

Oracle Banking Supply Chain Finance

SSL Setup Guide

Release 14.7.0.0.0

Part No. F72110-01

November 2022

Oracle Banking Supply Chain Finance
SSL Setup Guide
November 2022

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/

Copyright © 2020, 2021, 2022 Oracle and/or its affiliates.

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 de-compilation 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.

Table of Contents

1. PREFACE	4
1.1 INTRODUCTION	4
1.2 AUDIENCE.....	4
1.3 DOCUMENT ACCESSIBILITY	4
2. CONFIGURING SSL ON ORACLE WEBLOGIC	5
2.1 SETTING UP SSL ON ORACLE WEBLOGIC.....	5
2.2 CERTIFICATES AND KEYPAIRS	5
3. CHOOSING THE IDENTITY AND TRUST STORES.....	6
4. OBTAINING THE IDENTITY STORE	7
4.1 CREATING IDENTITY STORE WITH SELF-SIGNED CERTIFICATES	7
4.1.1 <i>Creation of Self-Signed Certificate</i>	7
4.2 KEYSTORE CREATION	8
4.3 CREATING IDENTITY STORE WITH TRUSTED CERTIFICATES ISSUED BY CA	9
4.3.1 <i>Creation of Public and Private Key Pair</i>	9
4.3.2 <i>Generating CSR</i>	11
4.4 EXPORT PRIVATE KEY AS CERTIFICATE.....	11
4.4.1 <i>Obtaining Trusted Certificate from CA</i>	11
4.4.2 <i>Importing Certificate into Identity Store</i>	12
4.4.2.1 <i>Importing the Intermediate CA Certificate</i>	12
4.4.2.2 <i>Importing the Identity Certificate</i>	13
4.5 IMPORT AS TRUSTED CERTIFICATE	13
5. CONFIGURING IDENTITY AND TRUST STORES FOR WEBLOGIC	15
5.1 ENABLING SSL ON ORACLE WEBLOGIC SERVER	15
5.2 CONFIGURING IDENTITY AND TRUST STORES	15
6. CONFIGURING WEBLOGIC CONSOLE (12.2.1.4)	17
7. CONFIGURING SSL MODE IN NODE MANAGER FOR CLUSTERED ENVIRONMENT	20
8. SETTING SSL ATTRIBUTES FOR MANAGED SERVERS	21
8.1 SETTING SSL ATTRIBUTES FOR PRIVATE KEY ALIAS AND PASSWORD	21
9. TESTING CONFIGURATION.....	23
9.1 TESTING CONFIGURATION	23

1. Preface

1.1 **Introduction**

This guide provides information about the configurations of SSL for Oracle Weblogic application server.

1.2 **Audience**

This guide is intended for WebLogic admin or ops-web team who are responsible for installing the Oracle Financial Services Software (OFSS) banking products.

1.3 **Document Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>

2. Configuring SSL on Oracle Weblogic

This chapter provides information about the configurations for SSL on Oracle Weblogic application server.

2.1 Setting up SSL on Oracle Weblogic

To setup SSL on Oracle Weblogic application server:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for Oracle Weblogic application server
2. Store the identity and trust. Private keys and trust CA certificates are stored in keystores
3. Configure the identity and trust the keystores for Oracle Weblogic application server in the administration console
4. Set SSL attributes for the private key alias and password in Oracle Weblogic administration console.

2.2 Certificates and Keypairs

Certificates are used for validating the authenticity of the server. Certificates contains the name of the owner, certificate usage, duration of validity, resource location or distinguished name (DN), which includes the common name (CN - web site address or e-mail address depending of the usage) and the certificate ID of the person who certified (signs) these information. It also contains the public key and a hash to ensure that the certificate has not been tampered with. A certificate is insecure until it is signed. Signed certificates cannot be modified.

A certificate can be self-signed or obtained from a reputable certificate authority such as Verisign, Inc., Entrust.net, Thawte, GeoTrust or InstantSSL.

SSL uses a pair of cryptographic keys - a **public key** and a **private key**. These keys are similar in nature and can be used alternatively. What one key encrypts can be decrypted by the other key of the pair. The private key is kept secret, while the public key is distributed using the certificate.

A **keytool** stores the keys and certificates in a **keystore**. The default keystore implementation implements it as a file. It protects private keys with a password. The different entities (key pairs and the certificates) are distinguished by a unique 'alias'. Through its keystore, Oracle Weblogic server can authenticate itself to other parties.

