Technical white paper

Service Manager 9.41 Collaboration Deployment

Table of contents

Introduction

As of version 9.41, HP Service Manager Collaboration supersedes the previous HP Enterprise Collaboration (EC) based instant messaging solution. As an instant messaging tool embedded in Service Manager, Collaboration integrates with Service Manager through LW-SSO and Apache proxy. Service Manager Collaboration enables Service Manager IT operators to collaborate in real time (or anytime) when handling an Interaction, Incident, Incident Task, Request, Request Task, Problem, Problem Task, Change, or Change Task by default. Service Manager users who do not log on to Service Manager but are available on Microsoft Office Lync can also be invited to a Collaboration conversation. In addition to the Service Manager Collaboration suggested participants that can be invited to a conversation, you can also search for users by email address or user name, and invite them to the conversation.

Purposes of this document

This document aims to help customers manually deploy Service Manager Collaboration environment with LW-SSO and SSL configured. It provides the following information:

- The Service Manager Collaboration deployment approach, including information on the chat server deployment, the Apache HTTP server deployment, LW-SSO configuration, and so on.
- Troubleshooting information, which can assist customers in solving issues related to the solution.

For detailed manual deployment steps, refer to the *Service Manager 9.41 Interactive Installation Guide*.

Target audience

This document is intended for HP customers and partners who want to deploy Service Manager 9.41 Collaboration. This document can help such customers understand the deployment process and perform detailed steps.

Prerequisites

The necessary prerequisites for Service Manager Collaboration deployment are described as follows:

- You must have the Apache configuration knowledge.
- You have installed Service Manager 9.41 binaries, Service Manager 9.41 applications, and Service Manager 9.41 web tier.
- You must know the domain of your Service Manager installation. In this document, the domain is training.com and the host name is sm941.training.com.

Requirements

To deploy Service Manager Collaboration successfully, read through the checklist below and make sure the configuration are completed by following the instructions provided in this document:

- Integrate Tomcat successfully with Apache OpenSSL.
- Deploy Openfire successfully.
- Configure proxy pass correctly in Apache.
- Configure LW-SSO correctly for Service Manager webtier, RTE and Openfire.
- Set the related parameters correctly in Service Manager.

About HP ITSM Deployment Manager

HP highly recommends you to install HP ITSM Deployment Manager and use it to deploy Service Manager Collaboration. HP ITSM Deployment Manager is a new free administration tool provided by HP to help you deploy and maintain your Service Manager environments as well as ease the setup and maintenance of Service Manager integration with other HP products. This tool is available at HP Live Network for free and all related information regarding its compatibility matrix and features are accessible at https://hpln.hp.com/group/itsm-deployment-manager. If you decide to use Deployment Manager to do your Collaboration installation, follow applicable instructions in the Deployment Manager documentation; otherwise, follow the instructions in this document.

Deploying Service Manager Collaboration

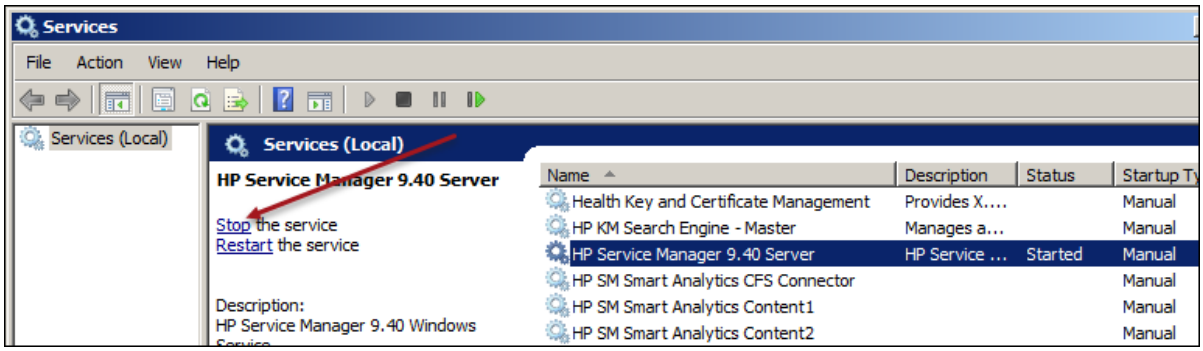
This section provides detailed tasks on HP Service Manager Collaboration deployment.

Task 1: Enable Lightweight Single Sign-On (LW-SSO) on Service Manager server

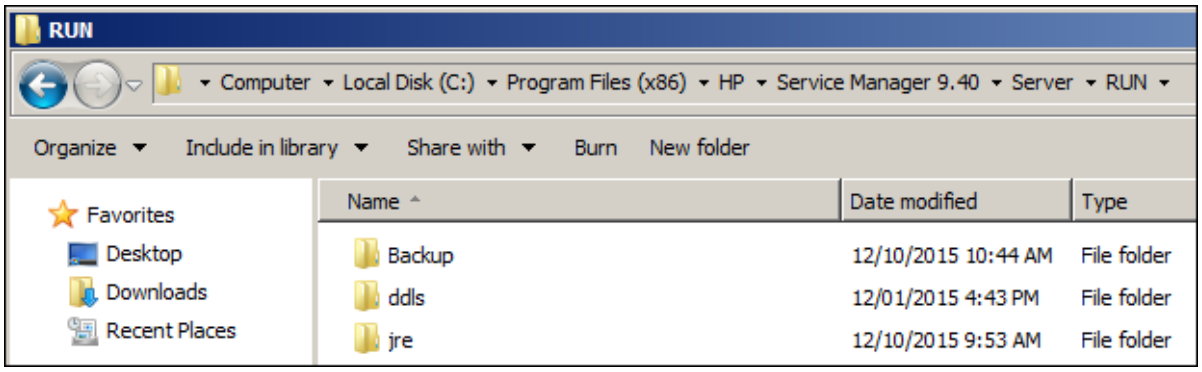
For Service Manager Collaboration to function, you need to configure Lightweight Single Sign-On (LW-SSO) on the Service Manager server, Service Manager web tier and Openfire service so that Service Manager users can use Service Manager Collaboration without logging on to the Service Manager server separately.

In this task, you will set up LW-SSO for the Service Manager Server. Follow these steps:

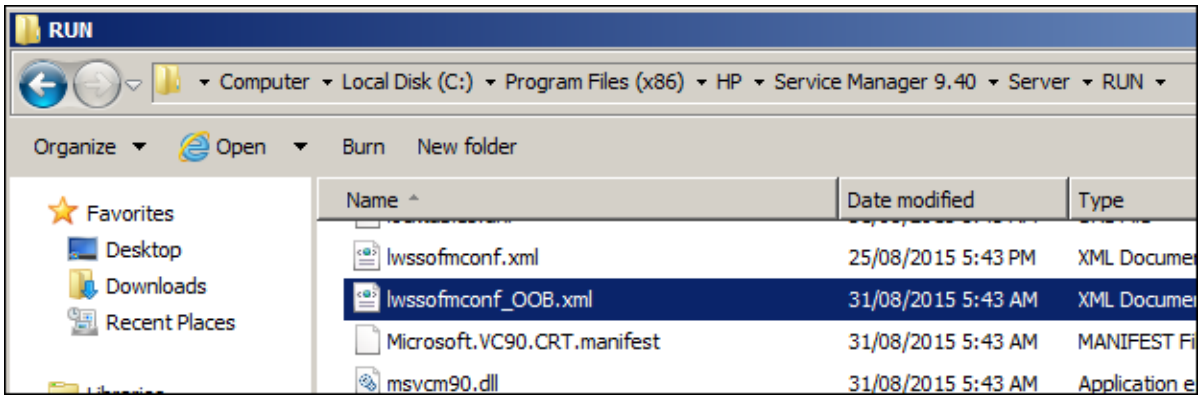
1. Log on to Service Manager as a system administrator.
2. Go to Windows Services and stop the **HP Service Manager 9.40 Server** service.



3. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.40\Server\RUN directory.

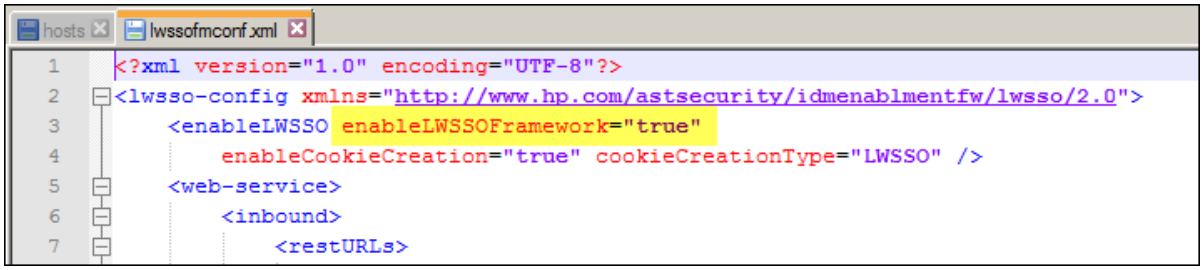


4. Copy the lwssofmconf.xml file and save it as lwssofmconf_OOB.xml.

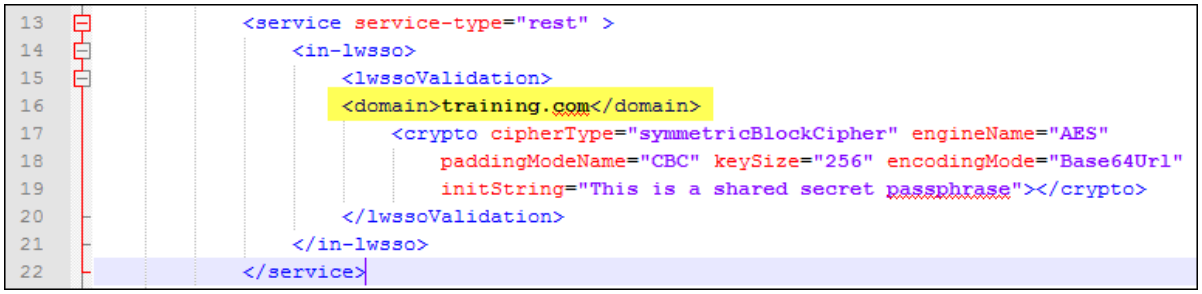


5. Open the lwssofmconf.xml file with a text editor.

6. Locate the `enableLWSSOFramework` parameter and ensure it is set to `true`.



7. Locate the `domain` value and set it to `training.com`.



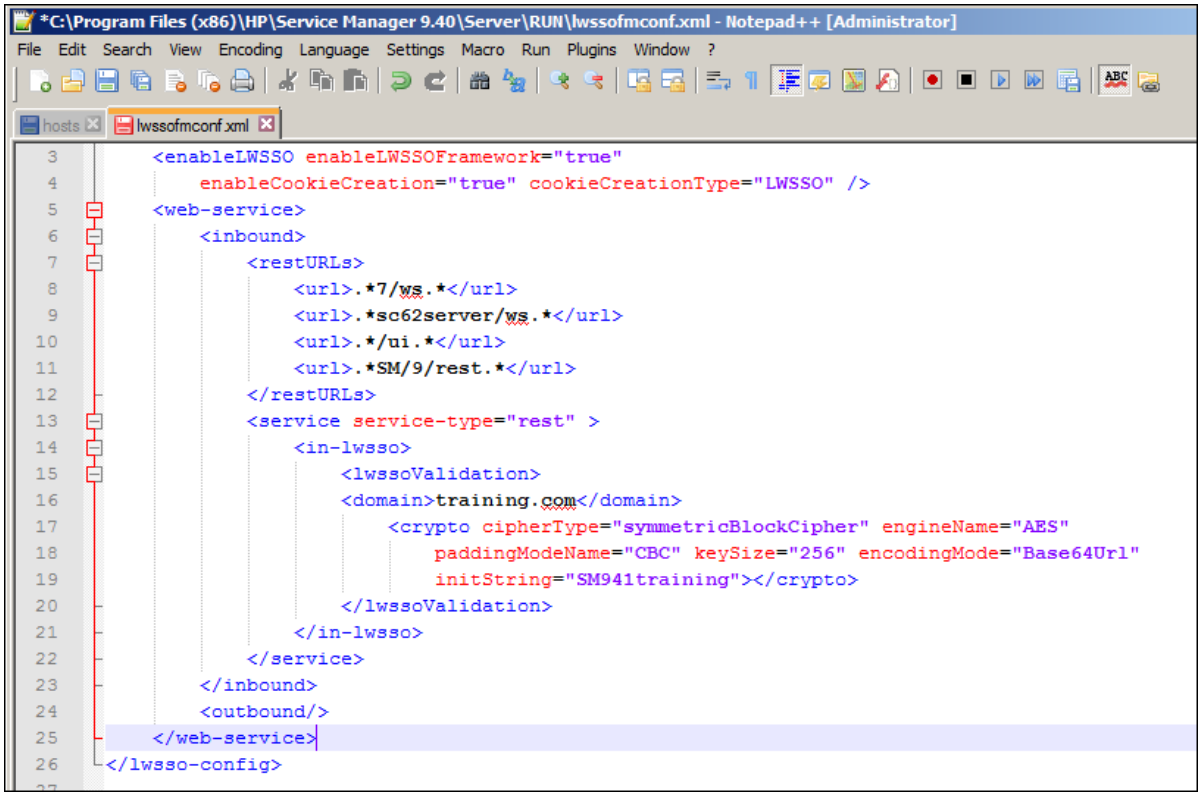
Note: To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application to the web tier can log in but may be forcibly logged out after a while.

