**HTTPS with Wildfly 8.1**

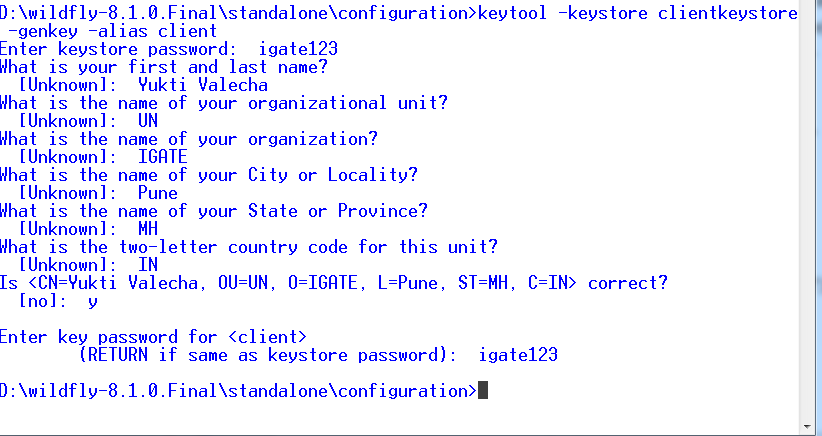
1. Generate keystore certificate

D:\wildfly-8.1.0.Final\standalone\configuration>keytool -keystore clientkeystore -genkey -alias client

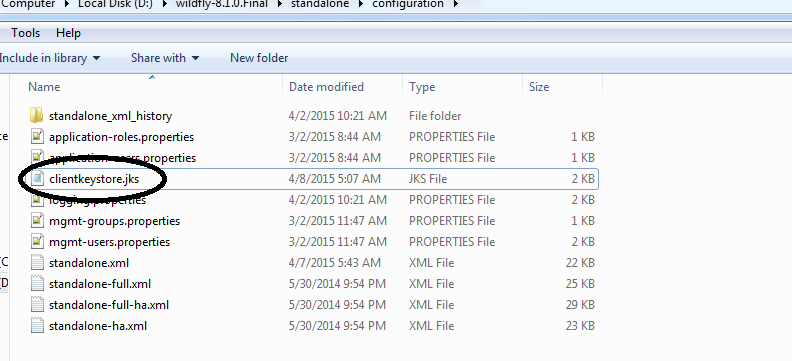
**[Keytool -keystore vaiClientkeystore -genkey -alias vaiClient**

**Keystore password=Vaishali**

**Key password=Vaishali**



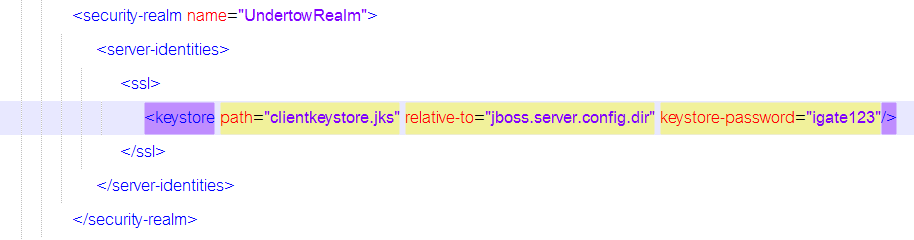
1. Answer the questions asked to generate certificate. When certificate is generated save it with extension (.jks) (Java KeyStore)



1. Following changes in standalone.xml file (D:\wildfly-8.1.0.Final\standalone\configuration)

Add following <security-realm> tag under <security-realms>

Below is the snapshot:



Below is the XML Listing:

<security-realms>

<security-realm name="UndertowRealm">

<server-identities>

<ssl>

<keystore path="clientkeystore.jks" relative-to="jboss.server.config.dir" keystore-password="igate123"/>