In Java, a keystore is a 'java.security.KeyStore' instance that you can create and manipulate using the **keytool** utility provided with the Java Runtime.

There are two keystores to be managed by Oracle Weblogic server to configure SSL:

1. Identity Keystore: Contains the key pairs and the Digital certificate. This can also contain certificates of intermediate CAs.
2. Trust Keystore: Contains the trusted CA certificates.

3. Choosing the Identity and Trust Stores

Oracle Financial Services Software recommends that the choice of Identity and Trust stores be made up front. Oracle Weblogic server supports the following combinations of Identity and Trust stores:

- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust
- Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

Oracle Financial Services does not recommend choosing Demo Identity and Demo Trust for production environments.

It is recommended to separate the identity and trust stores, since each Weblogic server tends to have its own identity, but might have the same set of trust CA certificates. Trust stores are usually copied across Oracle Weblogic servers, to standardize trust rules; it is acceptable to copy trust stores since they contain public keys and certificates of CAs. Unlike trust stores, identity stores contain private keys of the Oracle Weblogic server, and hence should be protected against unauthorized access.

Command Line Trust, if chosen requires the trust store to be specified as a command line argument in the Weblogic Server startup script. No additional configuration of the trust store is required in the Weblogic Server Administration Console.

Java Standard Trust would rely on the cacerts files provided by the Java Runtime. This file contains the list of trust CA certificates that ship with the Java Runtime, and is located in the

'JAVA_HOME/jre/lib/security' directory. It is highly recommended to change the default Java standard trust store password from 'changeit' (without quotes), and the default access permission of the file. Certificates of most commercial CAs are already present in the Java Standard Trust store. Therefore, it is recommended to use the Java Standard Trust store whenever possible. The rest of the document will assume the use of Java Standard Trust, since most CA certificates are already present in it.

One can also create custom trust stores containing the list of certificates of trusted CAs. For further details on identity and trust stores, please refer the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server.

4. Obtaining the Identity Store

4.1 Creating Identity Store with Self-Signed Certificates

Self-signed certificates are acceptable for use in a testing or development environment. Oracle Financial Services does not recommend the use of self-signed certificates in a production environment.

In order to create a self-signed certificate, the `genkeypair` option provided by the `keytool` utility of Sun Java 8 needs to be utilized.

4.1.1 Creation of Self-Signed Certificate

Browse to the `bin` folder of JRE from the command prompt and type the following command.

The items highlighted in blue are placeholders, and should be replaced with suitable values when running the command.

```
keytool -genkeypair -alias alias -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 365 -keystore keystore
```

In the above command,

1. **alias** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
2. **keystore** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

1. **Keystore Password:** Specify a password that will be used to access the keystore. This password needs to be specified later, when configuring the identity store in Oracle Weblogic Server.
2. **Key Password:** Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later, when configuring the SSL attributes of the managed server(s) in Oracle Weblogic Server.
3. **First and Last Name (CN):** Enter the domain name of the machine used to access OBSCF, for instance, `www.example.com`
4. **Name of your Organizational Unit:** The name of the department or unit making the request, for example, BPD. Use this field to further identify the SSL Certificate you are creating, for example, by department or by physical server.
5. **Name of your Organization:** The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.
6. **Name of your City or Locality:** The city in which your organization is physically located, for example Mumbai.
7. **Name of your State or Province:** The state/province in which your organization is physically located, for example Maharashtra.

8. **Two-Letter Country Code for this Unit:** The country in which your organization is physically located, for example US, UK, IN etc.

The key generation algorithm has been specified as RSA, the key size as 1024 bits, the signature algorithm as SHA1withRSA, and the validity days as 365. These can be changed to suitable values if the need arises. For further details, please refer to the documentation of the keytool utility in the JDK utilized by Oracle Weblogic Server.