8. Locate the `initString` value and set it to `SM941training`.

```
13          <service service-type="rest" >
14              <in-lwsso>
15                  <lwssoValidation>
16                  <domain>training.com</domain>
17                      <crypto cipherType="symmetricBlockCipher" engineName="AES"
18                          paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
19                          initString="SM941training"></crypto>
20                  </lwssoValidation>
21              </in-lwsso>
22          </service>
```

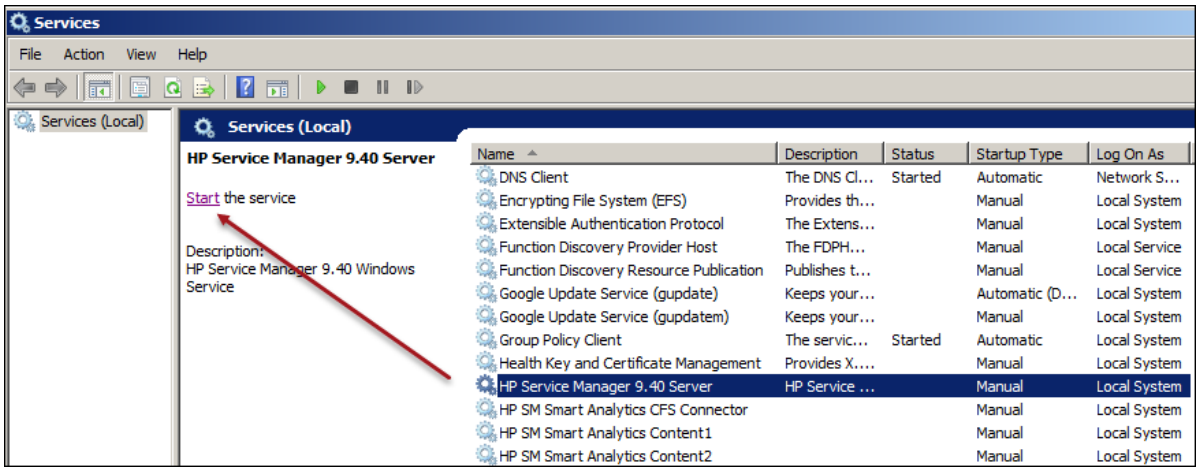
Note: This value can be set to anything as long as you use this value for all the `initString` values across the products you are installing LW-SSO for.

9. See the following screenshot for an overview of the lwssofmconf.xml file:



10. Save your changes and close the lwssofmconf.xml file.

11. Start the **HP Service Manager 9.40 Server** Windows service.

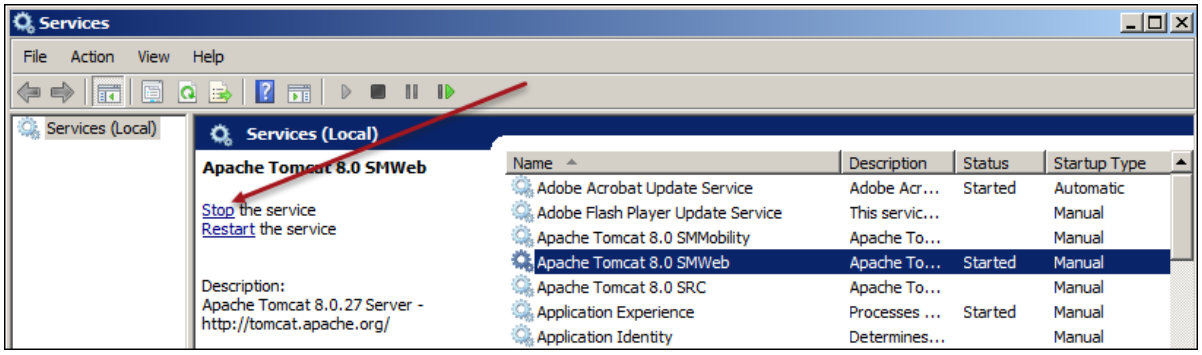


Task 2: Enable LW-SSO on Service Manager web tier

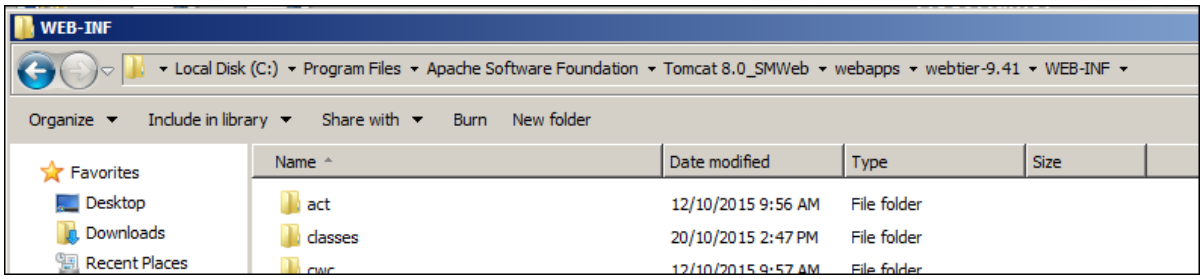
In this task, you will enable LW-SSO in the Service Manager web tier so that Service Manager users can use Service Manager Collaboration without logging on to the Service Manager server separately.

Follow these steps:

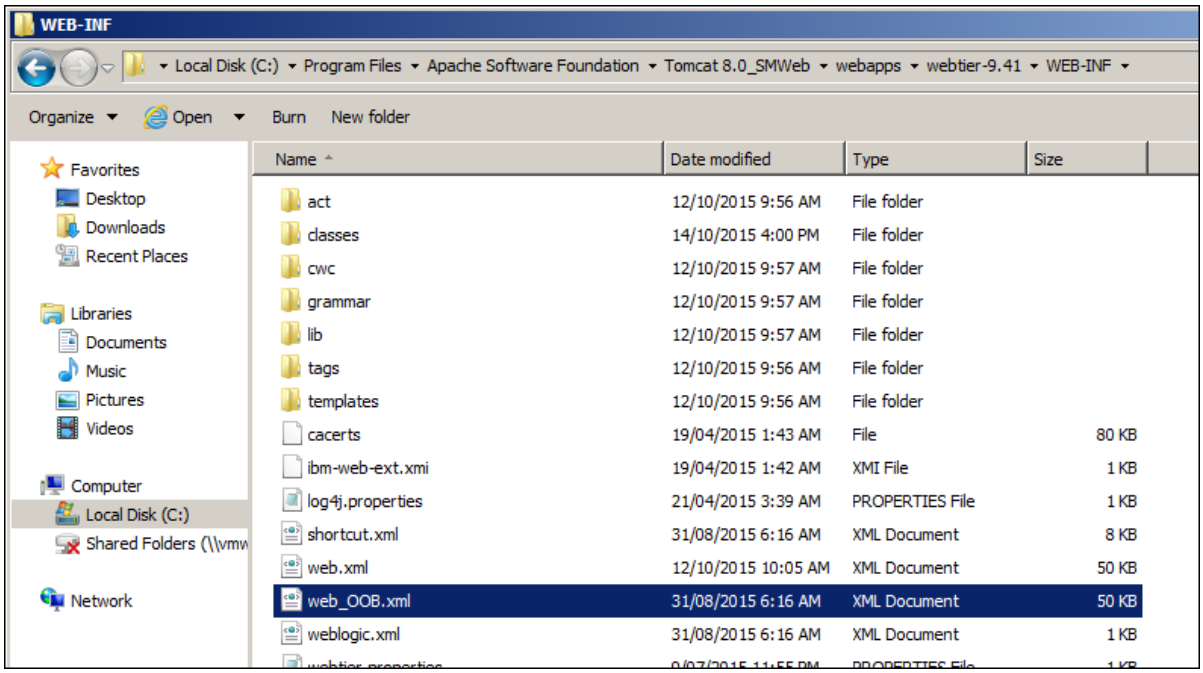
1. Go to Windows Services and stop the **Apache Tomcat 8.0 SMWeb** service.



2. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.41\WEB-INF directory.



3. Copy the web.xml file and save it as web_OOB.xml.



4. Open the web.xml file with a text editor.

5. Locate the `serverHost` parameter and set it to `sm941.training.com`.

```
572     <init-param>
573       <!-- Specify the HP Service Manager server host and port location -->
574       <param-name>serverHost</param-name>
575       <param-value>sm941.training.com</param-value>
576     </init-param>
```

6. Locate the `secureLogin` parameter and ensure it is set to `false`.

```
129    -->
130    <context-param>
131      <param-name>secureLogin</param-name>
132      <param-value>false</param-value>
133    </context-param>
```

7. Locate the `isCustomAuthenticationUsed` parameter and set it to `false`.

```
69
70    <context-param>
71      <param-name>isCustomAuthenticationUsed</param-name>
72      <param-value>false</param-value>
73    </context-param>
74
```

8. Locate `LWSSO filter`.

hosts | lwssofmconf.xml | web.xml | web_LWSSO.xml

```
395   <filter>
396     <filter-name>UIMMainFilter</filter-name>
397     <filter-class>com.hp.bsm.uim.web.UIMFilter</filter-class>
398   </filter>
399
400
401   <!-- LWSSO filter for integrations using HP lightweight single sign-on
402        PLEASE NOTE: Uncomment this filter and the associated filter-mapping,
403        and see application-context.xml for additional configuration needed
404        for LWSSO. -->
405   <!--
406   <filter>
407     <filter-name>LWSSO</filter-name>
408     <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
409   </filter>
410   -->
```

9. Uncomment the `<filter> ... </filter>` section by removing the preceding `<!--` and the posterior `-->`.

```
400
401   <!-- LWSSO filter for integrations using HP lightweight single sign-on
402        PLEASE NOTE: Uncomment this filter and the associated filter-mapping,
403        and see application-context.xml for additional configuration needed
404        for LWSSO. -->
405
406   <filter>
407     <filter-name>LWSSO</filter-name>
408     <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
409   </filter>
410   -->
411
412   <filter>
```

```
400
401   <!-- LWSSO filter for integrations using HP lightweight single sign-on
402        PLEASE NOTE: Uncomment this filter and the associated filter-mapping,
403        and see application-context.xml for additional configuration needed
404        for LWSSO. -->
405
406   <filter>
407     <filter-name>LWSSO</filter-name>
408     <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
409   </filter>
410
411
```

10. Locate `LWSSO filter` again.

```
474
475   <!-- LWSSO filter-mapping, please read description for LWSSO filter above
476        before uncommenting this. -->
477   <!--
478   <filter-mapping>
479     <filter-name>LWSSO</filter-name>
480     <url-pattern>/*</url-pattern>
481   </filter-mapping>
482   -->
483
```

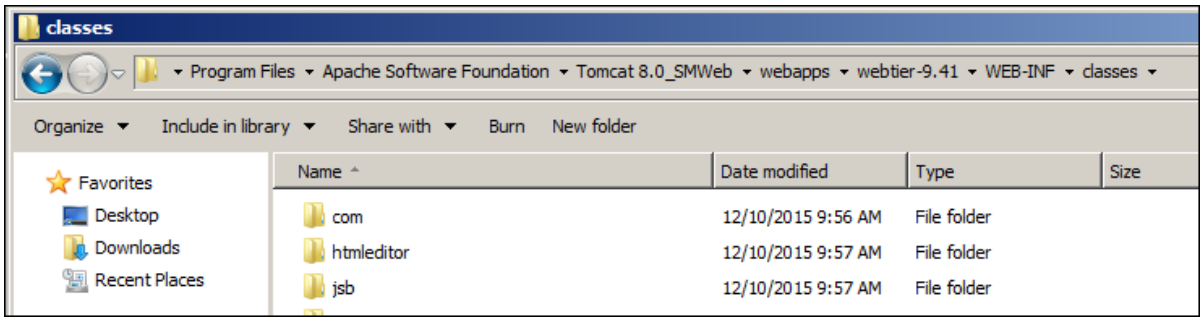
11. Uncomment the `<filter_mapping> ... </filter-mapping>` section by removing the preceding `<!--` and the posterior `-->`.

```
474
475   <!-- LWSSO filter-mapping, please read description for LWSSO filter above
476        before uncommenting this. -->
477
478   <filter-mapping>
479     <filter-name>LWSSO</filter-name>
480     <url-pattern>/*</url-pattern>
481   </filter-mapping>
482   -->
483
```

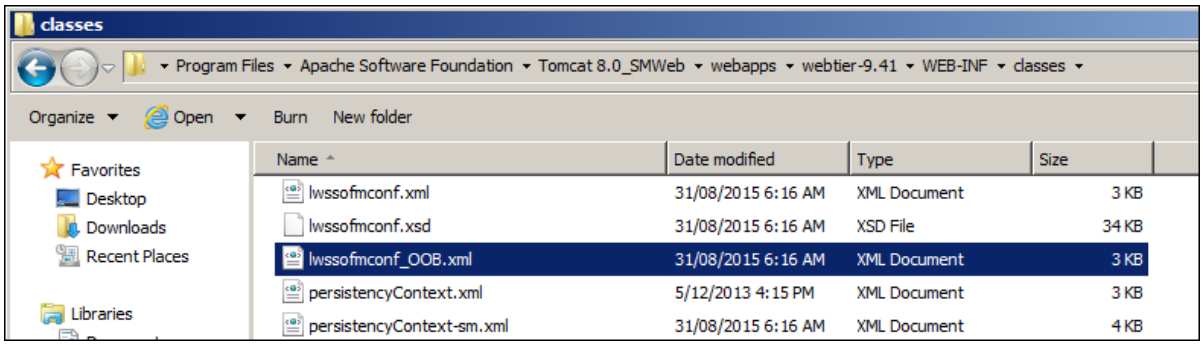
```
474
475   <!-- LWSSO filter-mapping, please read description for LWSSO filter above
476        before uncommenting this. -->
477
478   <filter-mapping>
479     <filter-name>LWSSO</filter-name>
480     <url-pattern>/*</url-pattern>
481   </filter-mapping>
482
```

12. Save your changes and close the web.xml file.

13. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.41\WEB-INF\classes directory.

