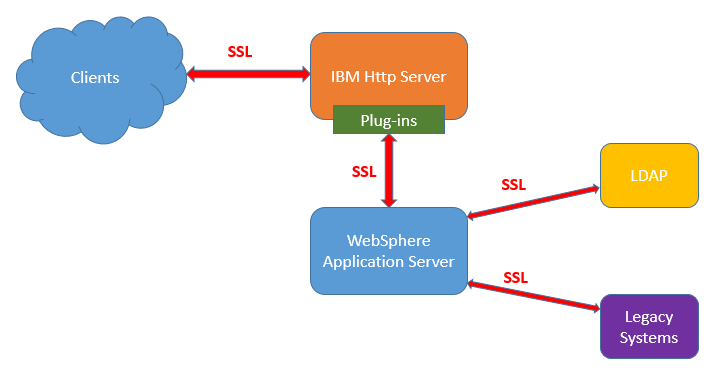
# CHAPTER 18: SSL

## Theory

WebSphere Application Server communicates with other components of a middleware environment and in order to prevent intrusions, WebSphere uses Java Secure Socket Extension (JSSE) which is an SSL implementation. SSL capabilities such as handshaking are delivered by JSSE using X.509 standard public key infrastructure (PKI).

PKI contains hardware, software, people and policies to handle whole lifecycle of digital certificates including activities like create, manage, store and renew. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository and revokes them if needed. Certificate Authority (CA) digitally sign and publish the public key bound to a given user. This is done using the CA's own private key, so that trust in the user key relies on one's trust in the validity of the CA's key.

SSL is a protocol which is designed to provide secure communication over networks. It uses certificates to authenticate the service provider by exchanging keys between server and client. WebSphere Application Server store these certificates in password protected files, in keystores. WebSphere allows you to work with certificates using administrative console where you can create and manage keystores.



WebSphere Application Server can use SSL in the cell between the nodes. The certificate required for this secure communication is created during profile creation. This certificate contains a signer certificate and a personal certificate created by embedded CA. You can also use your own certificate for this purpose.

Another important aspect of secure communication is between WebSphere Application Server and web server. For this purpose, plug-in uses only one keyring file. WebSphere allows you to create your personal keys and add them to the keyring files to be delivered to the web server.

It is also possible to secure the communication between external systems that WebSphere Application Server transmits sensitive information. Following systems worth to be considered to use SSL secured communication:

* Database connection
* LDAP connection
* Message channels (i.e. WebSphere MQ connection)
* Web services connections

## AIM

In this lab exercise, you will perform common SSL operations. When you finish this lab, you will be able to create a keystore and a personal certificate and configure it to use in communication between WebSphere Application Server and the web server. In order to achieve this goal, you need to complete following tasks:

* Create a keystore
* Create a self-signed certificate
* Configure plug-in to use new certificate