Example

Listed below is the result of a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -
genkeypair -alias selfcert -keyalg RSA -keysize 1024 -sigalg
SHA1withRSA -validity 365 -keystore
D:\keystores\AdminOBSCFKeyStore.jks

Enter keystore password: <Enter a password to protect the keystore>

Re-enter new password: <Confirm the password keyed above>

What is your first and last name?
[Unknown]: cvrhp0729.oracle.com

What is the name of your organizational unit?
[Unknown]: BPD

What is the name of your organization?
[Unknown]: Oracle Financial Services

What is the name of your City or Locality?
[Unknown]: Mumbai

What is the name of your State or Province?
[Unknown]: Maharashtra

What is the two-letter country code for this unit?
[Unknown]: IN

Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services,
L=Mumbai, ST=Maharashtra, C=IN correct? [no]: yes

Enter key password for <selfcert>

RETURN if same as keystore password): <Enter a password to protect
the key>

Re-enter new password: <Confirm the password keyed above>
```

4.2 Keystore Creation

keytool -genkeypair -keystore <keystore_name.jks> -alias <alias_name> -dname
"CN=<hostname>, OU=<Organization Unit>, O=<Organization>, L=<Location>, ST=<State>,
C=<Country_Code>" -keyalg <Key Algorithm> -sigalg <Signature Algorithm> -keysize <key

size> -validity <Number of Days> -keypass <Private key Password> -storepass <Store Password>

For example:

```
keytool -genkeypair -keystore AdminOBSCFKeyStore.jks -alias OBSCFCert -dname
"CN=ofss00001.in.oracle.com, OU=OFSS, O=OFSS, L=Chennai, ST=TN, C=IN" -keyalg "RSA"
-sigalg "SHA1withRSA" -keysize 2048 -validity 3650 -keypass Password@123 -storepass
Password@123
```

Note: CN=ofss00001.in.oracle.com is the Host Name of the weblogic server

4.3 Creating Identity Store with Trusted Certificates Issued by CA

4.3.1 Creation of Public and Private Key Pair

Browse to the bin folder of JRE from the command prompt and type the following command.

The items highlighted in blue are placeholders, and should be replaced with suitable values when running the command.

```
keytool -genkeypair -alias alias -keyalg keyalg -keysize keysize -
sigalg sigalg -validity valDays -keystore keystore
```

In the above command,

1. The **alias** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
2. The **keyalg** is the key algorithm used to generate the public and private key pair. The RSA key algorithm is recommended.
3. The **keysize** is the size of the public and private key pairs generated. A key size of 1024 or more is recommended. Please consult with your CA on the key size support for different types of certificates.
4. The **sigalg** is the algorithm used to generate the signature. This algorithm should be compatible with the key algorithm and should be one of the values specified in the Java Cryptography API Specification and Reference.
5. The **valdays** is the number of days for which the certificate is to be considered valid. Please consult with your CA on this period.
6. The **keystore** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

1. **Keystore Password:** Specify a password that will be used to access the keystore. This password needs to be specified later, when configuring the identity store in Oracle Weblogic Server.
2. **Key Password:** Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later, when configuring the SSL attributes of the managed server(s) in Oracle Weblogic Server.

3. **First and Last Name (CN):** Enter the domain name of the machine used to access OBSCF, for instance, www.example.com
4. **Name of your Organizational Unit:** The name of the department or unit making the request, for example, BPD. Use this field to further identify the SSL Certificate you are creating, for example, by department or by physical server.
5. **Name of your Organization:** The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.
6. **Name of your City or Locality:** The city in which your organization is physically located, for example Mumbai.
7. **Name of your State or Province:** The state/province in which your organization is physically located, for example Maharashtra.
8. **Two-letter Country Code for this Unit:** The country in which your organization is physically located, for example US, UK, IN etc.

Example: Listed below is the result of a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -
genkeypair -alias cvrhp0729 -keyalg RSA -keysize 1024 -sigalg
SHA1withRSA -validity 365 -keystore
D:\keystores\AdminOBSCFKeyStore.jks
```

Enter keystore password: *<Enter a password to protect the keystore>*

Re-enter new password: *<Confirm the password keyed above>*

What is your first and last name?
[Unknown]: cvrhp0729.i-flex.com

What is the name of your organizational unit?
[Unknown]: BPD

What is the name of your organization?
[Unknown]: Oracle Financial Services

What is the name of your City or Locality?
[Unknown]: Mumbai

What is the name of your State or Province?
[Unknown]: Maharashtra

What is the two-letter country code for this unit?
[Unknown]: IN

Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services,
L=Mumbai, ST=Maharashtra, C=IN correct? [no]: yes Enter key
password for <cvrhp0729>

RETURN if same as keystore password): *<Enter a password to protect
the key>*

Re-enter new password: *<Confirm the password keyed above>*

4.3.2 **Generating CSR**

To purchase an SSL certificate, you must generate a Certificate Signing Request (CSR) for the server where the certificate will be installed.