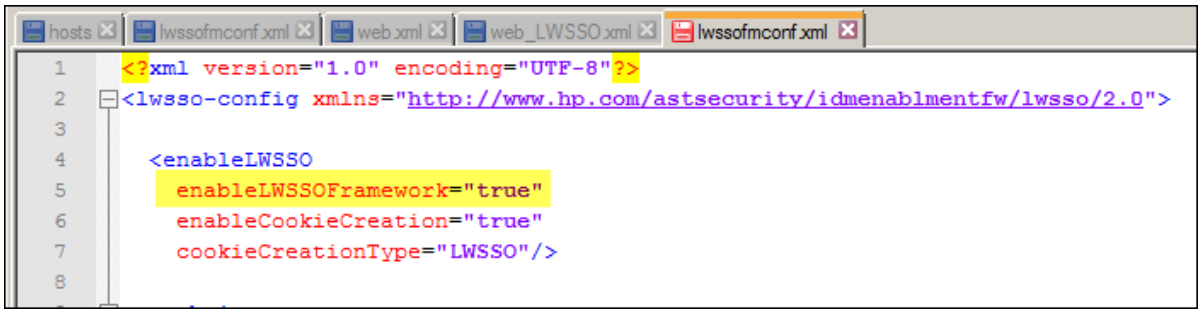


14. Copy the lwssofmconf.xml file and save it as lwssofmconf_OOB.xml.

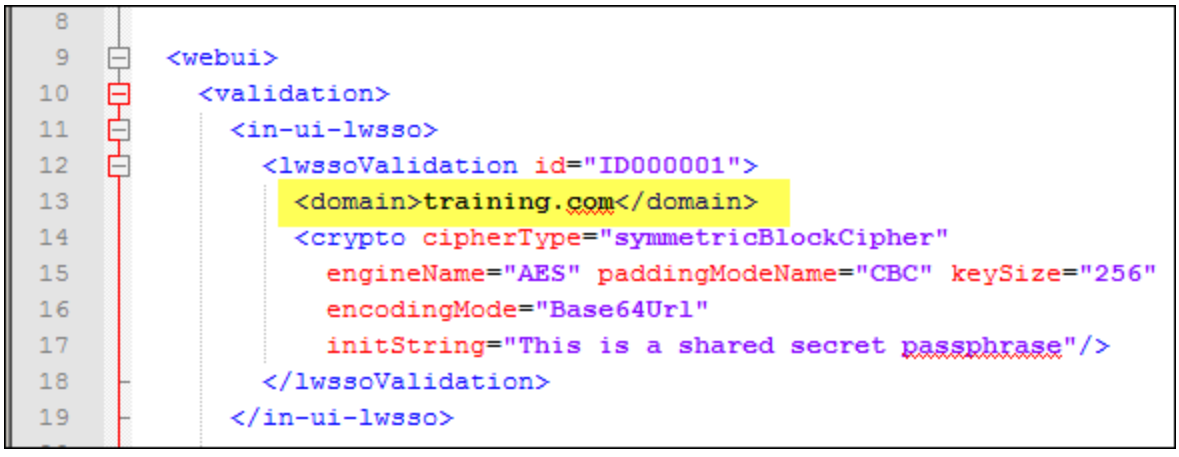


15. Open the lwssofmconf.xml file with a text editor.

16. Locate the `enableLWSSOFramework` parameter and set it to `true`.



17. Locate the `domain` parameter and set it to `training.com`.



18. Locate the `initString` value and set it to `SM941training`.

```
<webui>
  <validation>
    <in-ui-lwsso>
      <lwssoValidation id="ID000001">
        <domain>training.com</domain>
        <crypto cipherType="symmetricBlockCipher"
          engineName="AES" paddingModeName="CBC" keySize="256"
          encodingMode="Base64Url"
          initString="SM941training"/>
      </lwssoValidation>
    </in-ui-lwsso>
```

19. Locate the `secureHTTPCookie` value and set it to `false`.

```
  <creation>
    <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="false">
      <lwssoValidationRef refid="ID000001"/>
      <expirationPeriod>50</expirationPeriod>
    </lwssoCreationRef>
  </creation>
```

20. Locate the `multiDomain` section.

```
  <multiDomain>
    <trustedHosts>
      <DNSDomain>example.com</DNSDomain>
      <DNSDomain>example1.com</DNSDomain>
      <NetBiosName>myserver</NetBiosName>
      <NetBiosName>myserver1</NetBiosName>
      <IP>xxx.xxx.xxx.xxx</IP>
      <IP>xxx.xxx.xxx.xxx</IP>
      <FQDN>myserver.example.com</FQDN>
      <FQDN>myserver1.example1.com</FQDN>
    </trustedHosts>
  </multiDomain>
```

21. Set the first DNS Domain from `example.com` to `training.com`.

```
47
48      <multiDomain>
49        <trustedHosts>
50          <DNSDomain>training.com</DNSDomain>
51          <DNSDomain>example1.com</DNSDomain>
52          <NetBiosName>myserver</NetBiosName>
53          <NetBiosName>myserver1</NetBiosName>
```

22. Set the first FQDN from `myserver.example.com` to `sm941.training.com`.

```
48      <multiDomain>
49        <trustedHosts>
50          <DNSDomain>training.com</DNSDomain>
51          <DNSDomain>example1.com</DNSDomain>
52          <NetBiosName>myserver</NetBiosName>
53          <NetBiosName>myserver1</NetBiosName>
54          <IP>xxx.xxx.xxx.xxx</IP>
55          <IP>xxx.xxx.xxx.xxx</IP>
56          <FQDN>sm941.training.com</FQDN>
57          <FQDN>myserver1.example1.com</FQDN>
58        </trustedHosts>
59      </multiDomain>
```

23. Save your changes and close the lwssofmconf.xml file.

24. In the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.41\WEB-INF\classes directory, copy the application-context.xml file and save it as application-context_OOB.xml.

25. Open the application-context.xml file with a text editor.

26. Locate the `httpSessionContextIntegrationFilter` line.

```
45          /wf/**=ajaxFilter
46          /cm/**=ajaxFilter
47          /api/calendar/**=ajaxFilter
48          /**=httpSessionContextIntegrationFilter,anonymousProcessingFilter
49        </value>
50      </property>
51    </bean>
```

27. Add `lwSsoFilter` to this line as follows:

```
45          /wf/**=ajaxFilter
46          /cm/**=ajaxFilter
47          /api/calendar/**=ajaxFilter
48          /**=httpSessionContextIntegrationFilter,lwSsoFilter,anonymousProcessingFilter
49        </value>
50      </property>
51    </bean>
```

Caution: Use the correct case for lwSsoFilter.

28. Locate bean id="lwSsoFilter".

```
281
282   <!-- This bean is used for HP Lightweight Single Sign-on, to integrate with other
283        Hewlett-Packard software products. Uncomment it here and reference it in the
284        filterChainProxy as commented above. -->
285   <!--
286   <bean id="lwSsoFilter" class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
287     <property name="authenticationManager">
288       <ref bean="authenticationManager"/>
289     </property>
290     <property name="defaultRole">
291       <value>ROLE_PRE</value>
292     </property>
293   </bean>
294   -->
```

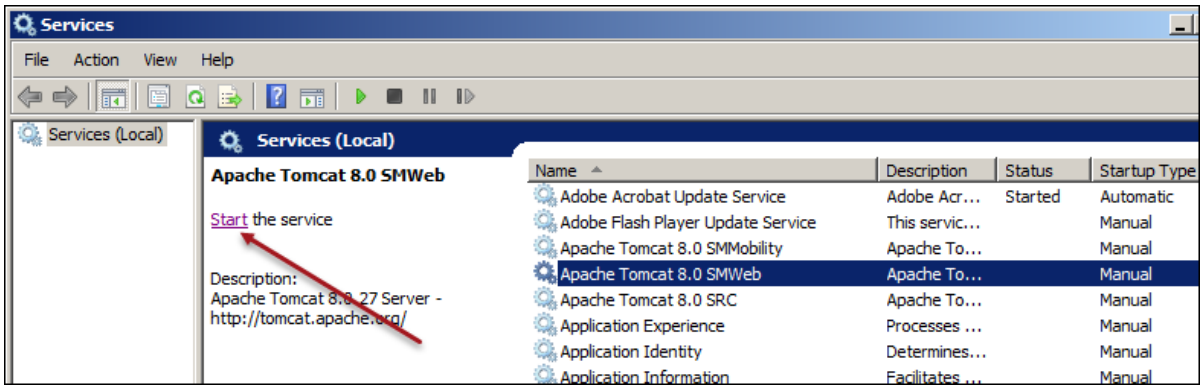
29. Uncomment this section by removing the preceding <!-- and the posterior -->.

```
281
282   <!-- This bean is used for HP Lightweight Single Sign-on, to integrate with other
283        Hewlett-Packard software products. Uncomment it here and reference it in the
284        filterChainProxy as commented above. -->
285
286   <bean id="lwSsoFilter" class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
287     <property name="authenticationManager">
288       <ref bean="authenticationManager"/>
289     </property>
290     <property name="defaultRole">
291       <value>ROLE_PRE</value>
292     </property>
293   </bean>
294   -->
```

```
281
282   <!-- This bean is used for HP Lightweight Single Sign-on, to integrate with other
283        Hewlett-Packard software products. Uncomment it here and reference it in the
284        filterChainProxy as commented above. -->
285
286   <bean id="lwSsoFilter" class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
287     <property name="authenticationManager">
288       <ref bean="authenticationManager"/>
289     </property>
290     <property name="defaultRole">
291       <value>ROLE_PRE</value>
292     </property>
293   </bean>
294
295
```

30. Save your changes and close the application-context.xml file.

31. Go to Windows Services and start the **Apache Tomcat 8.0 SMWeb** service.



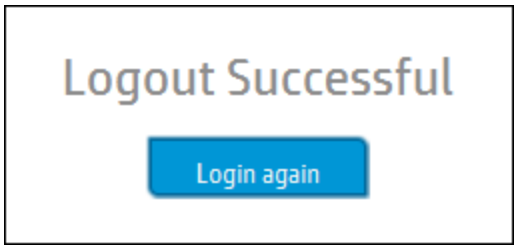
Task 3: Test LW-SSO with Service Manager web tier

In this task, you will test that you can log on to Service Manager.

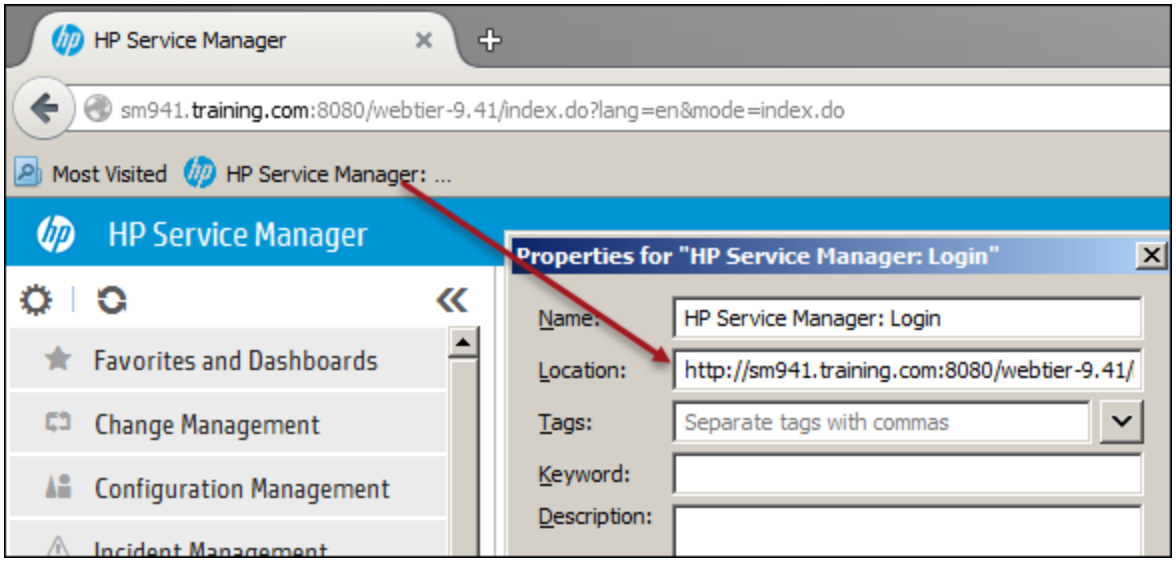
1. Access http://sm941.training.com:8080/webtier-9.41/index.do in your web browser to display the Service Manager log on screen.

2. Log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

   If you are directed to the Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.



3. Note that from now on, you need to use the fully qualified domain name (FQDN) in the URL when logging on to Service Manager. You may wish to update the bookmarks in the bookmark toolbar.



Note: At this stage, you are still using HTTP (not HTTPS) because SSL is not currently being used.

Task 4: Install 32-bit Java for the chat server

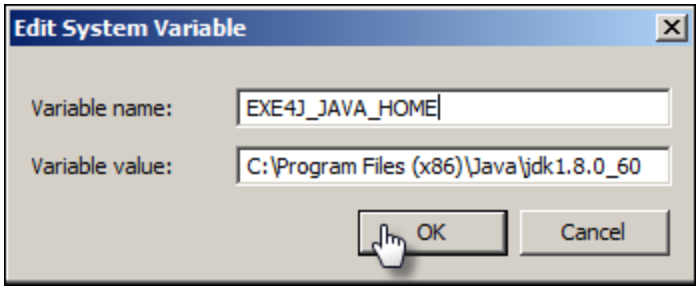
In this task, you will install the 32-bit Java and then set the `EXE4J_JAVA_HOME` variable for the chat server. If you are using your own server and already have the 32-bit Java installed, set JAVA_HOME to the location of the JRE or JDK and follow steps 11 to 12 only.