# Lab Exercise 18: SSL

|  |
| --- |
| Create Keystore  Create Certificate  Configure Plugin |

## Create a keystore

## Create a self-signed certificate

## Configure plug-in to use new certificate

Create Keystore

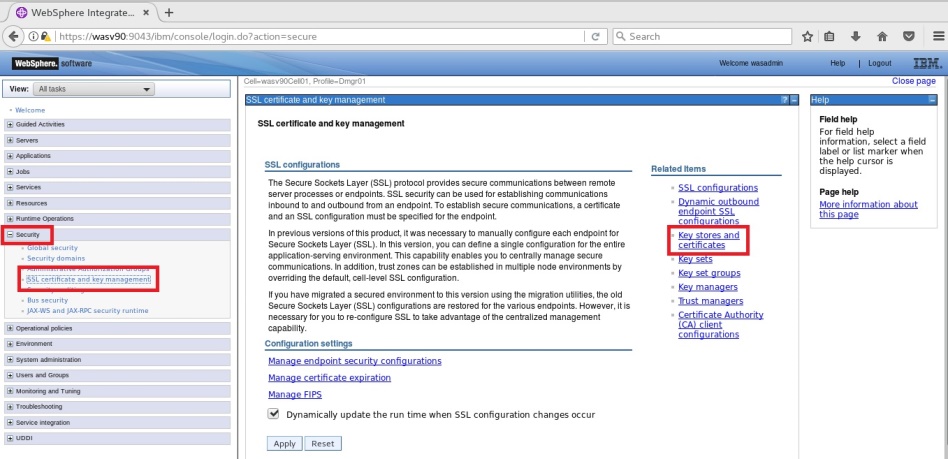
Create Certificate

Configure Plugin



**Task 1: Create a keystore**

**Step 1:** Navigate to “Security>SSL certificate and key management” and click “Key stores and certificates”.



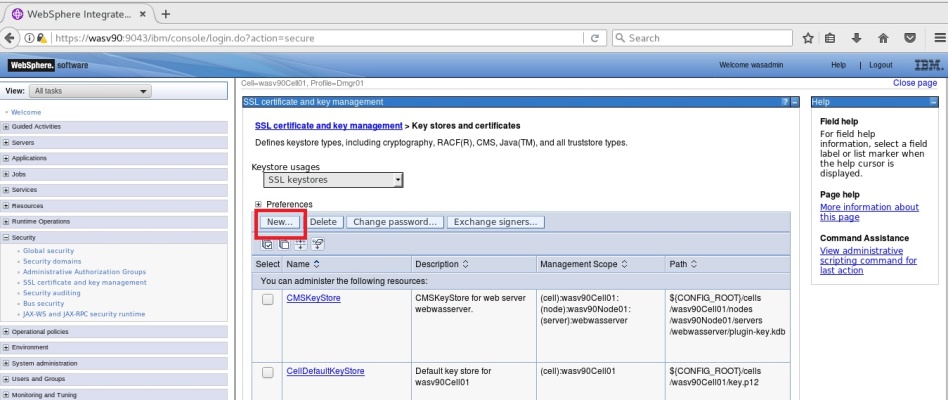
Create Keystore

Create Certificate