A CSR is generated from the server and is the server's unique "fingerprint". The CSR includes the server's public key, which enables server authentication and secure communication.

If the keystore file or the password is lost and a new one is generated, the SSL certificate and the private key will no longer match. A new SSL Certificate will have to be requested.

The CSR is created by running the following command in the bin directory of the JRE:

```
keytool -certreq -alias alias -file certreq_file -keystore keystore
```

In the above command,

1. The alias is used to identify the public and private key pair. The private key associated with the alias will be utilized to create the CSR. Specify the alias of the key pair created in the previous step.
2. The certreq_file is the file in which the CSR will be stored.
3. The keystore is the location of the keystore containing the public and private key pair.

Example: Listed below is the result of a sample execution of the command:

```
D:\Oracle\Weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
certreq -alias cvrhp0729 -file D:\keystores\certreq.csr -keystore
```

```
D:\keystores\AdminOBSCFKeyStore.jks
```

```
Enter keystore password: [Enter the password used to access the  
keystore]
```

```
Enter key password for <cvrhp0729> [Enter the password used to  
access the key in the keystore]
```

4.4 **Export Private Key as Certificate**

```
keytool -export -v -alias <alias_name> -file <export_certificate_file_name_with_location.cer> -  
keystore <keystore_name.jks> > -keypass <Private key Password> -storepass <Store  
Password>
```

For example:

```
keytool -export -v -alias OBSCFCert -file AdminOBSCFCert.cer -keystore  
AdminOBSCFKeyStore.jks -keypass Oracle123 -storepass Oracle123
```

If successful, the following message will be displayed:

Certificate stored in file < AdminOBSCFCert.cer>

4.4.1 **Obtaining Trusted Certificate from CA**

The processes of obtaining a trusted certificate vary from one CA to another. The CA might perform additional offline verification. Consult the CA issuing the certificate for details on the process to be followed for submission of the CSR and for obtaining the certificate.

4.4.2 **Importing Certificate into Identity Store**

Store the certificate obtained from the CA in the previous step, in a file, preferably in PEM format. Other formats like the p7b file format would require conversion to the PEM format. Details on performing the conversion are not listed here. Please refer to the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server, for details on converting a Microsoft p7b file to the PEM format.

The command to be executed for importing a certificate into the identity store depend on whether the trust store chosen (in the earlier step; see section 2 of this document). It is highly recommended to verify the trust path when importing a certificate into the identity store. The commands provided below assume the use of the Java Standard Trust store.

4.4.2.1 **Importing the Intermediate CA Certificate**

Most Certificate Authorities do not use the root CA certificates to issue identity certificates for use by customers. Instead, Intermediate CAs issue identity certificates in response to the submitted CSRs.

If the Intermediate CA certificate is absent in the Java Standard Trust store, the trust path for the certificate will be incomplete for the certificate, resulting in warnings issued by Weblogic Server during runtime. To avoid this, the intermediate CA certificate should be imported into the identity keystore. Although the intermediate CA certificate can be imported into the Java Standard Trust store, this is not recommended unless the intermediate CA can be trusted.

The following command must be executed to import the intermediate CA certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file -trustcacerts -  
keystore keystore
```

In the above command,

1. The *alias* is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.
2. The *cert_file* is the location of the file containing the intermediate CA certificate in a PKCS#7 format (PEM or DER file).
3. The *keystore* is the location of the keystore containing the public and private key pair.

The trustcacerts flag is used to consider other certificates (higher intermediaries and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed, when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
importcert -alias verisigntrialintermediateca -file  
D:\keystores\VerisignIntermediateCA.cer -trustcacerts - keystore  
D:\keystoreworkarea\AdminOBSCFKeyStore.jks
```

Enter keystore password: <Enter the password used to access the keystore>

Certificate was added to keystore

4.4.2.2 **Importing the Identity Certificate**

The following command should be executed to import the identity certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file - trustcacerts -  
keystore  
  
keystore
```

In the above command:

1. The alias is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.
2. The cert_file is the location of the file containing the PKCS#7 formatted reply from the CA, containing the signed certificate.
3. The keystore is the location of the keystore containing the public and private key pair.

The trustcacerts flag is used to consider other certificates (intermediate CAs and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed, when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command

