration Console, select the target server and restart SSL.

Steps for WebLogic Server 9.2 are listed here.

- Click the **Environment > Servers** node on the left pane and select the target server on the right.
- Click the **Control - Start/Stop** tab
- Go to the **Server Status** table in lower part of the page and select the check box next to the name of the target server.
- Click the **Restart SSL** button.

---

### **Procedure for Versions prior to WebLogic Server 9**

For WebLogic Server products that cannot restart SSL (for example, WebLogic Server 8.1), stop the target WebLogic server while running jks\_inst.bat program.

- Shutdown the target WebLogic server
- Run jks\_inst.bat
- Start the target WebLogic server

---

## 4. Start Managing Existing WebLogic Server Certificate

Even If your SSL certificate on a WebLogic Server instance is not expiring any time soon, it is advisable to bring it under the control of CertMgr. This way, you will obtain benefits of certificate inventorying and monitoring, as well as being able to redeploy the certificate in case the certificate needs to be reinstalled it.

### 4.1. Importing the Existing Keystore File

By importing the ID keystore currently used on a WebLogic Server instance, you can register the certificate, the private key and associated information in the CertMgr repository.

- Copy the ID keystore JKS file from the the filesystem of the WebLogic Server computer to a location where you can access from your web browser.
- Log in to the Kousec CertMgr and click **Import Certificate** on the Certificate Definition screen.
- On the import screen, specify the JKS file as the **Private Key** file. Also specify the password for the keystore in the **Pass Phrase** text box. **Note:** In CertMgr, keystore password and key password must be the same. If they are not, you need to change the keystore password of the JKS file before importing it. You can use 'keytool' command included in JDK.
- In the Add Information screen, you only need to add the following to enable certificate monitoring for now. For other information you can add or modify values later when you actually do certificate renewal or install.
  - Server Software Type: **JKS(generic)**
  - Server name: **<intranet-name-of-the-weblogic-server>**
  - Server Instance: **<any-string>**  
a descriptive text that identifies this WebLogic Server instance on the target server (this information is intended for server administrators)
  - Server Admin's Email: **<email-address-of-the-server-administrator>**
  - Server Name to Check/Monitor: enter the hostname of the WebLogic Server computer via which CertMgr will check the certificate. If omitted, CertMgr will use the common name of the certificate (e.g., www.example.com). If the CertMgr computer is unable to access the WebLogic Server computer through the Internet, you can specify the intra-net name here.
- At the end of the process, answer 'Yes' to the question of whether to start a deployment

---

process.

- In the deployment process,

#### **4.2. Importing Certificate in another Format**

You can also import Apache-style and IIS-style certificate and key files. Use the same import screen to import either a PEM certificate or PKCS#12 (".p12") keystore.

#### **4.3. Daily Operations after the Import**

Once the existing certificate is imported, its validity is checked daily by the CertMgr computer. If no certificate is found on the server or verification of the certificate fails due to some reason, an alert email will be sent to both the CertMgr administrator and the server administrator for the server.

The CertMgr administrator will also start receiving alert emails once the certificate's expiration comes near. Follow instructions from CertMgr when you need to start a certificate renewal process ("acquisition" process in CertMgr terms).

---

## 5. Installing an SSL Server Certificate on Node Manager

When you use WebLogic Server instances for the production environment, it is usually required to install a Node Manager agent on each WebLogic Server computer. Node Manager supports several communication protocols between WebLogic Server instances and Node Manager agents, but SSL is the only one that is both secure and available on all platforms.

### 5.1. Obtaining SSL Certificate for Node Manager

Can the Node Manager agent (“agent”) share the SSL certificate with a WebLogic Server instance (“server”) running on the same machine? If you are exposing the SSL certificate of the server to end users, the certificate is used to represent the service, which should not be tied to a particular computer. For example, a certificate “www.example.com” is probably used to represent the web service.

In such a case, you would need another SSL certificate for the agent that represents the computer itself, not the service. For example, another certificate “wlserver01” should be prepared for the agent.

#### Operations

Follow the standard procedure of certificate acquisition process in CertMgr. For the common name of the certificate, use an internal name (e.g., “wlserver01”). If your CA requires FQDN for the common name, append your domain name appropriately (e.g., “wlserver01.example.com”).

Specify “Apache2” as the server software type to the CA. Specify “JKDS(generic)” as the server software type in CertMgr.