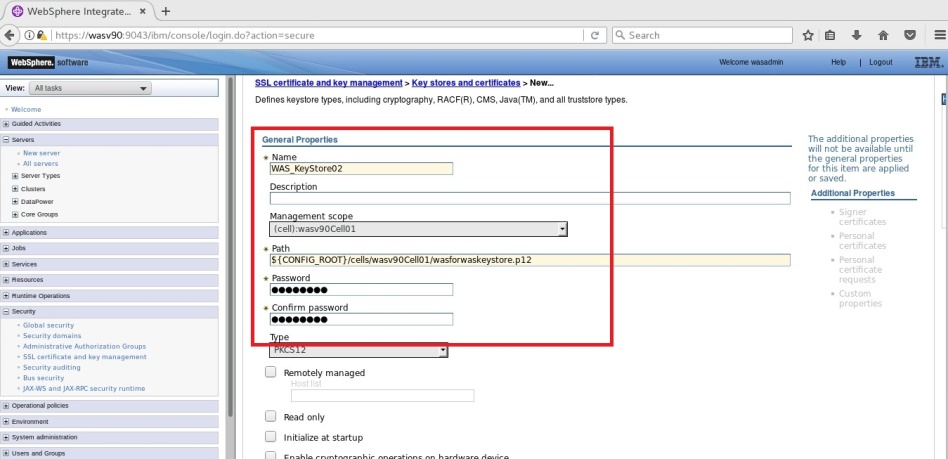
Configure Plugin



**Step 2:** Click “New”.



**Step 3:** Enter the properties of the new keystore similar to following picture.



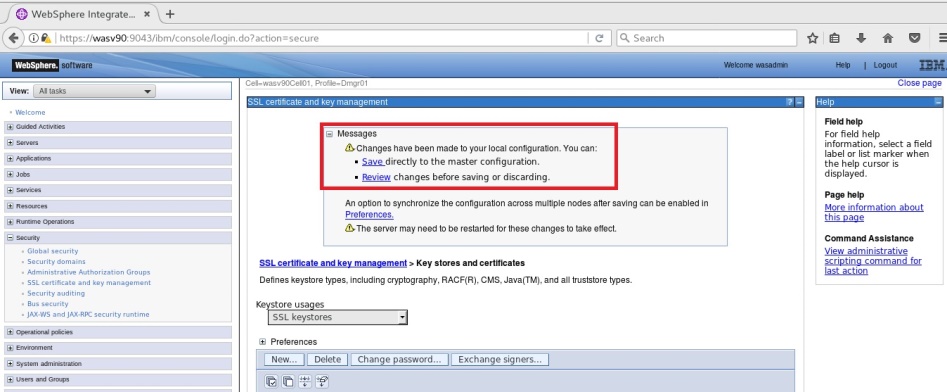
Create Keystore

Create Certificate

Configure Plugin



**Step 4:** Click “Save” to write changes to the master configuration file.

****

**Task 1 is complete!**

Create Keystore

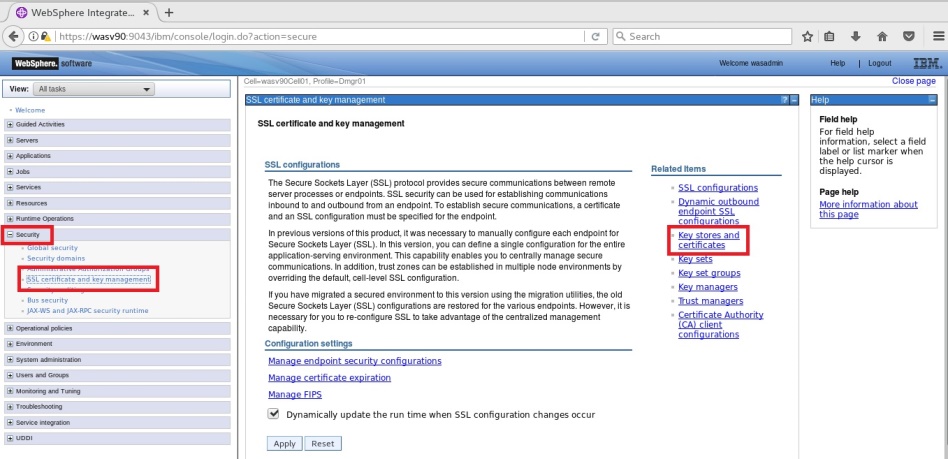
Create Certificate

Configure Plugin