```
D:\Oracle\weblogic11g\jrocket_160_05_R27.6.2-20\bin>keytool -  
importcert -alias cvrhp0729 -file D:\keystores\cvrhp0729.cer -  
trustcacerts -keystore  
  
D:\keystoreworkarea\AdminOBSCFKeyStore.jks  
  
Enter keystore password: <Enter the password used to access the  
keystore>  
  
Enter key password for <cvrhp0729>: <Enter the password used to  
access the private key>  
  
Certificate reply was installed in keystore
```

The previous set of commands assumed the presence of the appropriate root CA certificate (in the chain of trust) in the Java Standard Trust store, i.e. in the cacerts file. If the CA issuing the identity certificate (for the Weblogic Server) does not have the root CA certificate in the Java Standard Trust store, one can opt to import the root CA certificate into cacerts, or into the identity store, depending on factors including trustworthiness of the CA, necessity of transporting the trust store across machine, among others.

4.5 **Import as Trusted Certificate**

```
keytool -import -v -trustcacerts -alias rootcacert -file
```

```
<export_certificate_file_name_with_location.cer> -keystore <keystore_name.jks> > -keypass  
<Private key Password> -storepass <Store Password>
```

For example:

```
keytool -import -v -trustcacerts -alias rootcacert -file  
AdminOBSCFCert.cer -keystore AdminOBSCFKeyStore.jks -keypass  
Oracle123 -storepass Oracle123
```

5. Configuring Identity and Trust Stores for Weblogic

5.1 Enabling SSL on Oracle Weblogic Server

To configure SSL on Oracle Weblogic server, login in to the Admin Console:

1. Under **Change Center**, click **Lock & Edit**.
2. Expand **Servers** node.
3. Select the name of the server for which you want to enable SSL. Example: exampleserver
4. Go to **Configuration** and select **General** tab.
5. Select the option **SSL Listen Port Enabled** and specify the SSL listen port.
6. Against **Listen Address**, specify the hostname of the machine in which the application server is installed.

5.2 Configuring Identity and Trust Stores

To configure the Identity and Trust stores in Oracle Weblogic Server, log in to the Admin Console of Weblogic Server.

1. Under **Change Center**, click **Lock & Edit**.
2. Expand **Servers** node.
3. Select the name of the server for which you want to configure the keystores (example - exampleserver).
4. Go to **Configuration** and select **Keystores** tab.
5. In the filed **Keystores**, select the method for storing and managing private keys/digital certificate pairs and trusted CA certificates. This choice should match the one made in Section 2 of this document (Choosing the Identity and Trust Stores).
6. In the **Identity** section, provide the following details:
 - **Custom Identity Keystore File Name:** Fully qualified path to the Identity keystore.
 - **Custom Identity Keystore Type:** Set this attribute to JKS, the type of the keystore. If left blank, it is defaulted to JKS (Java KeyStore).