Follow these steps:

1. This task use Java 8 update 60. Download the latest Java 32-bit version (jdk-8u60-windows-i586.exe) from the Java website http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-

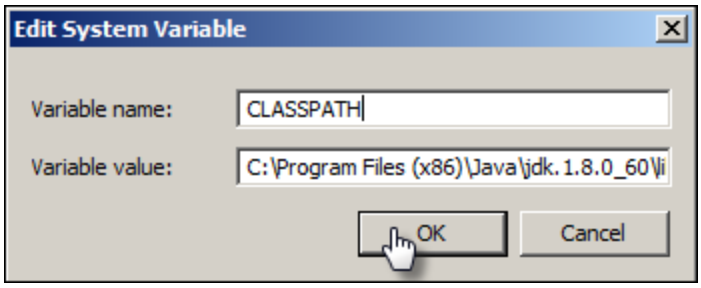
2133151.html.

2. The system displays the welcome screen. Click **Next**.
3. Accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_60), and then click **Next** to start the Java installation process.
4. On the JRE Destination Folder screen, accept the default installation folder (C:\Program Files (x86)\Java\jdk1.8.0_60) and click **Next**.
5. When the 32-bit Java is installed, click **Close**.
6. To add and update the environment variables for the server, right-click **Computer** on the Windows desktop and select **Properties**.
7. Click **Advanced system settings**.
8. On the **System Properties** window, click the **Environment Variables** button.
9. In the **System variables** section, click **New...**.
10. Edit the new system variable as illustrated below, and then click **OK**.



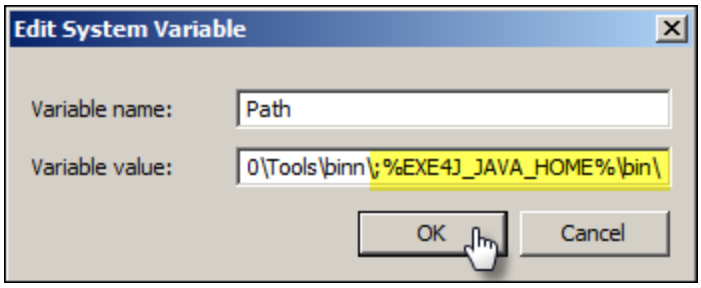
Field	Value
Variable name	EXE4J_JAVA_HOME
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_60\

11. In the **System variables** section, click **New...** again.
12. Edit the new system variable as illustrated below, and then click **OK**.



Field	Value
Variable name	CLASSPATH
Variable value	C:\Program Files (x86)\Java\jdk.1.8.0_60\lib\

13. Locate the **Path** system variable and click **Edit**.
14. Add `;%EXE4J_JAVA_HOME%\bin\` to the end of the value, and then click **OK**.



15. Click **OK** to close the **Environment Variables** window.
16. Click **OK** to close the **System Properties** window.

Task 5: Deploy the chat server

HP provides a preconfigured version of Openfire as the Service Manager Collaboration chat server, which is easy to set up and administer, but offers rock-solid security and performance. In this task, you will install the Openfire chat server and go through configuration steps for it.

Note:

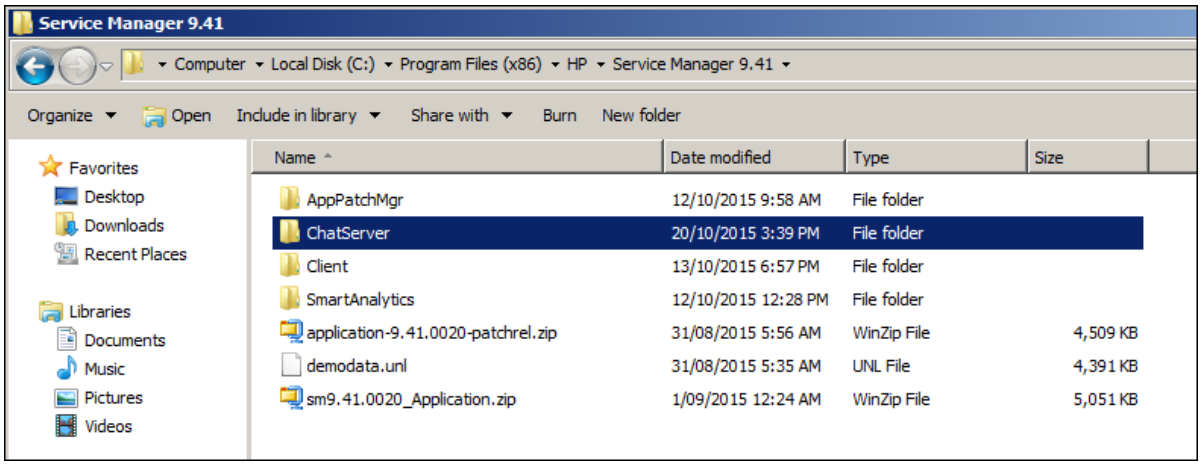
- The Openfire chat server can be deployed on the Windows system only, but it works well with the

Service Manager servers on all the platforms such as Linux.

- Openfire shares the Service Manager database. You may need to back up the Service Manager database before beginning this task.

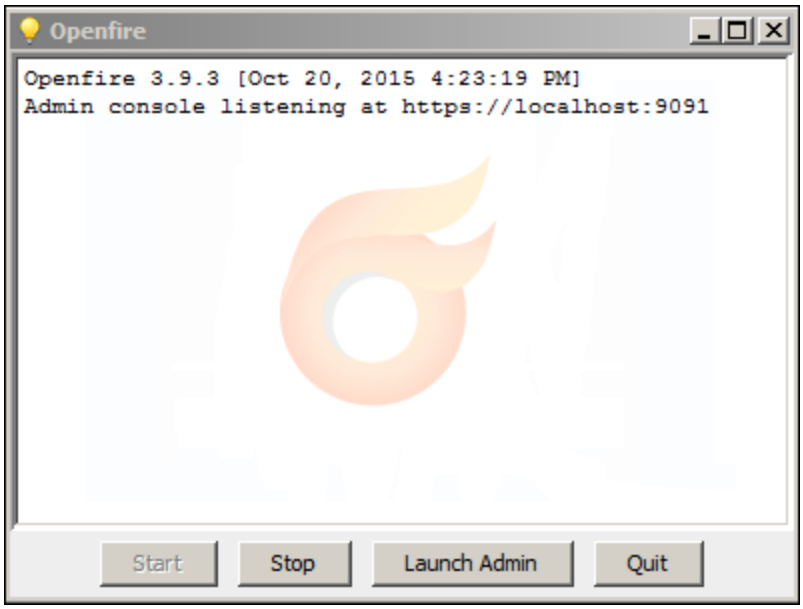
Follow these steps:

1. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.41 folder and create a new directory called ChatServer.



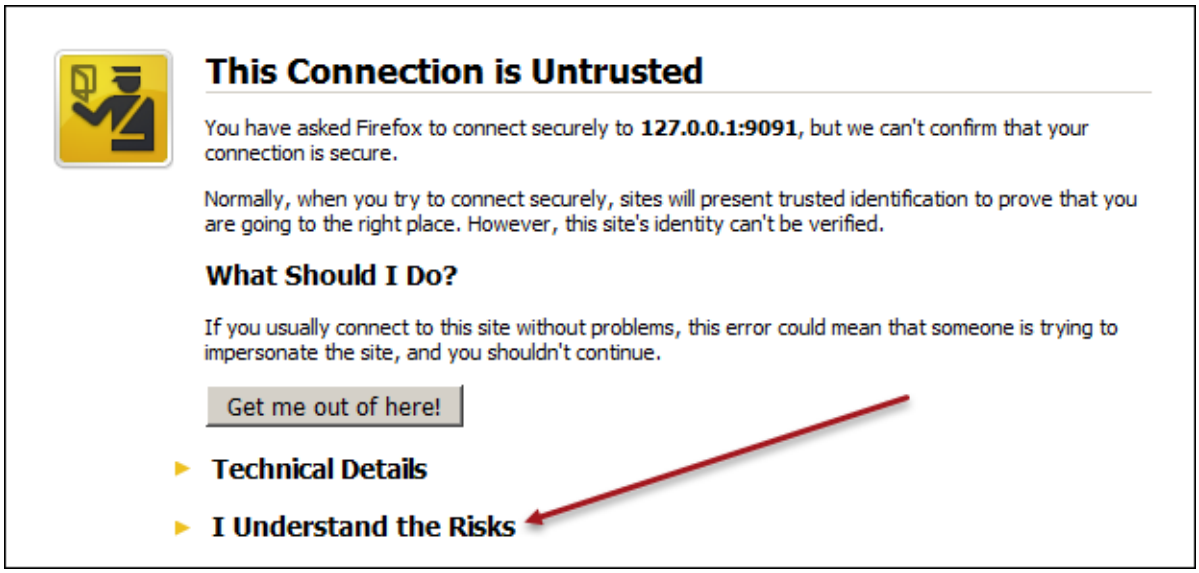
2. Extract the sm9.41.0020_ChatServer.zip file to the C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer folder.

3. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\bin folder, and then double-click openfire.exe to display the Openfire window.

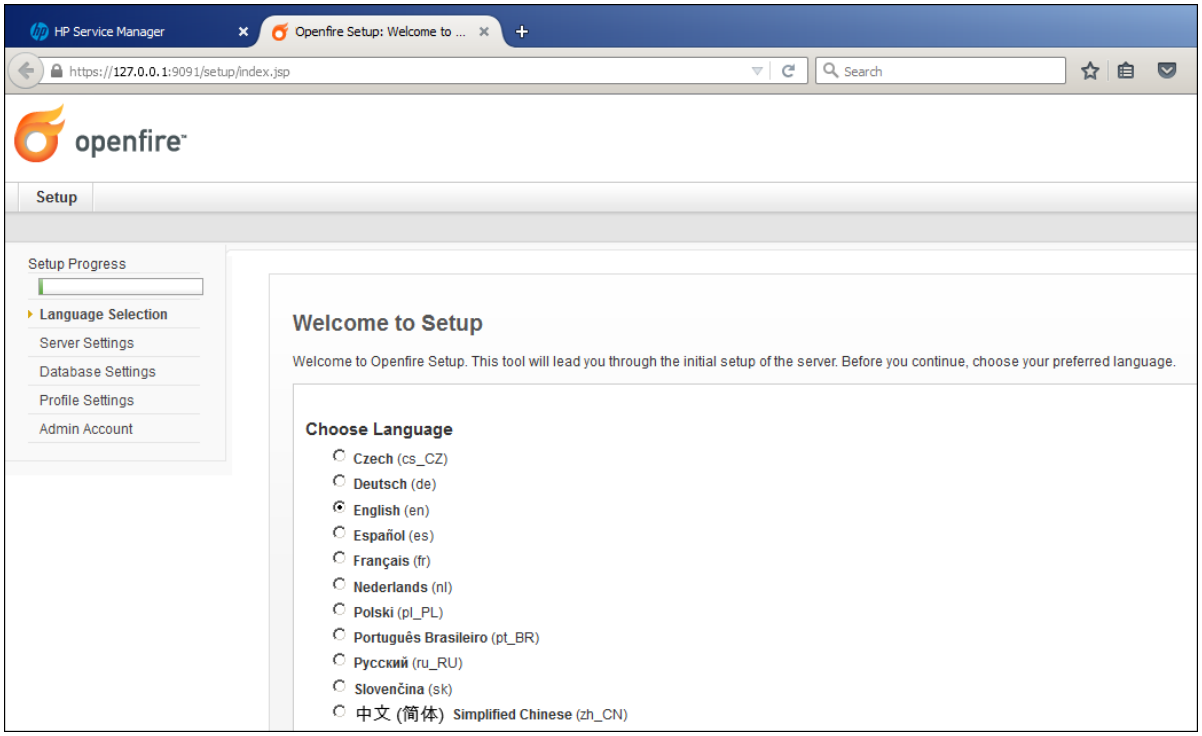


It may take a few seconds for the buttons to become available.

4. Click **Launch Admin**. If you see the following or similar screen, click **I Understand the risks**.



The Openfire Setup: Welcome to Setup screen is displayed.

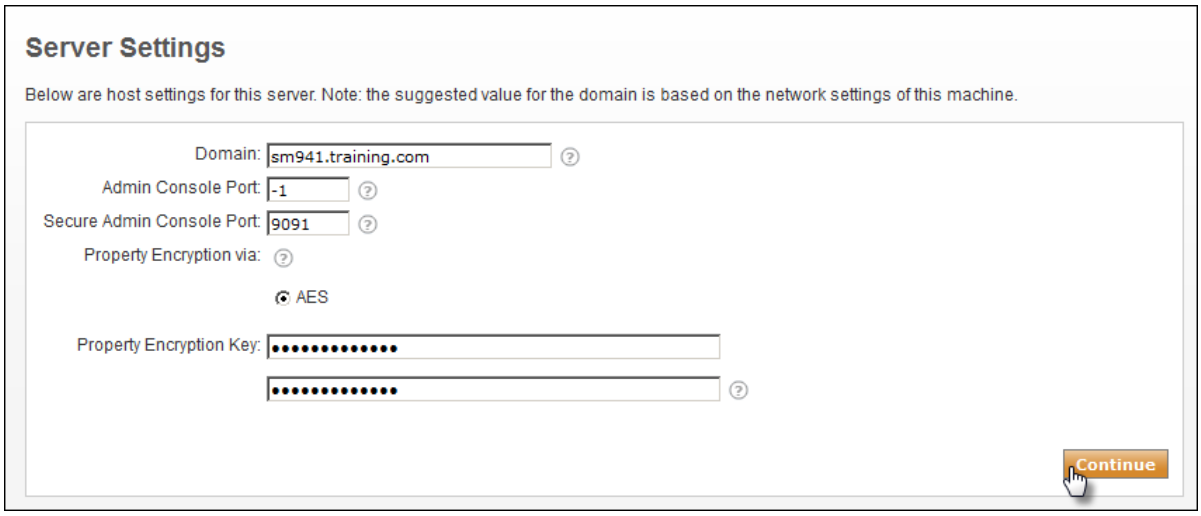


Note:
You can also visit https://127.0.0.1:9091/setup/index.jsp or https://localhost:9091/setup/index.jsp to access the Openfire Administrator Console web page at any time. However, the Openfire Administrator Console web page is accessible only from the same computer on which the Openfire server is deloyed. Error messages will be displayed if you try to visit https://*<IP address>*:9091 from another computer.