### 5.2. Installing SSL Certificate on to Node Manager

#### Location of JKS File

First decide the location to store the ID keystore file for Node Manager. The following are candidates in case of WebLogic Server 9.2:

C:\bea\weblogic92\common\nodemanager

---

---

C:\bea\weblogic92\server\ssl-private (created to store JKS file for the server instance)

### Creating Certificate Install Package on CertMgr

In the CertMgr deployment process, enter the following in Server Software Type and Server Software Options.

- Server Software Type: **JKS (generic)**
- Server Instance: a descriptive text that identifies this WebLogic Server instance on the target server (this information is intended for server administrators)
- Server Software Options:
  - JKS File Path: **C:\bea\weblogic92\server\ssl-private\wlserver01.jks**
  - Alias in Keystore: **wlserver**
  - Keystore Password: **changeit**

### Configuring ID Keystore for Node Manager

Insert SSL configuration parameters in the Node Manager configuration file, nodemanager.properties, located in:

C:\bea\weblogic92\common\nodemanager\

If this file does not exist, start the Node Manager from the WebLogic start menu once. It will be created. Then, enter the following parameter set.

```
KeyStores=CustomIdentityAndJavaStandardTrust
CustomIdentityKeyStoreFileName=C:\\bea\\weblogic92\\server\\ssl-private\\wlserver01.jks
CustomIdentityAlias=wlserver
CustomIdentityKeyStorePassPhrase=changeit
CustomIdentityPrivateKeyPassPhrase=changeit
```

### 5.3. Configuration on WebLogic Administration Server

Now, the node manager should be running on the server machine. Next step is to

---

---

configure the WebLogic Administration Server so that it can connect to the node manager to carry out administrative tasks.

### **Adding CA Certificate to Standard Java Trust Keystore**

If you obtained the certificate for Node Manager from a private CA or your CA is not recognized by the standard trust keystore in the Java Runtime Environment in which the Administration Server is running, you need to put the CA's certificate into the Java trust keystore. This can be done by using “-import” command of “keytool” utility.

```
> cd C:\bea\jrockit_150_12\jre\lib\security
[Adjust the directory path to suite your WebLogic Server version]
> copy cacerts cacerts.orig
> ..\..\bin\keytool -import -v -alias alias-for-this-CA -keystore cacerts -file CA-cert.crt
[You can specify any string for alias-for-this-CA]
Enter keystore password: changeit
Trust this certificate? [no]: yes
Certificate was added to keystore
[Storing cacerts]
```

### **Configuring Node Manager Information on Administration Console**

Here we illustrate the procedure for WebLogic Server 9.2.

- Log in to the Administration Console.
- Go to **Environment > Machines** and either create a new machine or select an existing machine.
- Open the **Configuration - Node Manager** tab.
- Enter the following:
  - Type: **SSL**
  - Listen Address: Enter the common name of the node manager certificate. In our example, it can be either “**wlserver01**” or “**wlserver01.example.com**”.
  - Listen Port: **5556**

Finally click Save and Activate Changes to make it in effect.

---

---

To make sure that the Administration Server can connect to the node manager, open the **Monitoring** tab. See Status and Problem description to determine if the connection is established.

Likely Errors:

- Certificate chain received from <name> - nn.nn.nn.nn was not trusted causing SSL handshake failure.

This error indicates that you did not correctly import your CA's certificate into the standard trust keystore in your JRE.

- Certificate chain received from <name> - nn.nn.nn.nn failed hostname verification check. Certificate contained <cert-common-name> but check expected <name>.

You specified <name> in the Node Manager configuration on the Administration Console but the common name of node manager's certificate is <cert-common-name>. Make them identical, for example, by changing <name> and adding <name> in etc/hosts file.

- FATAL Alert:BAD\_CERTIFICATE - A corrupt or unuseable certificate was received.

Add `-Dweblogic.security.SSL.allowSmallRSAExponent=true` to `JAVA_OPTIONS` in `setDomainEnv.cmd` (Windows) or `setDomainEnv.sh` (Linux/Unix), located in:

```
c:\bea\weblogic92\samples\domains\wl_server\bin
```

---

## 6. Summary

In this document, we have explained basic procedures for importing the SSL certificate from a WebLogic Server instance into Kousec Server Certificate Manager, and installing SSL certificates into WebLogic Server instance and WebLogic Node Manager instance using the Kousec Server Certificate Manager Certificate Installer program.

If you have a large number of WebLogic Server instances and Node Manager instances, you can also use Certificate Discovery feature in Kousec Server Certificate Manager to inventory all network-exposed SSL certificates in your network and have them imported into the certificate repository, enabling you to jump-start managing your SSL server certificates with Kousec Server Certificate Manager.

For the details, please visit Kousec Software website at <http://www.kousec.com/>.

---