**Task 2: Create a self-signed certificate**

**Step 1:** Navigate to “Security>SSL certificate and key management” and click “Key stores and certificates”.



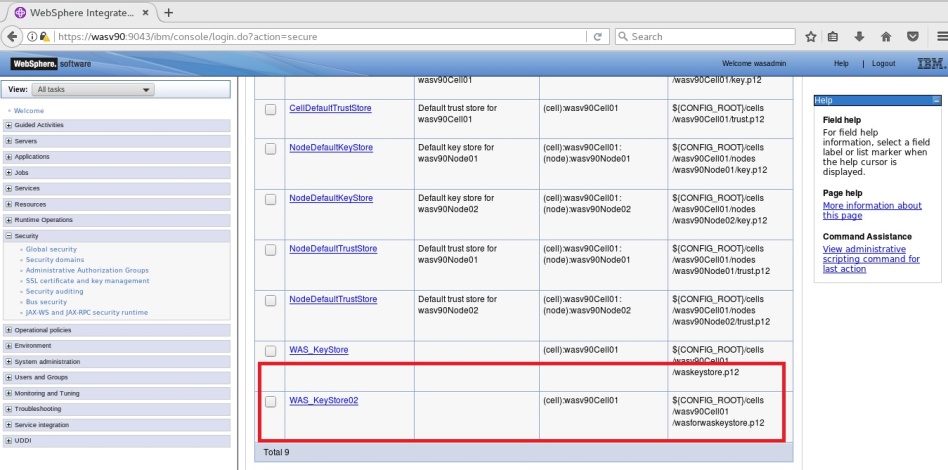
Create Keystore

Create Certificate

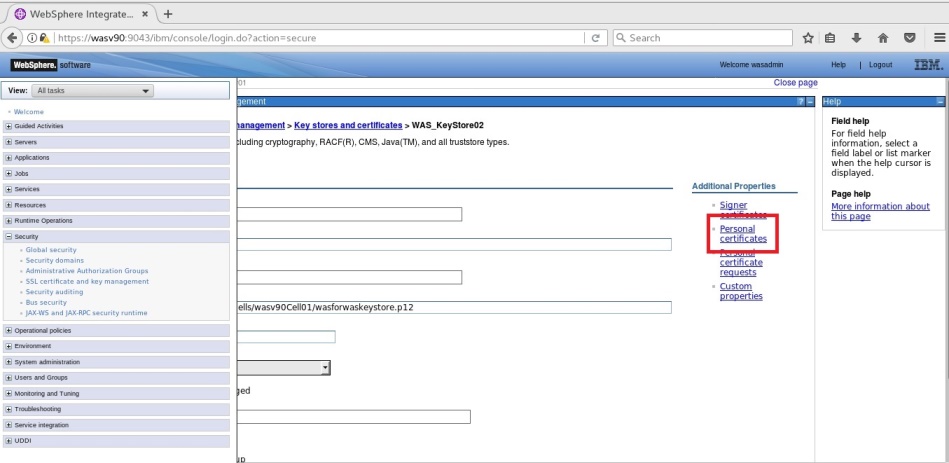
Configure Plugin



**Step 2:** Click on “WAS\_Keystore02”.



**Step 3:** Click “Personal certificates”.



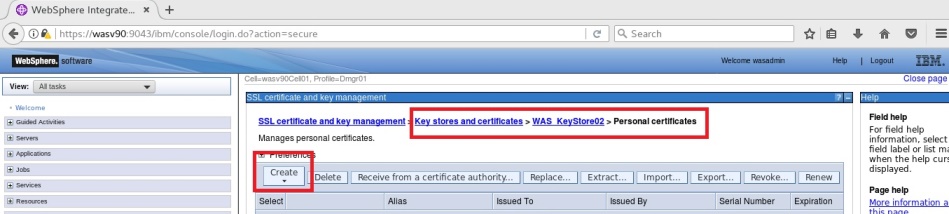
Create Keystore

Create Certificate

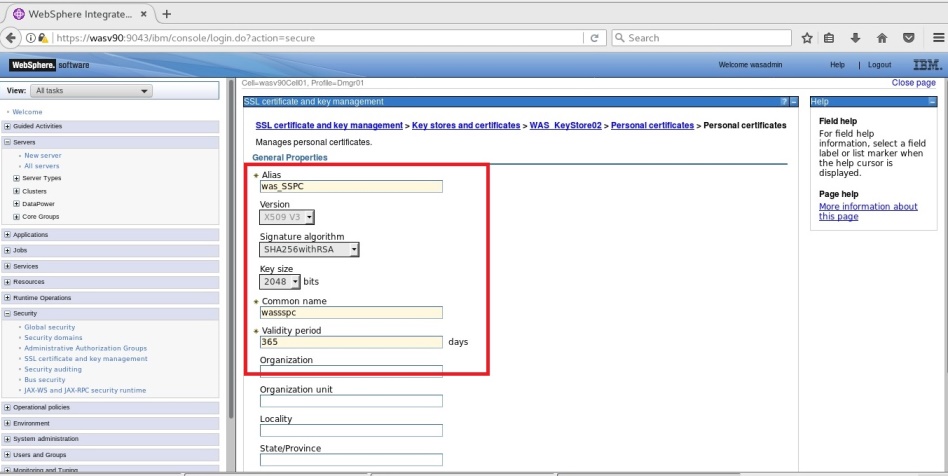
Configure Plugin