</ssl>

</server-identities>

</security-realm>

</security-realms>

**[In my case**

**It is**

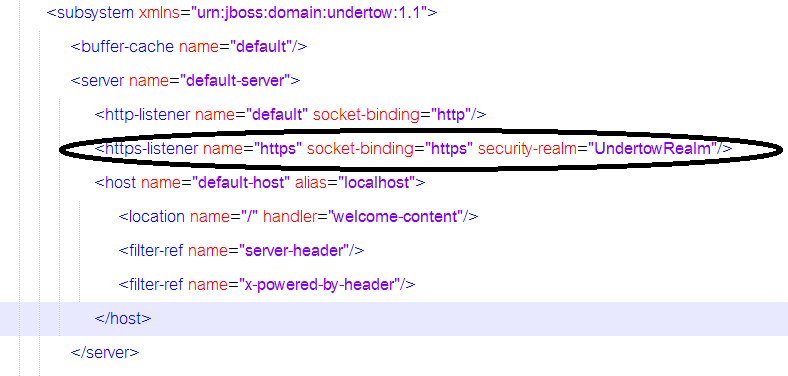
**<keystore path="vaiClientkeystore.jks" relative-to="jboss.server.config.dir" keystore-password="vaishali"/>**

**]**

1. Add the following tag high lightened:

(Note: This tag is already existing, need to add text which is high lightened)

Below is the snapshot:



Below is the XML Listing:

<subsystem xmlns="urn:jboss:domain:undertow:1.1">

<server name="default-server">

<http-listener name="default" socket-binding="http"/>

**<https-listener name="https" socket-binding="https" security- realm="UndertowRealm"/>**

<host name="default-host" alias="localhost">

<location name="/" handler="welcome-content"/>

<filter-ref name="server-header"/>

<filter-ref name="x-powered-by-header"/>

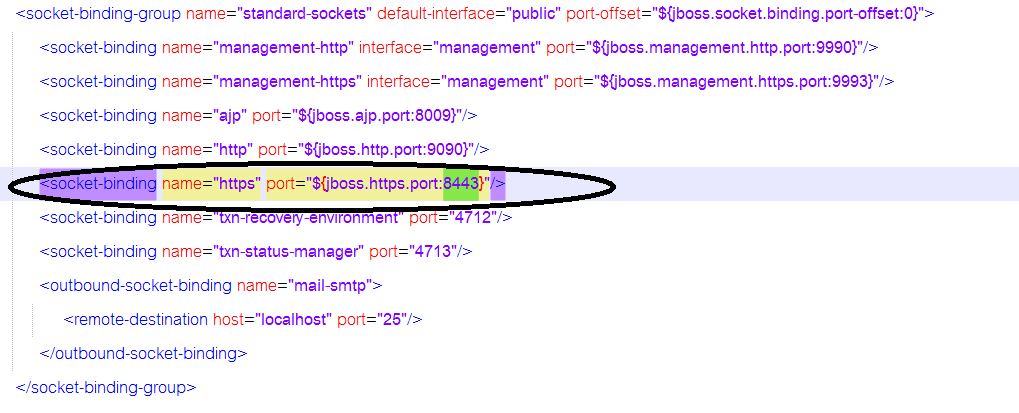
</host>

</server>

</subsystem>

1. The Https port number is 8443. Modify standalone.xml to supply port number.

Below is the snapshot:



Below is the XML Listing: (Observe the text which is highlightened)

<socket-binding-group name="standard-sockets" default-interface="public" port-offset="${jboss.socket.binding.port-offset:0}">

<socket-binding name="management-http" interface="management" port="${jboss.management.http.port:9990}"/>

<socket-binding name="management-https" interface="management" port="${jboss.management.https.port:9993}"/>