5. Select **English** and click **Continue**.

   The Openfire Administrator Console supports Czech (cs), German (de), English (en), Spanish (es), French (fr), Dutch (nl), Polish (pl_PL), Brazilian Portuguese (pt_BR), Russian (ru_RU), Slovak (sk), and Simplified Chinese (zh_CN).

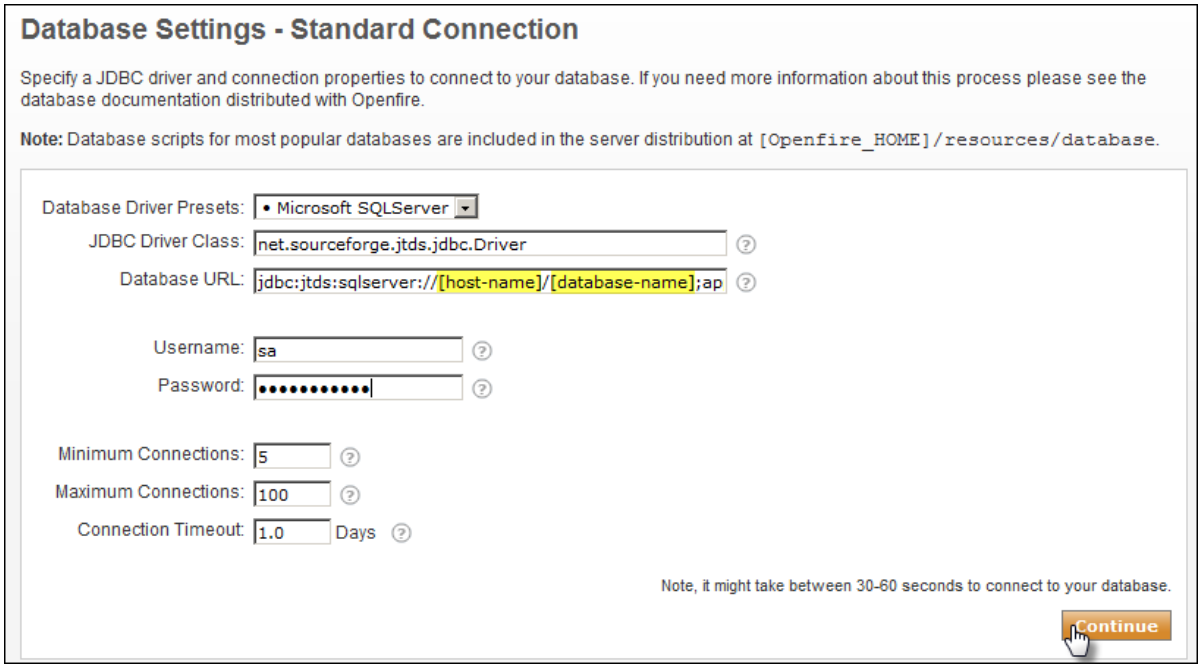
6. You need to specify the database details so that Openfire can connect to your Service Manager database and create the DB tables. Update the fields as illustrated below on the Server Settings screen, and then click **Continue**.



Parameter	Value in this task	Description
Domain	sm941.training.com	Domain name of the Openfire server host. Note that this domain has no relationship with LW-SSO. You can type any value, including symbols such as underline(_) and hyphen(-). This value is used on the SM collaboration setting page later.
Admin Console Port	-1	The port used for unsecured Admin Console access. The default value is -1. Leave this port to its default value if you do not need to open an HTTP port.
Secure Admin Console Port	9091	The HTTPS port used for secured Openfire Admin Console access. The default value is 9091.
Property Encryption via	AES	The encryption algorithm used by the Openfire server to prevent sensitive data from being exposed. The default option is AES.
Property Encryption Key	SM941training	Specify the AES encryption key. This field is mandatory. You can specify any value in the first field, and then type this value again in the second field.

7. Click **Continue** on the Database Settings screen.

8. Specify a JDBC driver and the connection properties to connect to your database. Update the fields as illustrated below on the Database Settings – Standard Connection screen, and then click **Continue**.



Parameter	Value in this task	Description
Database Driver Presets	Microsoft SQL Server	Select the database type of Service Manager. You can select either SQL server or Oracle.

Parameter	Value in this task	Description
JDBC Driver Class	Do not modify the default value	Value in this field is populated automatically after the database type is selected.

Parameter	Value in this task	Description
Database URL	jdbc:jtds:sqlserver://SM940BETA/SM940;appName=jive	Value in this field is populated automatically after the database type is selected. ■ The default Oracle database URL is `jdbc:oracle:thin:@[host-name]:1521:[SID]`, where [host-name] and [SID] are the actual values of you server. ■ The default Microsoft SQL server database URL is `jdbc:jtds:sqlserver://[host-name]/[database-name];appName=jive`, where [host-name] and [database-name] are the actual values of you server. If you have multiple database instances on a SQL server, refer to the **Named and Multiple SQL Server Instances** section on the Building the Connection URL web page for more information about the database URL configuration.
Username	*<Your Service Manager database user name>*	Specify the user name to log on to the Service Manager database.

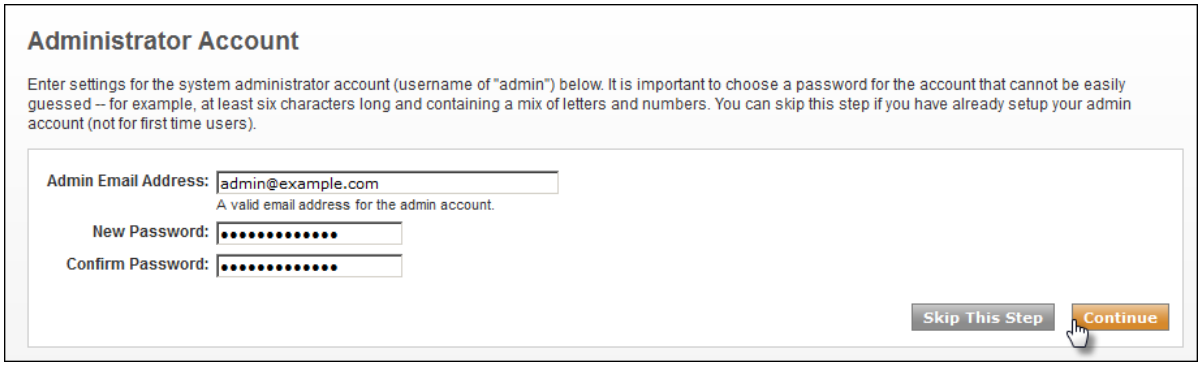
Parameter	Value in this task	Description
Password	*<Your Service Manager database password>*	Specify the password to log on to the Service Manager database. HP suggests that you use a strong password.
Minimum Connections	5	Specify the minimum number of database connections the connection pool should maintain. The default value is 5.
Maximum Connections	100	Specify the maximum number of database connections the connection pool should maintain. The default value is 100.
Connection Timeout	1.0	Specify the time (in days) before connections in the connection pool are recycled. The default value is 1.0.

Note:

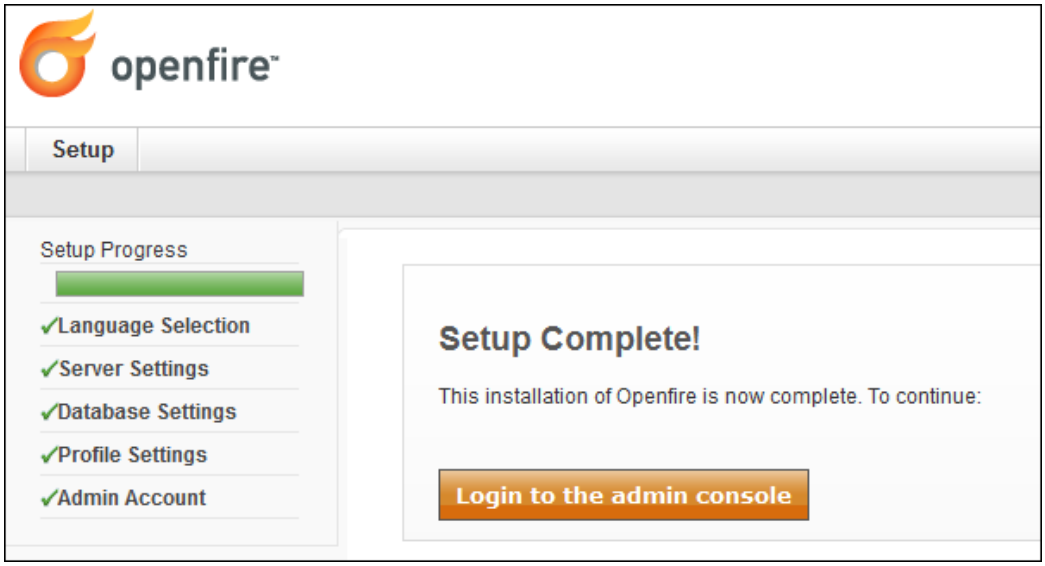
- If you are working with an Oracle database, copy the JDBC driver (for example, ojdbc6.jar) to the <sm9.41.00xx-ChatServer>\lib directory.
- Service Manager Collaboration uses the Service Manager database and inserts a number of Openfire tables into the database. Each table is prefixed with of. Therefore, you need to update the [host-name] with your database host name, and the [database-name] with your Service Manager database name in the Database URL field. It may take a minute to connect to the database.

9. Click **Continue** on the Profile Settings screen.

10. Create the user name and password for your Openfire administrator on the Administrator Account screen. Later you will log on to Openfire as `admin` with this password. Click **Continue** to finish the Openfire installation



11. Your Openfire setup is complete now.



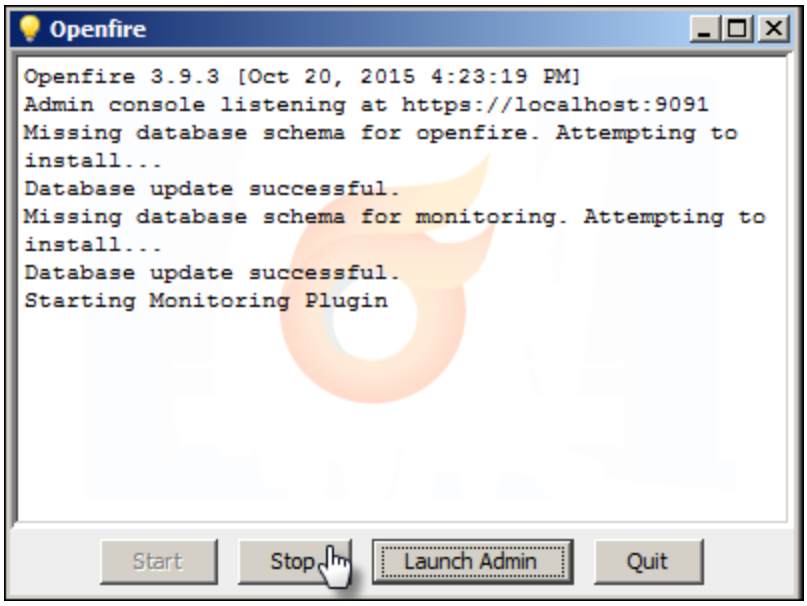
12. Click the **Login to the admin console** button to log in to your Openfire Administration Console.
13. Click **Server** > **Server Manager** > **System Properties**, and then manually add the following properties to the list:

Property name	Description	Property value
xmpp.client.processing.threads	The thread pool of the woker pool in Openfire to process incoming XMPP requests. The default value is 32, which can be increased to 254 for heavy loads.	32
lyncplugin.brokerService.memoryLimit	The total memory size of the message queues between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value for heavy message queues.	1024
lyncplugin.brokerService.policy.memoryLimit	The memory size of each message queue between Collaboration and the Lync server when you are integrating Collaboration with Lync. You can increase the value when the message queue is considered as a bottleneck.	64

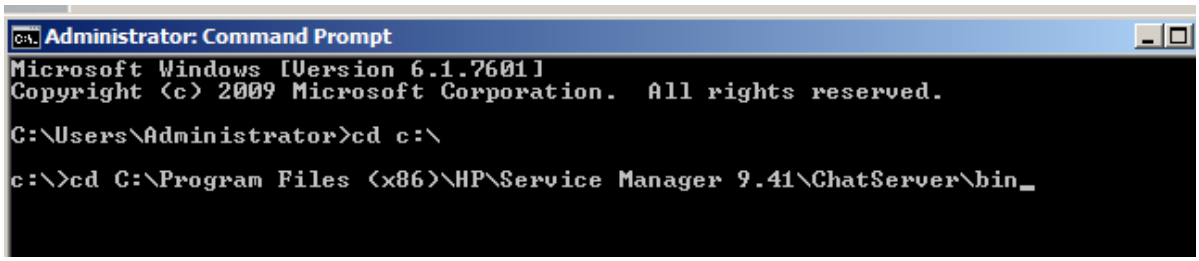
14. Click **Group Chat** > **Group Chat Settings** > **conference** > **Other Settings**.
15. In the **Conversation Logging** section, update the values as follows:

Property	Description	Value
Flush interval (seconds)	The two parameters control the frequency of inserting the chat log to the database. The recommended value is 3000 records per 30s.	30
Batch size		3000

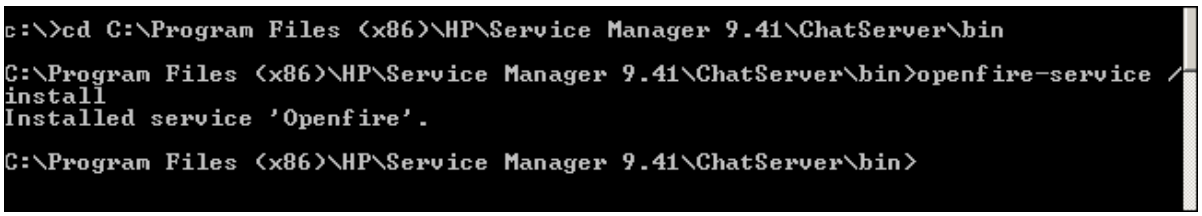
16. Click **Save Settings**.
17. Close the web browser tab.
18. Click **Stop** on the Openfire screen.