**Step 4:** Click “Create” to define a new personal certificate.



**Step 5:** Enter the values for the certificate as follows and click “OK”.



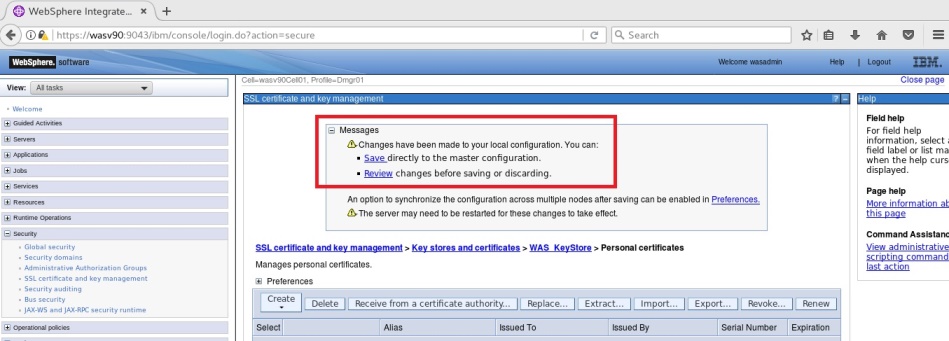
Create Keystore

Create Certificate

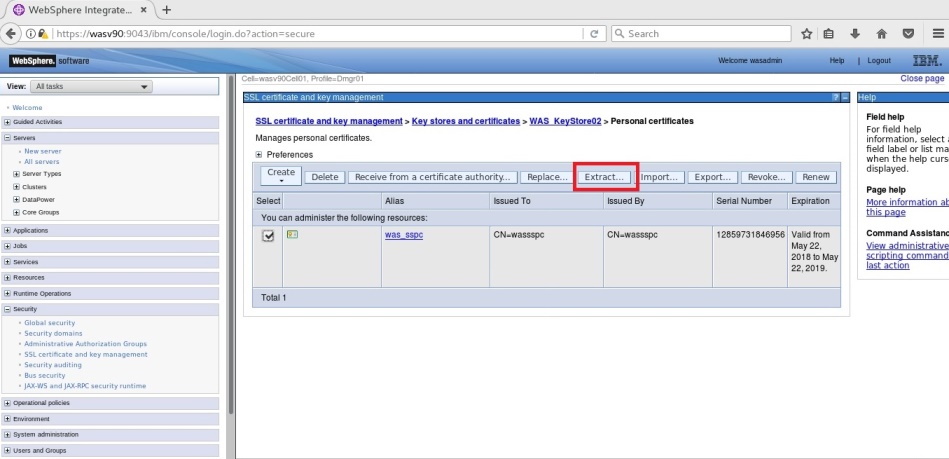
Configure Plugin



**Step 6:** Click “Save” to write changes.



**Step 7:** Select the “Alias” name and click “Extract”.



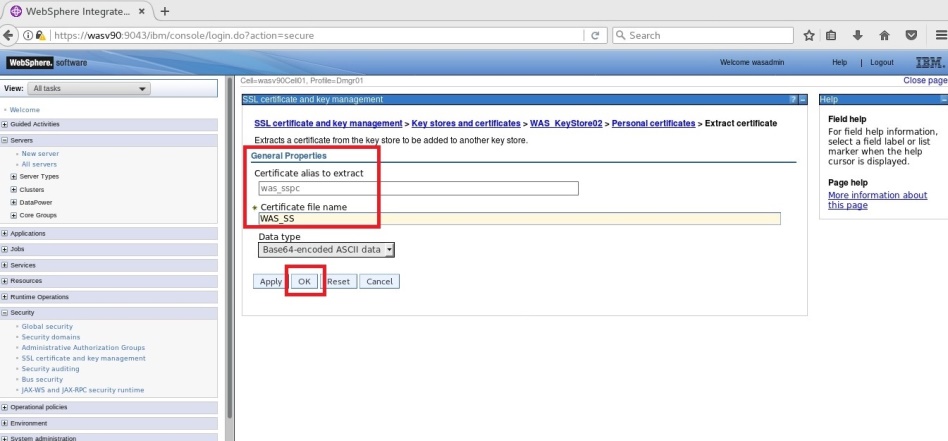
Create Keystore

Create Certificate

Configure Plugin



**Step 8:** Enter a name for “Certificate file name” and click “OK”.



**Task 2 is complete!**

Create Keystore

