Steps to enable Third-Party SSL in OpManager:

1. Open the command prompt and change to **OpManager_Home directory.**

2. Generating keystore file:

Execute the following command and provide requested details to create OpManager.truststore file under conf folder.

>jre\bin\keytool.exe -v -genkey -keyalg RSA -keystore conf\OpManager.truststore -alias opmanager (Press Enter)

Enter keystore password:(Enter a password for this keystore. atleast 6 characters long. Press Enter)

What is your first and last name?

[Unknown]: (Enter the Server's name in which OpManager is running. It must be a FQDN [Fully Qualified Domain Name] Ex.: opmserver.manageengine.com. Press Enter.)

What is the name of your organizational unit?

[Unknown]: (Name of your Orgazational Unit. Ex: SYSADMIN. Press Enter.)

What is the name of your organization?

[Unknown]: (Your Organization Name. Ex:Zoho Corp. Press Enter.)

What is the name of your City or Locality?

[Unknown]: (Your city name. Ex:Pleasanton. Press Enter.)

What is the name of your State or Province?

[Unknown]: (Your state name. Ex:California. Press Enter.)

What is the two-letter country code for this unit?

[Unknown]: (Your country's two letter code. Ex:US. Press Enter.)

Is CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US correct?

[no]: (Check the details and if it is correct type yes and press enter. If else just press Enter to modify)

Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)
for CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US

Enter key password for <opmanager>
(RETURN if same as keystore password): (Just press enter. For tomcat both keystore password and key [alias] password must be the same)

[Storing conf\OpManager.truststore]

3. Generating CSR File (Certificate Signing Request):

Execute the following commands to create opmssl.csr file under conf folder.

>jre\bin\keytool.exe -v -certreq -file conf\opmssl.csr -keystore conf\OpManager.truststore -alias opmanager

Enter keystore password: (Enter the password for the keystore file)

Certification request stored in file <conf\opmssl.csr>

Submit this to your CA

4. Getting certificates from CA (Certification Authority):

Contact a CA like Verisign, Equifax, with the csr file generated in the previous step to get ssl certificate. Mostly you have to copy and paste the content of the csr file in a text area of theier website.

After verifying your request, mostly they will sent you the certficate content through mail. Copy and paste the content in a text editor and save it as "ServerCert.cer" under OpManager_Home\conf folder. Be cautious that while doing copy-paste, no extra space added at the end of lines.

5. Importing root and intermediate certifacates:

Before importing our certificate, we have to import the CA's root and intermediate certificates into the keystore file we generated at the second step. While mailing you the certificate, CA's will mention the link to their root and intermediate certificates. Save them under conf directory in the name "CARoot.cer" and "CAIntermediate.cer" respectively. Some CAs may have two or more intermediate certificates. Refer their document clearly before importing.

To import root certificate:

>jre\bin\keytool.exe -import -trustcacerts -file conf\CARoot.cer -keystore conf\OpManager.truststore -alias CARootCert

Enter keystore password: (Enter the keystore password)

(Root Certifiate's information will be printed)

Trust this certificate? [no]: (type yes and press enter if it is the certificate of your CA)

Certificate was added to keystore

To import Intermediate certificate:

>jre\bin\keytool.exe -import -trustcacerts -file conf\CAIntermediate.cer -keystore conf\OpManager.truststore -alias CAInterCert

Enter keystore password: (Enter the keystore password)

Certificate was added to keystore

6. Importing Server's Certificate:

Execute the follwing command to add the certificate received from CA to the keystore file.

>jre\bin\keytool.exe -import -trustcacerts -file conf\ServerCert.cer -keystore conf\OpManager.truststore -alias opmanager

Enter keystore password: (Enter the keystore password)

Certificate reply was installed in keystore

7. Configuring Tomcat:

Open "ssl_server.xml" file (under OpManager_Home\tomcat\conf\backup) in a text editor. Search for term "keystoreFile". It will be an attribute for connector tag. And set the value as "WEBNMS_ROOT_DIR/conf/OpManager.truststore". Change the value for "keystorePass" attribute with your keystore file password.

8. Modifying conf file:

Open "OpManagerStartUp.properties" file (under OpManager_Home\conf) in a text editor. Set the value of the parameter "https" as "Enable".

9. Start OpManager server. Connect client with https. Ex:https://opmserver.manageengine.com:80

Note:

If you are already having a certificate for this server and that certificate was requested by the keystore file generated using Java keytool, you may use it for SSL configuration. Just copy and paste the keystore file under OpManager_Home\conf and rename it to “OpManager.truststore” and follow the steps from 5.