 - **Custom Identity Keystore PassPhrase:** The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic server only reads from the keystore. So whether or not you define this property depends on the requirements of the keystore.
7. In the **Trust** section, provide the following details:

If you choose **Java Standard Trust**, specify the password used to access the trust store.

If you choose **Custom Trust**, the following attributes have to be provided:

 - **Custom Trust Keystore:** The fully qualified path to the trust keystore.
 - **Custom Trust Keystore Type:** Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).

- Custom Trust Keystore Passphrase: The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic

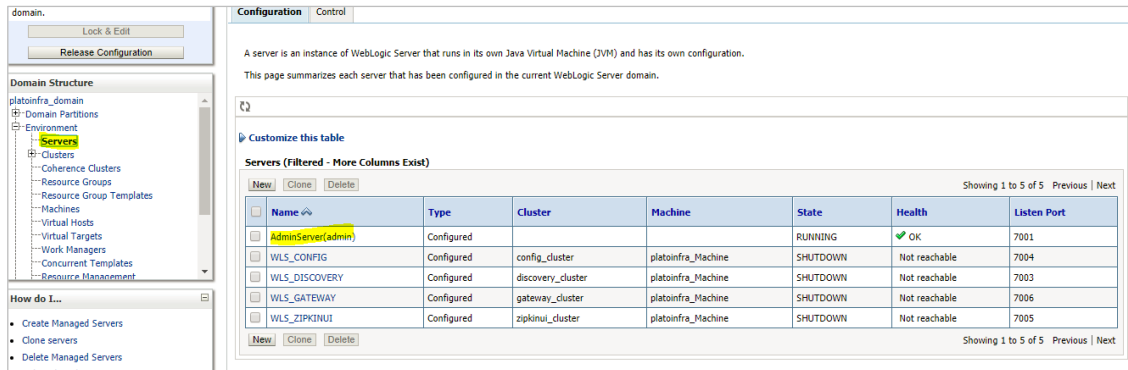
Server only reads from the keystore. So, whether or not you define this property depends on the requirements of the keystore.

When identity and trust stores are of the JKS format, the passphrases are not required

6. Configuring Weblogic Console (12.2.1.4)

After domain creation, follow the below steps to enable SSL in weblogic Admin server.

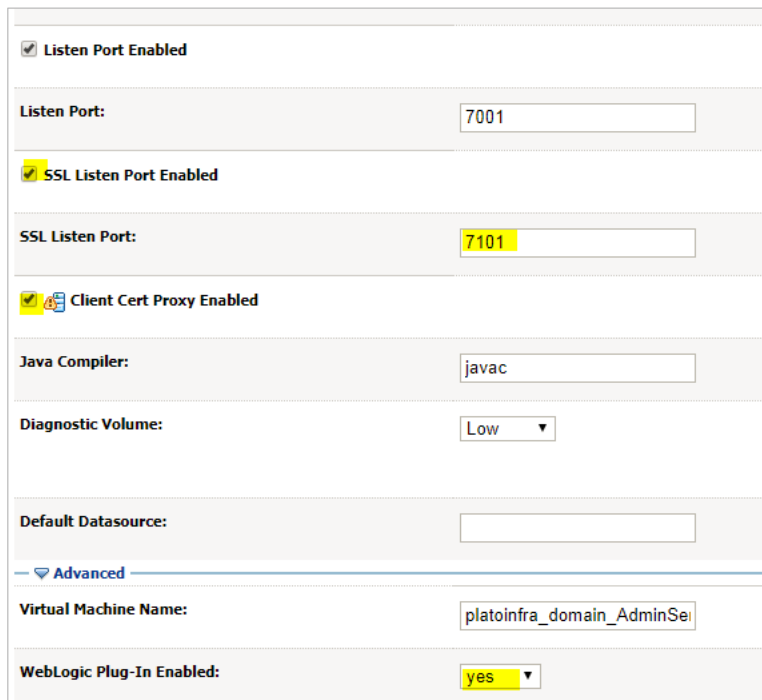
1. Select Admin Server to Enable SSL Options.



The screenshot shows the WebLogic Console Configuration page. On the left, the Domain Structure tree is visible, with 'Servers' selected under 'Environment'. The main area displays the 'Servers (Filtered - More Columns Exist)' table. The table has columns: Name, Type, Cluster, Machine, State, Health, and Listen Port. The 'AdminServer(admin)' is highlighted in yellow, showing it is 'Configured', in the 'config_cluster', on 'platoinfra_Machine', in 'RUNNING' state, with 'OK' health, and listening on port 7001. Other servers listed include WLS_CONFIG, WLS_DISCOVERY, WLS_GATEWAY, and WLS_ZIPKINUI, all in 'SHUTDOWN' state with 'Not reachable' health.

Name	Type	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)	Configured	config_cluster	platoinfra_Machine	RUNNING	OK	7001
WLS_CONFIG	Configured	config_cluster	platoinfra_Machine	SHUTDOWN	Not reachable	7004
WLS_DISCOVERY	Configured	discovery_cluster	platoinfra_Machine	SHUTDOWN	Not reachable	7003
WLS_GATEWAY	Configured	gateway_cluster	platoinfra_Machine	SHUTDOWN	Not reachable	7006
WLS_ZIPKINUI	Configured	zipkinui_cluster	platoinfra_Machine	SHUTDOWN	Not reachable	7005

2. Click **General** tab.
3. Select **SSL Listen Port Enabled**, **Client Cert Proxy Enabled**, **Weblogic Plug-In Enabled**. 4. Click **Save**.



The screenshot shows the 'General' tab configuration page. It contains several settings:

- ☒ **Listen Port Enabled**
- Listen Port:** 7001
- ☒ **SSL Listen Port Enabled**
- SSL Listen Port:** 7101
- ☒ **Client Cert Proxy Enabled**
- Java Compiler:** javac
- Diagnostic Volume:** Low
- Default Datasource:** (empty)
- Advanced** (expanded)
- Virtual Machine Name:** platoinfra_domain_AdminSei