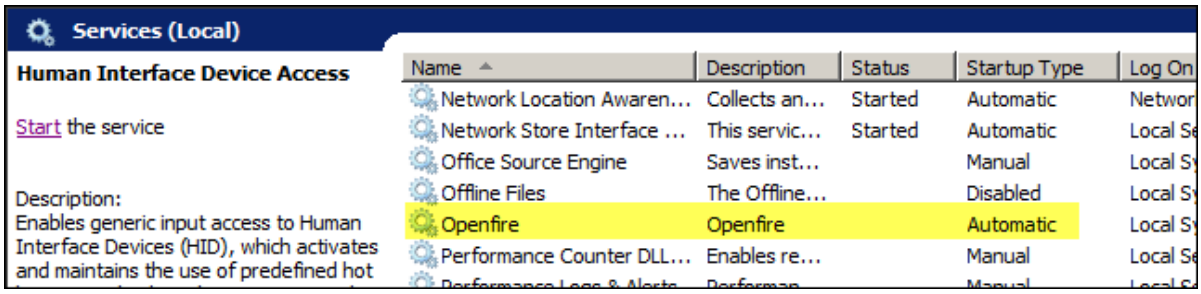
19. To install Openfire as a Windows service, open a DOS command prompt and change the directory to C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\bin.



20. Run the **openfire-service /install** command to install the Openfire service.



21. Go to Windows Services and see the new Openfire service has been installed. Do not start the service as you will make further changes to Openfire in the next task.



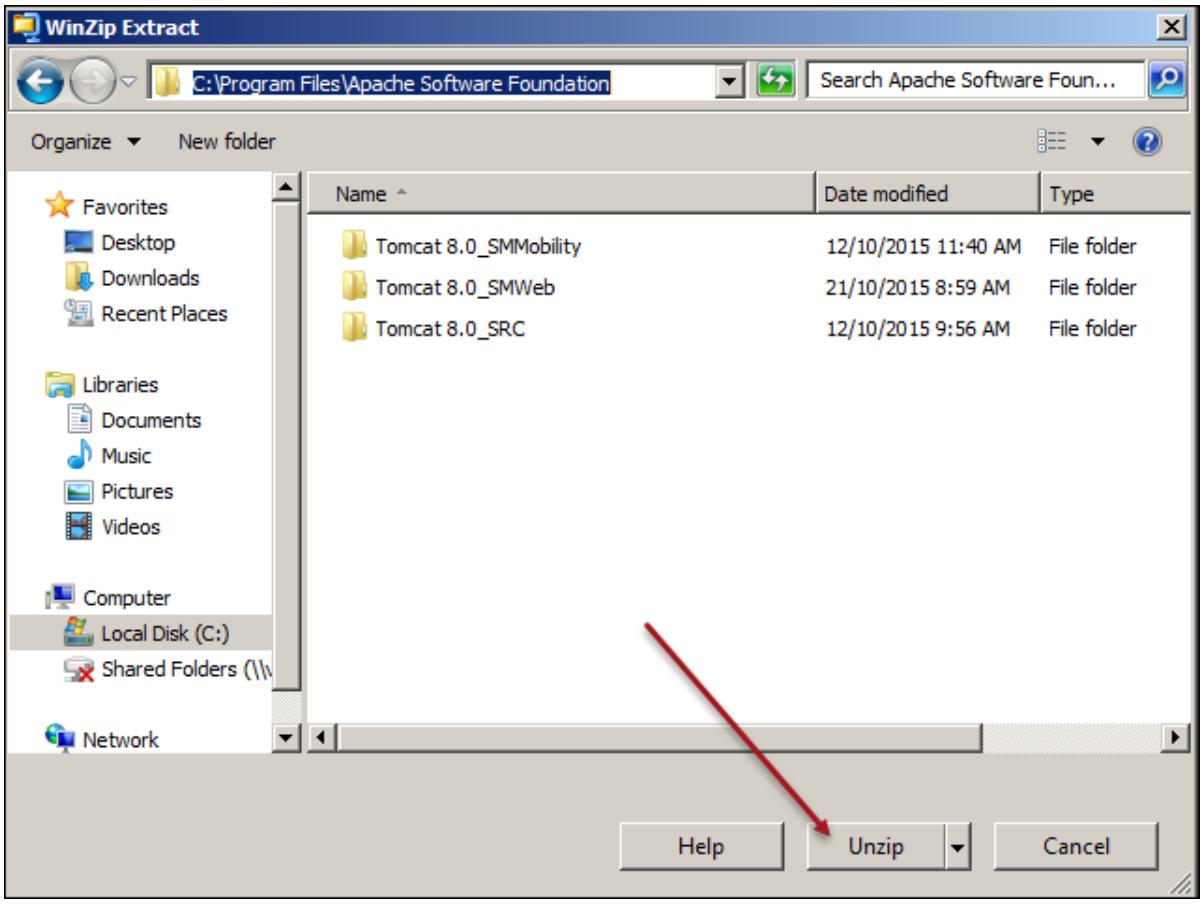
Task 6: Deploy the Apache 2.2 HTTP server

In this task, you will deploy and configure the Apache 2.2 HTTP server for Service Manager Collaboration.

Note: The deployment instructions in this document are for a sample OpenSSL Apache server. If you have profound Apache knowledge, you can also customize the Apache server by following your own business rules.

Follow these steps:

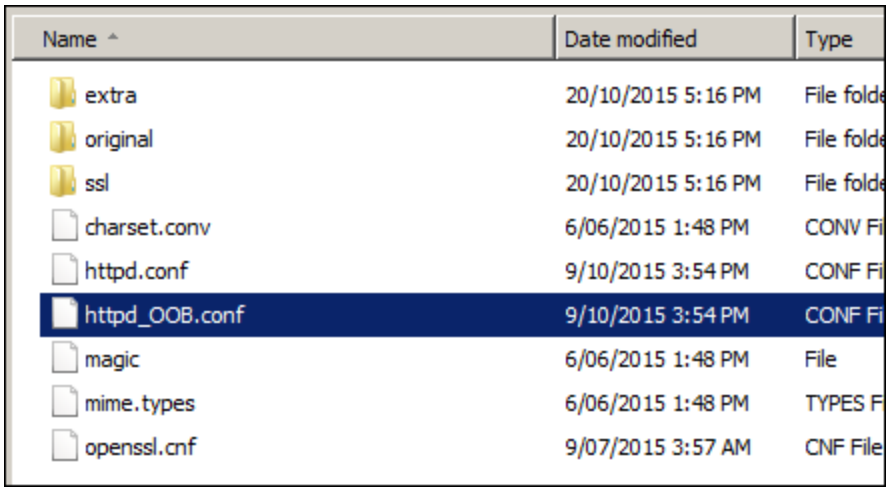
1. Download Apache with OpenSSL (httpd-2.2.31-x64-r3.zip) from http://www.apachehaus.com/cgi-bin/download.plx, and then extract the zip file to the C:\Program Files\Apache Software Foundation directory with an archive management program.



This unzip process creates a new C:\Program Files\Apache Software Foundation\Apache22 directory.

2. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\conf folder.

3. Copy the httpd.conf file and save it as httpd_OOB.conf.



4. Open the httpd.conf file with a text editor.

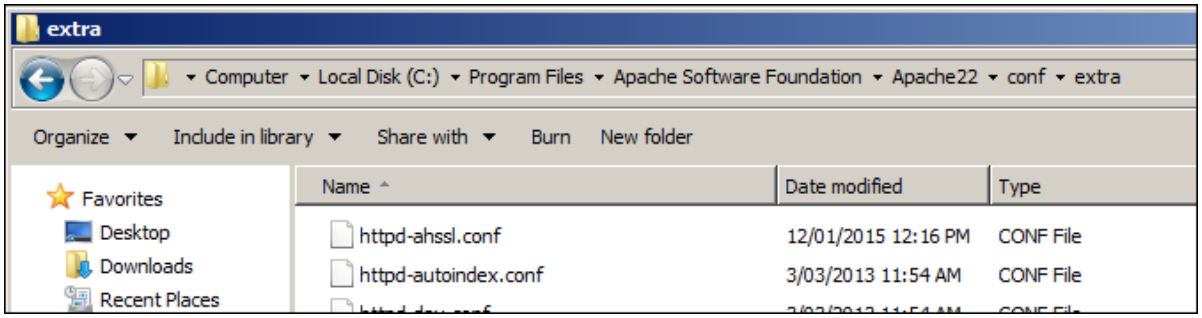
5. Locate the SRVROOT parameter.

6. Set SRVROOT to where you installed Apache. In this task, update the directory for SRVROOT to C:\Program Files\Apache Software Foundation\Apache22.

```
37
38  Define SRVROOT "C:/Program Files/Apache Software Foundation/Apache22"
39  ServerRoot "${SRVROOT}"
40
```

7. Save your changes and close the httpd.conf file.

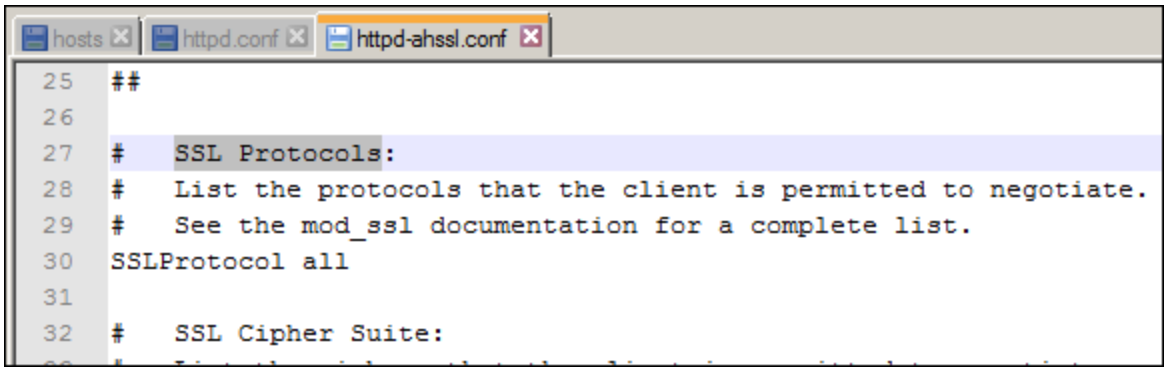
8. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\conf\extra directory.



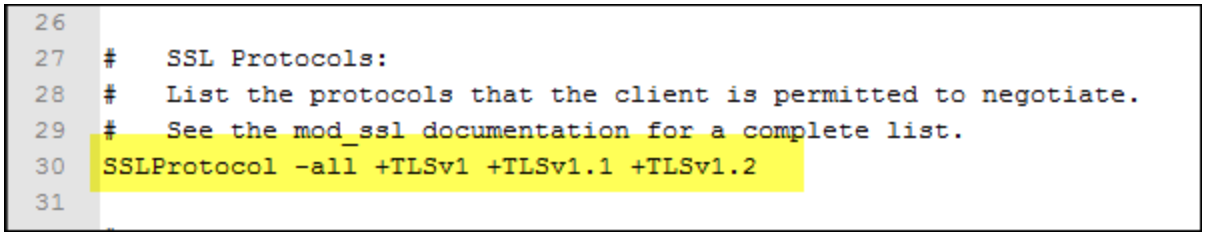
9. Copy the httpd-ahssl.conf file and save it as httpd-ahssl_OOB.conf.

10. Open httpd-ahssl.conf with a text editor.

11. Locate the `SSL Protocols` section.



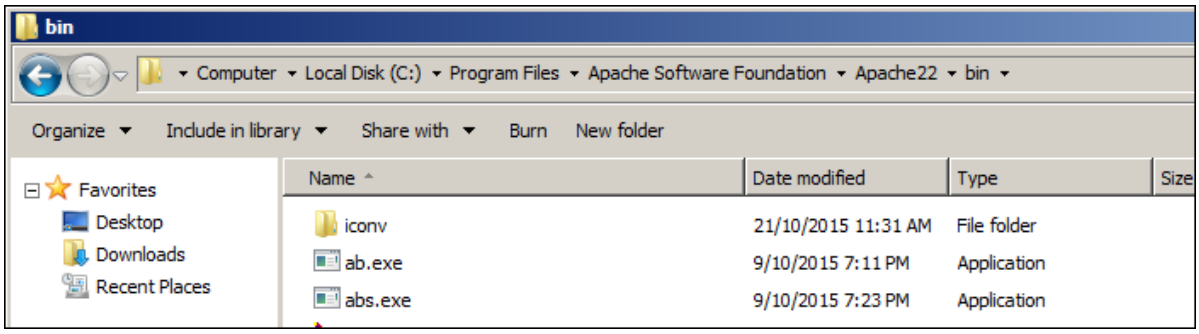
12. Change `SSLProtocol all` to `SSLProtocol -all +TLSv1 +TLSv1.1 +TLSv1.2` so that only TLS v1.0, TLS v1.1, and TLSv1.2 are enabled on the Apache server.