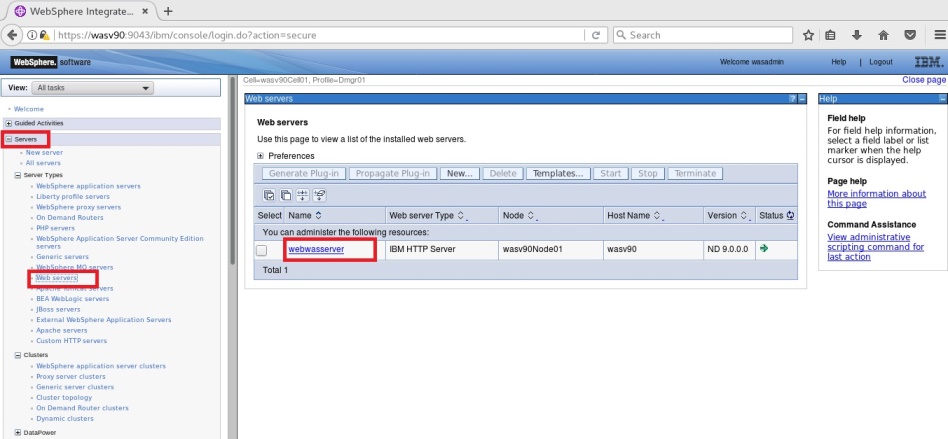
Create Certificate

Configure Plugin



**Task 3: Configure plug-in to use new certificate**

**Step 1:** Navigate to “Servers>Server Types>Web servers” and click on the web server name.



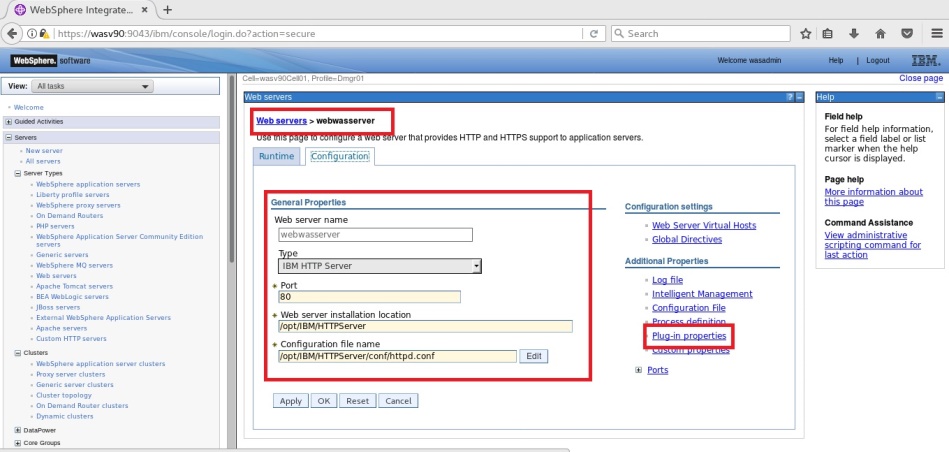
Create Keystore

Create Certificate

Configure Plugin



**Step 2:** Click on “Plug-in properties”.



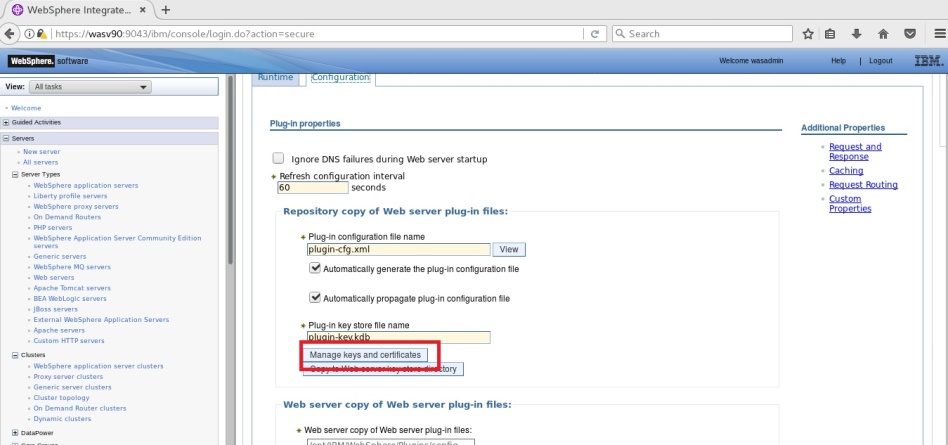
Create Keystore

Create Certificate