- WebLogic Plug-In Enabled:** yes

✔ Settings updated successfully.

Settings for AdminServer

Configuration Protocols Logging Debug Monitoring Control Deployments Services

General Cluster Services **Keystores** SSL Federation Services Deployment Migration

Save

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

Keystores: Custom Identity and Custom Trust [Change](#)

Identity

Custom Identity Keystore: C:\AdminOBLMKeyStore.jks

Custom Identity Keystore Type: jks

Custom Identity Keystore Passphrase:

Confirm Custom Identity Keystore Passphrase:

Trust

Custom Trust Keystore: C:\AdminOBLMKeyStore.jks

Custom Trust Keystore Type: jks

Custom Trust Keystore Passphrase:

Confirm Custom Trust Keystore Passphrase:

4. Click **Keystores** tab.
5. Enter Custom Identity Keystore and Custom Trust Keystore same as the Keystore Name created in above steps with full path.
6. Enter Custom Identity Keystore Type and Custom Trust Keystore Type as jks.
7. Enter Custom Identity Keystore Passphrase, Confirm Custom Identity Keystore Passphrase, Custom Trust Keystore Passphrase and Confirm Custom Trust Keystore Passphrase same as the Store Password entered in above steps.
8. Click **Save**.
9. Click **SSL** tab.
10. Enter Private Key Alias as same as the alias name entered in above steps.

11. Enter Private Key Passphrase and Confirm Private Key Passphrase as same as the Private Key Password entered in above steps.
12. Change the Hostname Verification to None.
13. Click **Save**.

The screenshot shows the 'SSL' tab in the Oracle WebLogic Server Administration Console. The top navigation bar includes 'General', 'Cluster', 'Services', 'Keystores', 'SSL' (selected), 'Federation Services', 'Deployment', 'Migration', and 'Tuning'. Below the navigation bar is a 'Save' button. A descriptive text states: 'This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings are used by the server to establish secure connections with clients and other servers.' The main configuration area is divided into three sections: 'Identity and Trust Locations', 'Identity', and 'Trust'. The 'Identity and Trust Locations' section has a 'Keystores' label and a 'Change' button. The 'Identity' section includes: 'Private Key Location' (from Custom Identity Keystore), 'Private Key Alias' (OBLMCert), 'Private Key Passphrase' (masked with dots), and 'Confirm Private Key Passphrase' (masked with dots). The 'Trust' section includes 'Certificate Location' (from Custom Identity Keystore) and 'Trusted Certificate Authorities' (from Custom Trust Keystore). At the bottom, there is an 'Advanced' section with a right-pointing arrow.

Repeat the same steps for all the managed servers as well. The admin server and managed servers are SSL enabled. Restart all the servers.

7. Configuring SSL Mode in Node Manager for Clustered Environment

1. Edit the nodemanager.properties with SSL configurations and restart the node manager