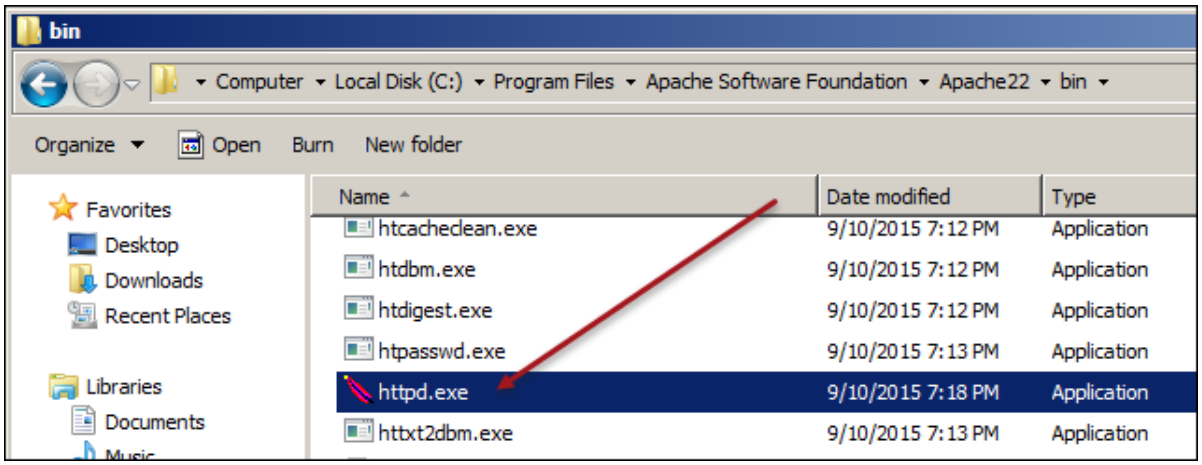
Tip: For more information about the SSL configuration, see http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslprotocol.

13. Save your changes and close the httpd-ahssl.conf file.

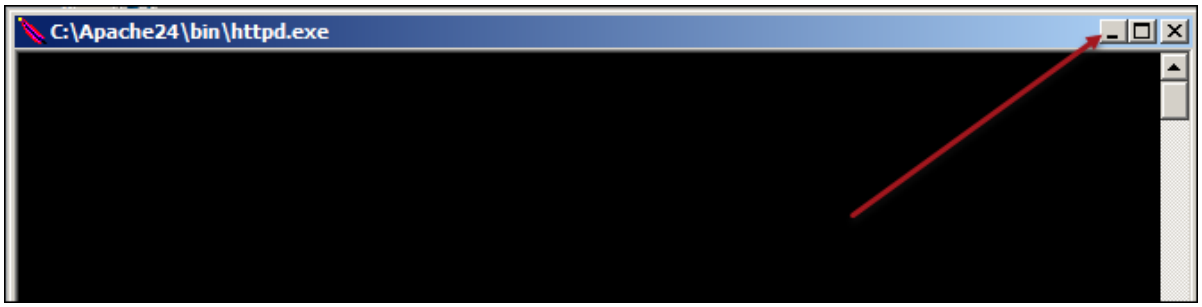
14. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\bin folder.



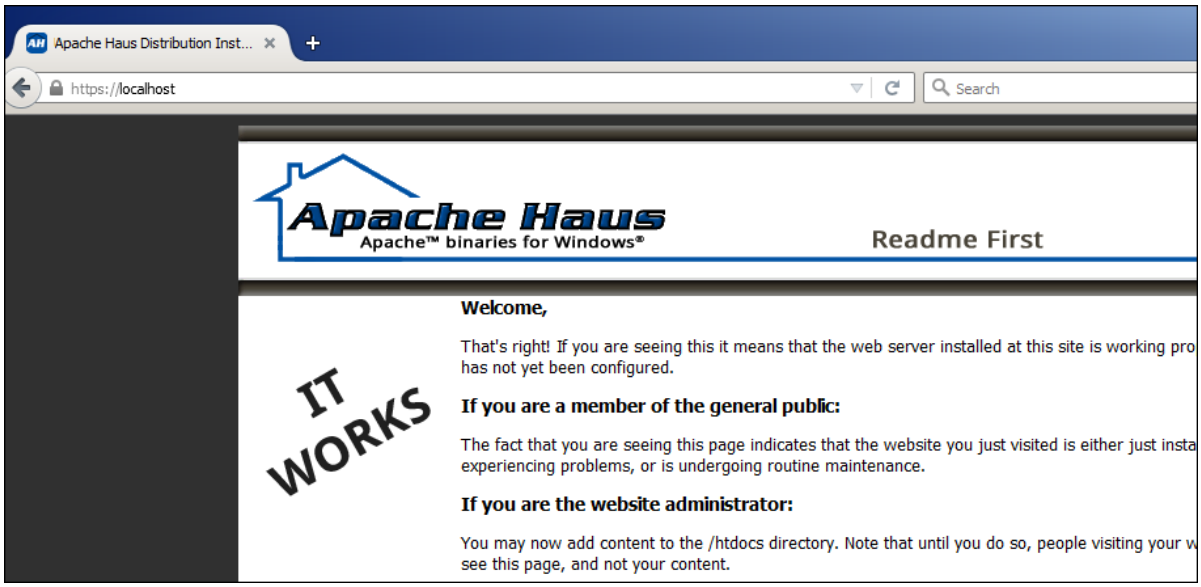
15. Double-click httpd.exe to start the Apache server.



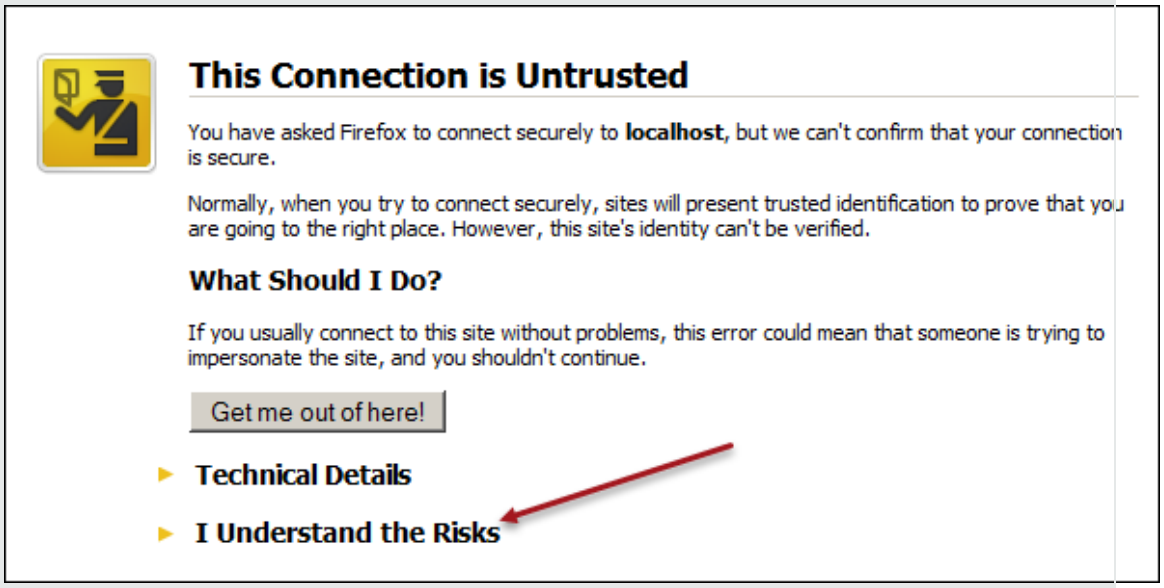
The httpd.exe window opens. Click the minimize button to minimize this window.



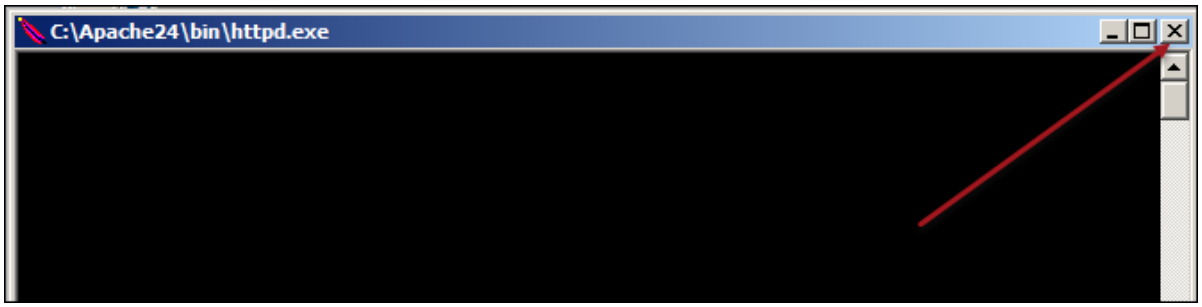
16. In your web browser, type `https://localhost` and press Enter. The system opens the following page and indicates SSL is enabled successfully.



Note: If the system displays the following screen, click **I Understand the Risks** and proceed.

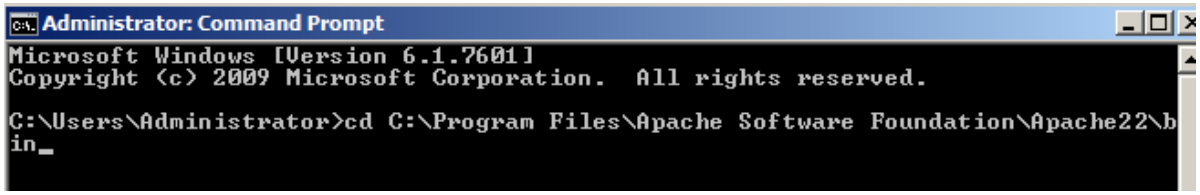


17. Close the browser.
18. Close the Apache window.

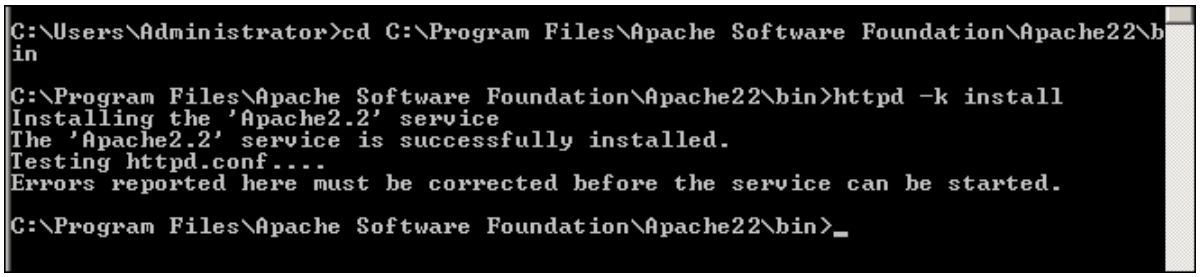


The steps below is to install Apache as a Windows service.

19. Open a DOS command prompt and change the directory to C:\Program Files\Apache Software Foundation\Apache22\bin.

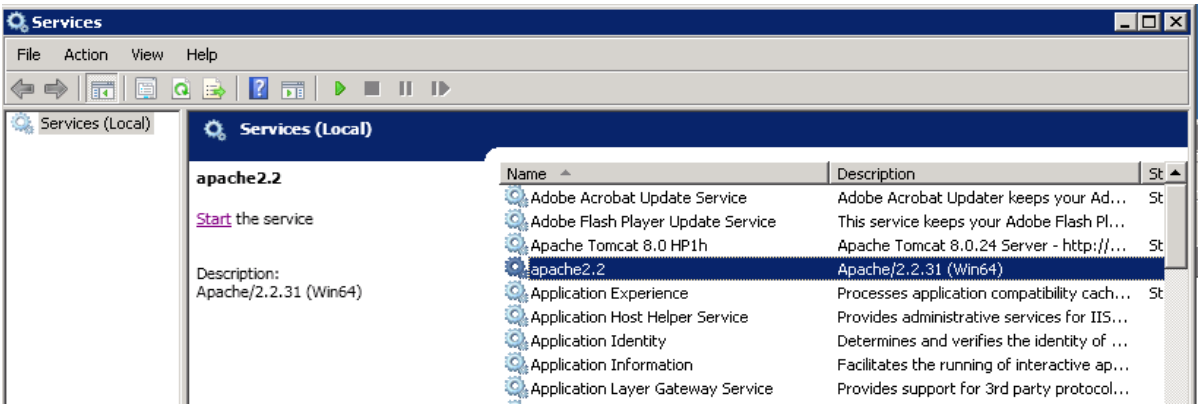


20. Run the **httpd –k install** command to install the Windows service.



Note: If you see an error here, navigate to the logs directory and check the error.log file. Depending upon the error, you may need to reapply the steps above. To start Apache from the command line to verify whether the error still exists, type **httpd –k start**.

21. Go to Windows Services and see the new Apache2.2 service has been installed. Start the service.



Task 7: Enable Apache 2.2 reverse proxy

In this task, you will enable the reverse proxy in Apache to protect the sensitive information of Openfire, such as the IP address, ports, and so on.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\conf folder.
2. Open the httpd.conf file with a text editor.

   The next few steps describe how to uncomment a number of `LoadModule` codes in the httpd.conf file.