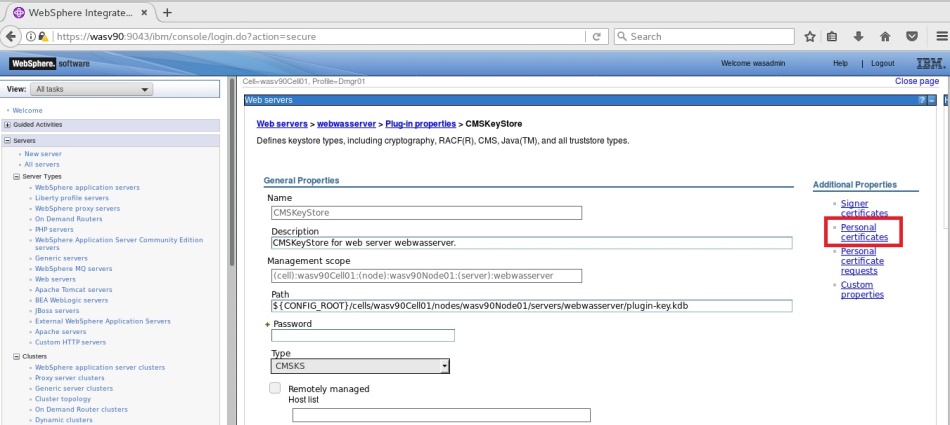
Configure Plugin



**Step 3:** In the configuration tab, click on “Manage keys and certificates”.



**Step 4:** Click on “Personal certificates”.



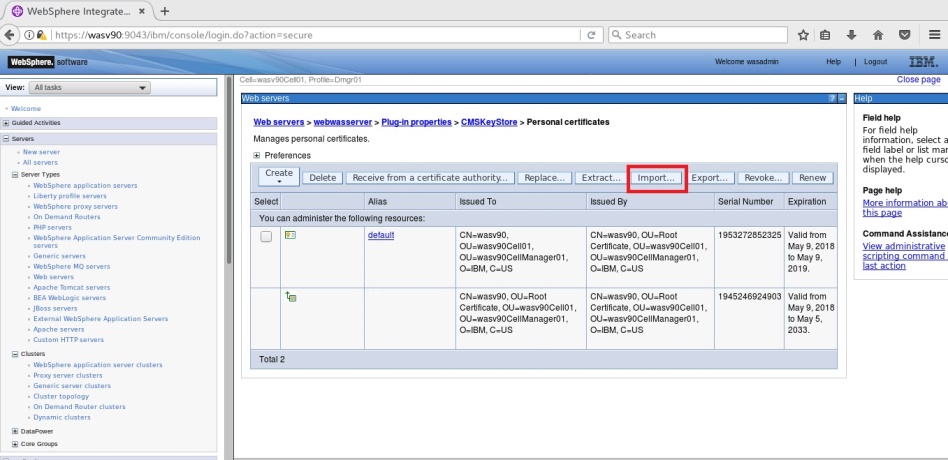
Create Keystore

Create Certificate

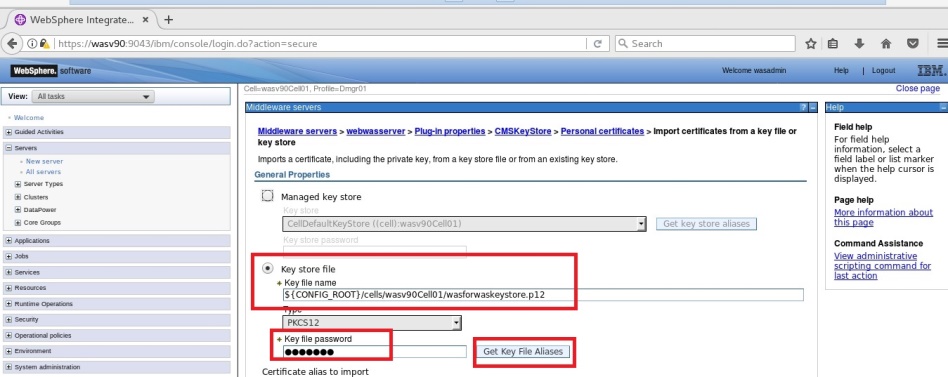
Configure Plugin



**Step 5:** Click “Import”.



**Step 6:** Enter the “Key store file” path and name, “${CONFIG\_ROOT}/cells/wasv90Cell01/wasforwaskeystore.p12” and the password. Click on “Get Key File Aliases”.