<socket-binding name="ajp" port="${jboss.ajp.port:8009}"/>

<socket-binding name="http" port="${jboss.http.port:9090}"/>

**<socket-binding name="https" port="${jboss.https.port:8443}"/>**

<socket-binding name="txn-recovery-environment" port="4712"/>

<socket-binding name="txn-status-manager" port="4713"/>

<outbound-socket-binding name="mail-smtp">

<remote-destination host="localhost" port="25"/>

</outbound-socket-binding>

</socket-binding-group>

1. In web.xml of the web application created:

<security-constraint>

<web-resource-collection>

<web-resource-name>Secure URLs</web-resource-name>

<url-pattern>/\*</url-pattern>

</web-resource-collection>

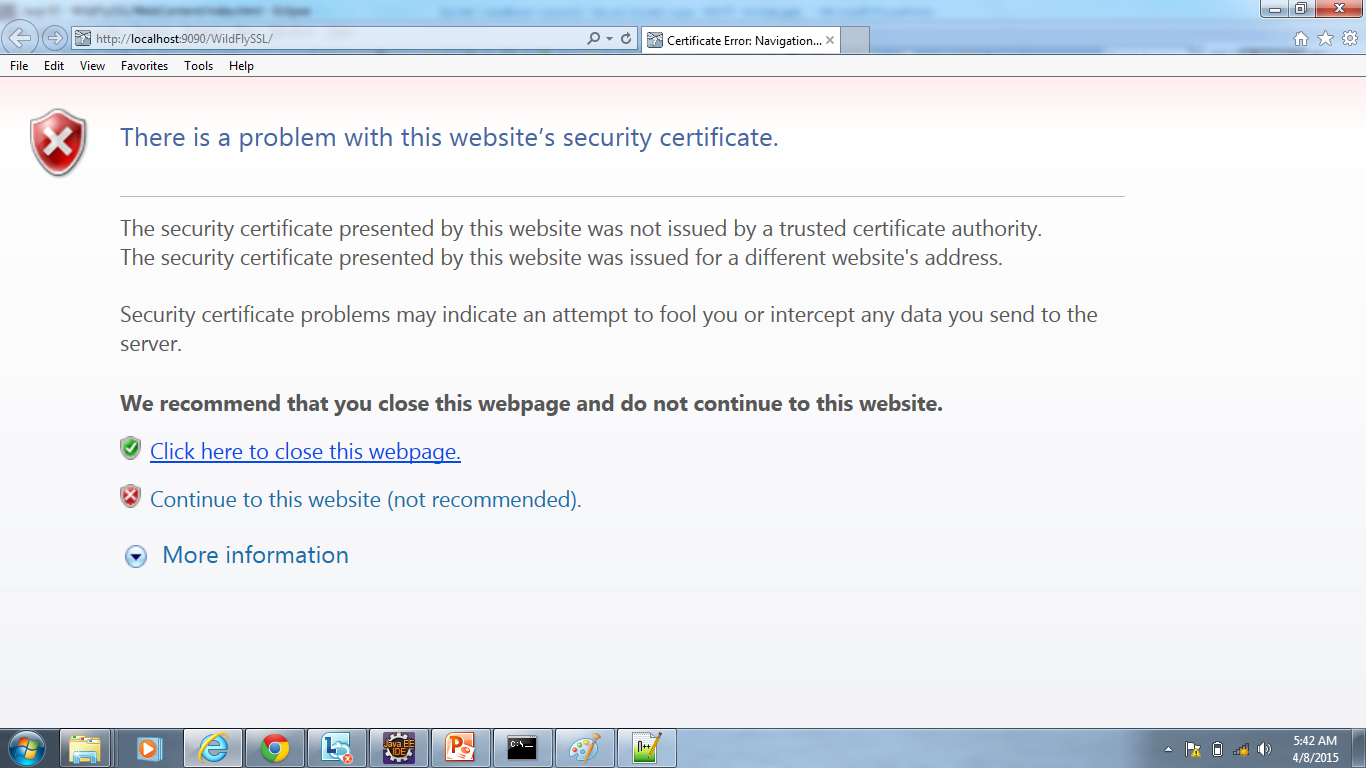
<user-data-constraint>

<transport-guarantee>CONFIDENTIAL</transport-guarantee>

</user-data-constraint>

</security-constraint>

1. See below snapshot on running the web application



1. Click on Continue to website (not recommended) to proceed. The port number is changed to 8443.