```
PropertiesVersion=12.2.1.3.0
AuthenticationEnabled=true
NodeManagerHome=D:\Oracle\Middleware\12cPs3\Oracle_home_new\user_projects\domains\platoinfra_domain\nodemanager
JavaHome=C:\Program Files\Java\jdk1.8.0_1
LogLevel=INFO
DomainsFileEnabled=true
ListenAddress=localhost
NativeVersionEnabled=true
ListenPort=5556
LogToStderr=true
weblogic.StartScriptName=startWebLogic.cmd

SecureListener=true
ListenPort=5557
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeystoreType=jks
CustomIdentityKeystoreFileName=C:\AdminOBIMKeyStore.jks
CustomIdentityKeystorePassPhrase=Oracle123
CustomIdentityPrivateKeyPassPhrase=Oracle123
CustomIdentityAlias=OBIMCert
CustomTrustKeystoreType=jks
CustomTrustKeystoreFileName=C:\AdminOBIMKeyStore.jks
CustomTrustKeystorePassPhrase=Oracle123

LogCount=1
QuitEnabled=false
LogAppend=true
weblogic.StopScriptEnabled=false
StateCheckInterval=500
CrashRecoveryEnabled=false
weblogic.StartScriptEnabled=true
LogFile=D:\Oracle\Middleware\12cPs3\Oracle_home_new\user_projects\domains\platoinfra_domain\nodemanager\nodemanager.log
LogFormatter=weblogic.nodemanager.server.LogFormatter
ListenBacklog=50
```

2. Ensure the SSL configuration is performed in other artifacts, such as startNodeManager.cmd/.sh, startup.properties, config.xml(enable jsse).

8. Setting SSL Attributes for Managed Servers


8.1 Setting SSL Attributes for Private Key Alias and Password

To configure the private key alias and password, log in to the Oracle Weblogic Server Admin Console.

1. Under **Change Center**, click **Lock & Edit**.
2. Expand **Servers** node.
3. Select the name of the server for which you want to configure keystores. Example: exampleserver
4. Go to **Configuration** and select **SSL** tab.
5. Select Keystores from **Identity and Trust Locations**.
6. Under Identity section, specify the following details:
 - **Private Key Alias**: set this attribute to the alias name defined for the key pair when creating the key pair in the Identity keystore.
 - **Private Key Passphrase**: The password defined for the key pair (alias_password), at the time of its creation. . Confirm the password.
7. Click **Save**.
8. Under **Change Center**, click **Activate changes**.
9. Go to **controls** tab, check the appropriate server and click **Restart SSL**. Confirm when it prompts.

The screenshot displays the Oracle Weblogic Server Admin Console interface. On the left, the 'Domain Structure' tree is visible, with 'Environment' expanded and 'Machines' selected. Below it, a 'How do I...' section provides links for creating and configuring machines, monitoring Node Manager status, and monitoring Node Manager logs. The main panel shows the 'Settings for platoinfra_Machine' configuration page. The 'Configuration' tab is active, and the 'Node Manager' sub-tab is selected. A 'Save' button is at the top left of the configuration area. The page contains descriptive text about Node Manager configuration and several input fields: 'Type' is set to 'SSL', 'Listen Address' is a text field, 'Listen Port' is set to '5557', 'Node Manager Home' is a text field, and 'Shell Command' is a text field.

ake effect.

 **Activate Changes**

Undo All Changes

Main Structure

- infra_domain
- Domain Partitions
- Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Resource Groups
 - Resource Group Templates
 - Machines


Configuration | Monitoring | Notes

General | **Node Manager** | Servers

Save

This page allows you to define the Node Manager configuration for this managed domain. Managed Servers are installed.

The settings defined on this page are used to configure communication between the Node Manager instances.

 **Type:** SSL ▼

Click the **Lock & Edit** button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Main Structure

- infra_domain
- Domain Partitions
- Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Resource Groups
 - Resource Group Templates
 - Machines
 - Virtual Hosts
 - Virtual Targets
 - Work Managers
 - Concurrent Templates
 - Resource Management

What do I...?

- Start and stop servers
- Start Managed Servers from the Administration Console
- Restart SSL

Summary of Servers

Configuration | **Control**

Use this page to change the state of the servers in this WebLogic Server domain. Control operations on Managed Servers require starting the Node Manager. Starting Managed Servers in Standby mode requires the domain-wide administration port.



Customize this table

Servers (Filtered - More Columns Exist)

Start Resume Suspend ▼ Shutdown ▼ Restart SSL Showing 1 to 5 of 5 Previous Next

Server	Machine	State	Status of Last Action
<input checked="" type="checkbox"/> AdminServer(admin)		RUNNING	None
<input checked="" type="checkbox"/> WLS_CONFIG	platoinfra_Machine	SHUTDOWN	None
<input checked="" type="checkbox"/> WLS_DISCOVERY	platoinfra_Machine	SHUTDOWN	None
<input checked="" type="checkbox"/> WLS_GATEWAY	platoinfra_Machine	SHUTDOWN	None
<input checked="" type="checkbox"/> WLS_ZIPKINUI	platoinfra_Machine	SHUTDOWN	None

Start Resume Suspend ▼ Shutdown ▼ Restart SSL Showing 1 to 5 of 5 Previous Next

9. Testing Configuration

9.1 Testing Configuration

Once the Oracle Weblogic has been configured for SSL, deploy the application in the usual manner. After deployment, you can test the application in SSL mode. To launch the application in SSL mode you need to enter the URL in the following format:

https://(Machine Name):(SSL_Listener_port_no)/(Context_root)

It is recommended that the Oracle Banking Virtual Account Management web application be accessed via the HTTPS channel, instead of the HTTP channel.