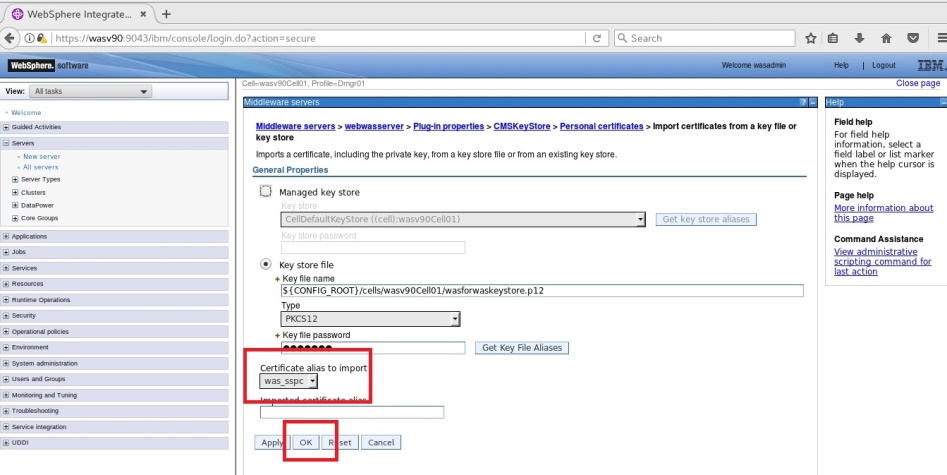
Create Keystore

Create Certificate

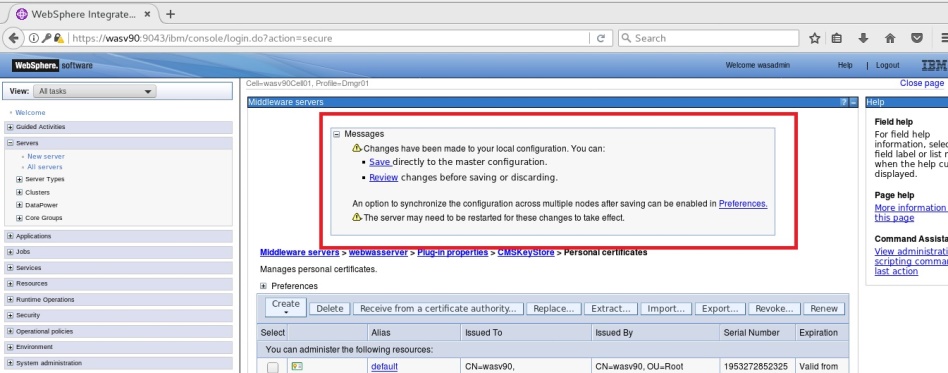
Configure Plugin



**Step 7:** Select the alias created on the second task, and click “OK”.



**Step 8:** Click “Save” to write changes to the master configuration file.



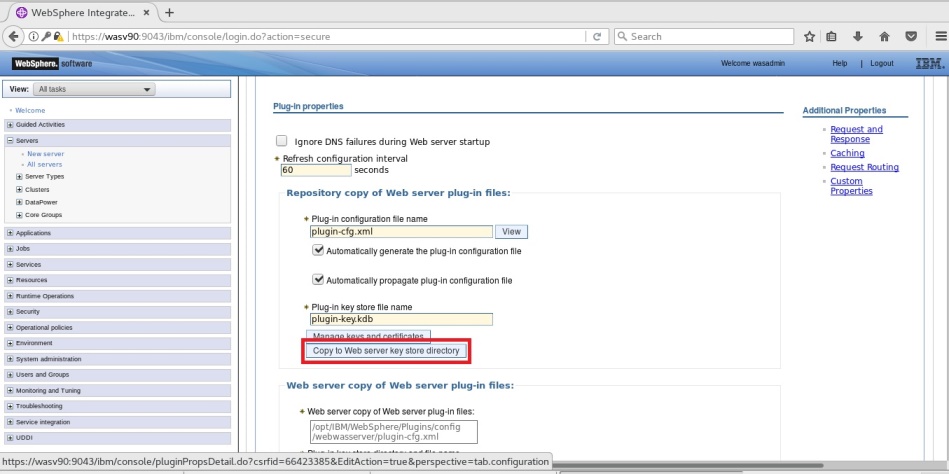
Create Keystore

Create Certificate

Configure Plugin



**Step 9:** On the “Configuration” tab, click “Copy to Web server key store directory”.



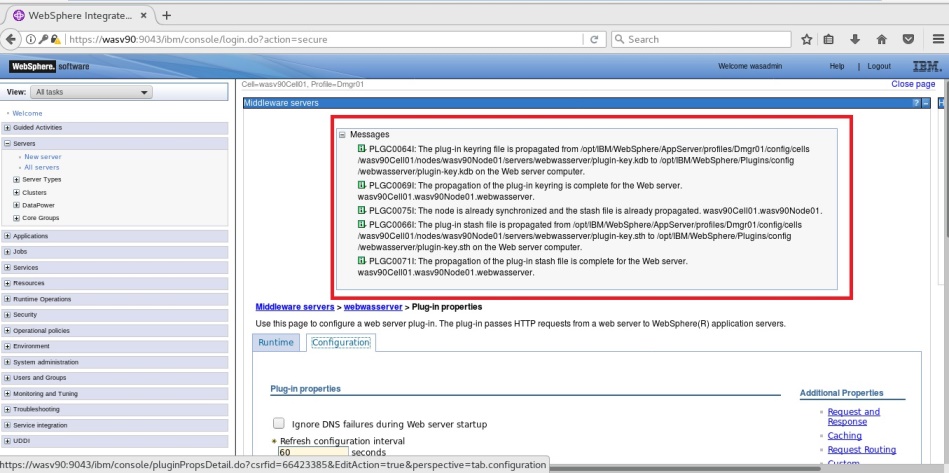
Create Keystore

Create Certificate

Configure Plugin



**Step 10:** Keyring file should be propagated to the web server.



**Task 3 is complete!**

# SUMMARY

WebSphere uses Java Secure Socket Extension (JSSE) which is an SSL implementation. SSL capabilities such as handshaking are delivered by JSSE using X.509 standard public key infrastructure (PKI). SSL uses certificates to authenticate the service provider by exchanging keys between server and client. WebSphere Application Server store these certificates in password protected files, in keystores. WebSphere Application Server can use SSL in the cell between the nodes, or to secure the communication between external systems that WebSphere Application Server transmits sensitive information such as database connection, LDAP connection, messaging connection and web services connection.

# REFERENCES

* http://publib.boulder.ibm.com/infocenter/iisinfsv/v8r0/index.jsp?topic=/com.ibm.swg.im.iis.productization.iisinfsv.install.doc/tasks/configurethewebsphereapplicationserverforssl.html
* http://www.ibm.com/developerworks/websphere/techjournal/1210\_lansche/1210\_lansche.html
* http://www-01.ibm.com/support/knowledgecenter/linuxonibm/liaag/l0wascry00\_2013.htm?cp=linuxonibm%2F0-4-3-2-0
* http://www-01.ibm.com/support/docview.wss?uid=swg21179559

# INDEX

JSSE 535

keyring 536

keystore 535

PKI 535

X.509 535