3. Locate `proxy_module`.

```
#LoadModule lua_module modules/mod_lua.so
#LoadModule macro_module modules/mod_macro.so
LoadModule mime_module modules/mod_mime.so
#LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_html_module modules/mod_proxy_html.so
```

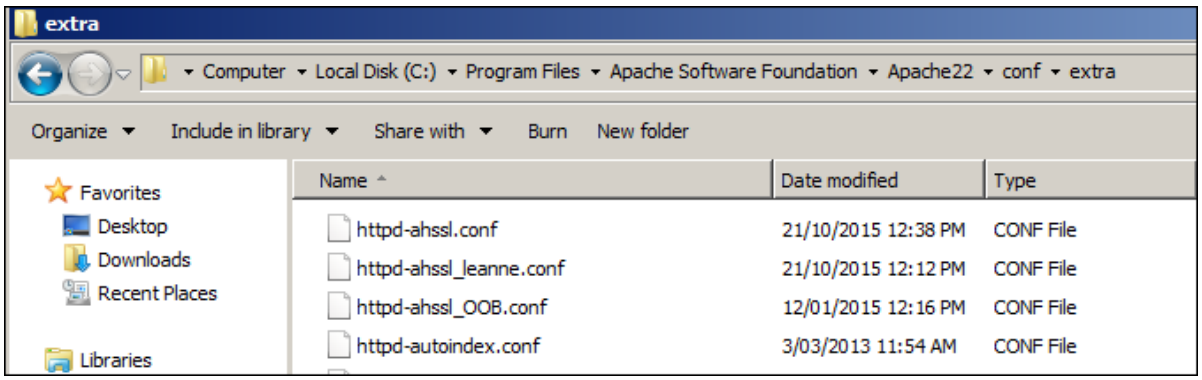
4. Uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

```
109  LoadModule negotiation_module modules/mod_negotiation.so
110  LoadModule proxy_module modules/mod_proxy.so
111  LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
112  #LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
113  LoadModule proxy_connect_module modules/mod_proxy_connect.so
114  LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
115  LoadModule proxy_http_module modules/mod_proxy_http.so
```

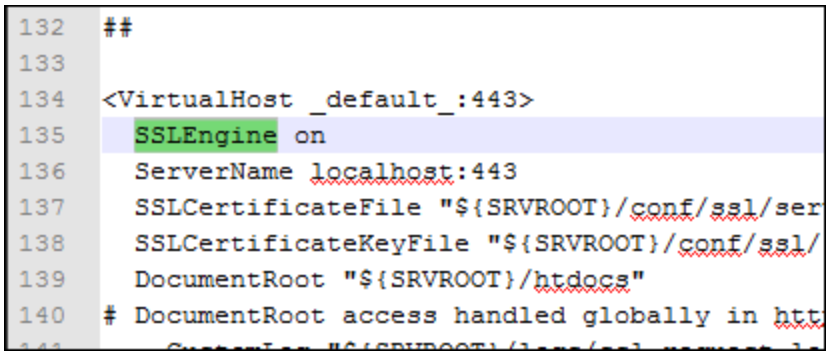
5. Save your changes and close the httpd.conf file.

6. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\conf\extra directory.



7. Open the httpd-ahssl.conf file with a text editor.

8. Locate `SSLEngine`.

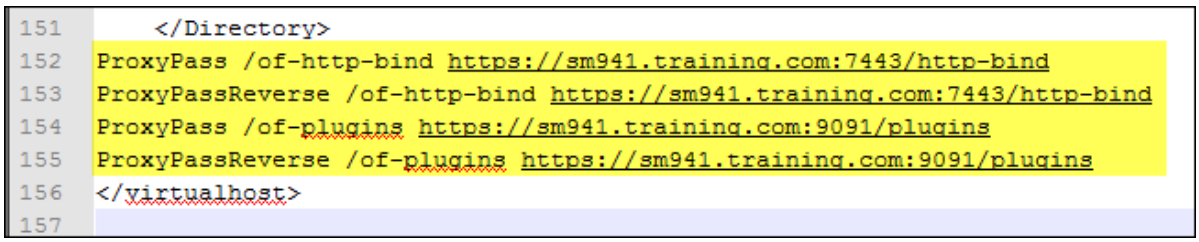


9. Add the following lines below `SSLEngine on`.

```
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

10. Add the following lines below `</Directory>` but before `</virtualhost>`.

```
ProxyPass /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPass /of-plugins https://sm941.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm941.training.com:9091/plugins
```



`/of-http-bind` is the path of the Openfire HTTP binding (also known as BOSH) reverse configuration, whereas `/of-plugins` is the identifier of the Openfire plugin directory. These two parameters are used on the SM collaboration setting page later.

> **Note:** You can change `sm941.training.com` to your host name. In addition, 9091 is the secure admin console port for the chat server. If you changed this port from the default value during the chat server installation, you need to update the port number here.

11. Locate `SSLEngine` again.

```
157
158  <VirtualHost *:443>
159    SSLEngine on
160    ServerName serverone.tld:443
161    SSLCertificateFile "${SRVROOT}/
```

12. Add the following codes below `SSL Engine on`.

```
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

13. Add the following lines below `</Directory>` but before `</virtualhost>`.

```
ProxyPass /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPass /of-plugins https://sm941.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm941.training.com:9091/plugins
```

```
174     </Directory>
175  ProxyPass /of-http-bind https://sm941.training.com:7443/http-bind
176  ProxyPassReverse /of-http-bind https://sm941.training.com:7443/http-bind
177  ProxyPass /of-plugins https://sm941.training.com:9091/plugins
178  ProxyPassReverse /of-plugins https://sm941.training.com:9091/plugins
179  </virtualhost>
180
```

14. Locate `SSLEngine` one more time.

```
180
181  <VirtualHost *:443>
182    SSLEngine on
183    ServerName servertwo.tld:443
184    SSLCertificateFile "${SRVROOT}/conf.
185    SSLCertificateKeyFile "${SRVROOT}/c
```

15. Add the following lines below `SSL Engine on`.

```
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

16. Add the following lines below `</Directory>` but before `</virtualhost>`.

```
ProxyPass /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPassReverse /of-http-bind https://sm941.training.com:7443/http-bind
ProxyPass /of-plugins https://sm941.training.com:9091/plugins
ProxyPassReverse /of-plugins https://sm941.training.com:9091/plugins
```

```
196     Require all granted
197     </Directory>
198 ProxyPass /of-http-bind https://sm941.training.com:7443/http-bind
199 ProxyPassReverse /of-http-bind https://sm941.training.com:7443/http-bind
200 ProxyPass /of-plugins https://sm941.training.com:9091/plugins
201 ProxyPassReverse /of-plugins https://sm941.training.com:9091/plugins
202 </virtualhost>
203
```

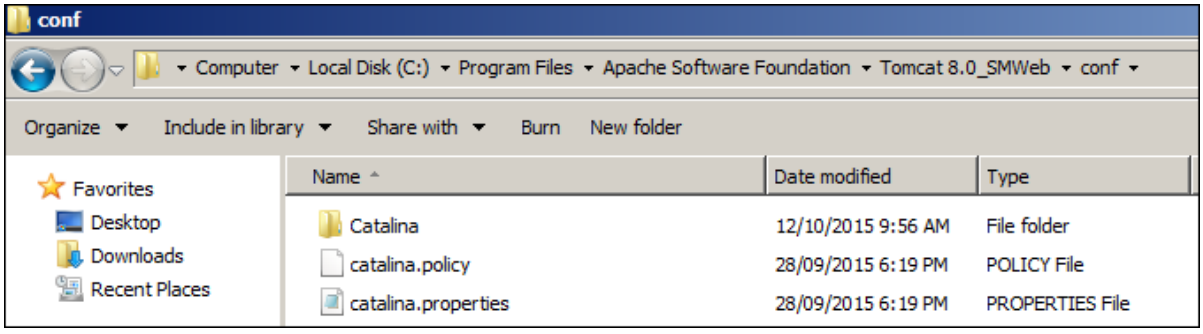
17. Save your changes and close the httpd-ahssl.conf file.

Task 8: Connect Apache 2.2 to Tomcat

In this task, you will set up Apache to connect to Tomcat through the AJP port by using `mod_jk`. Consequently, Secure Sockets Layer (SSL) is open by default. You can perform this step instead of enable full SSL on the Service Manager environment.

Follow these steps:

1. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\conf directory.



2. Open the server.xml file with a text editor.

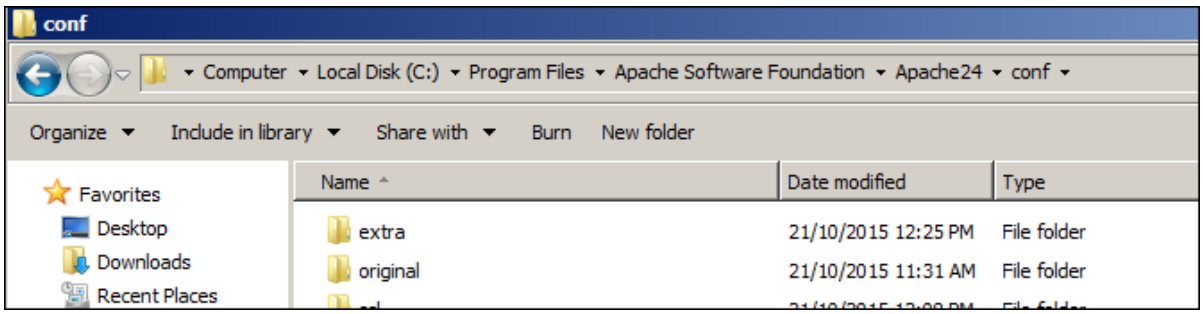
3. Locate `AJP 1.3 Connector`, and then confirm the port is set to `8009`.

```
88      -->
89
90      <!-- Define an AJP 1.3 Connector on port 8009 -->
91      <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
92
```

Note: If the `AJP 1.3 connector` is set to another port, record that port number as you will need it later in this task.

4. Close the server.xml file.

5. Navigate to the C:\Program Files\Apache Software Foundation\Apache24\conf directory.



6. Open the httpd.conf file with a text editor.

7. Locate `proxy_balancer`.

```
110  LoadModule proxy_module modules/mod_proxy.so
111  LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
112  #LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
113  LoadModule proxy_connect_module modules/mod_proxy_connect.so
114  LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
115  LoadModule proxy_http_module modules/mod_proxy_http.so
```

8. Uncomment the following line:

```
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
```

```
110  LoadModule proxy_module modules/mod_proxy.so
111  LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
112  LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
113  LoadModule proxy_connect_module modules/mod_proxy_connect.so
114  LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
115  LoadModule proxy_http_module modules/mod_proxy_http.so
```

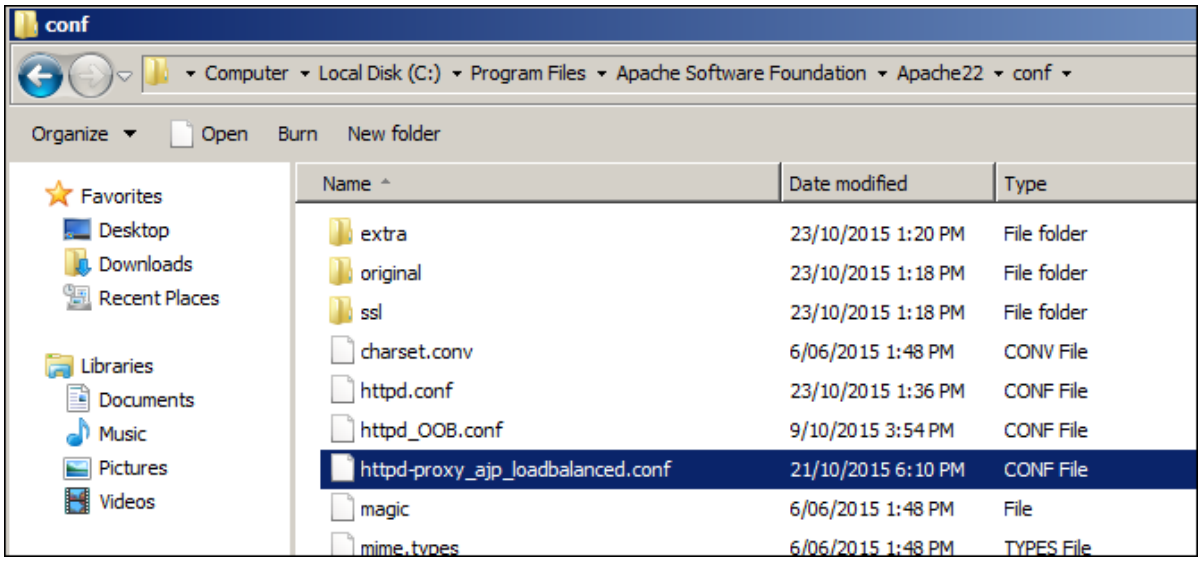
9. Browse to the end of the file, and then add the following line:

   ```
   Include conf/httpd-proxy_ajp_loadbalanced.conf
   ```

```
528  </IfModule>
529
530  Include conf/httpd-proxy_ajp_loadbalanced.conf
531
```

10. Save your changes and close the httpd.conf file.

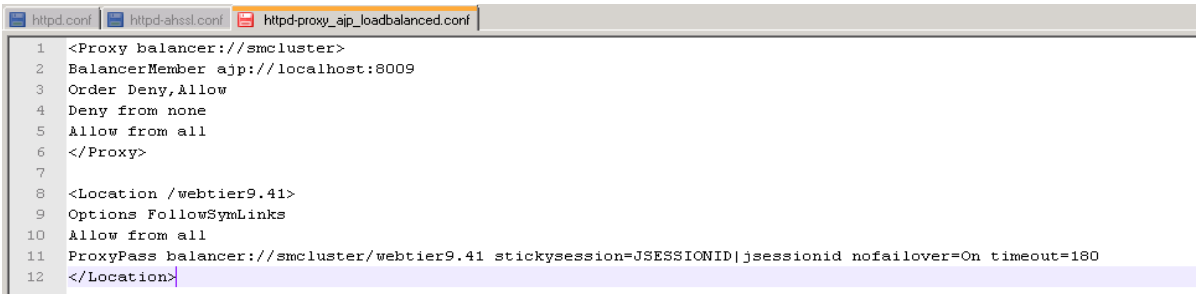
11. Navigate to the C:\Program Files\Apache Software Foundation\Apache22\conf directory, and then create a new file called httpd-proxy_ajp_loadbalanced.conf.



Copy and paste the following codes to the httpd-proxy_ajp_loadbalanced.conf file:

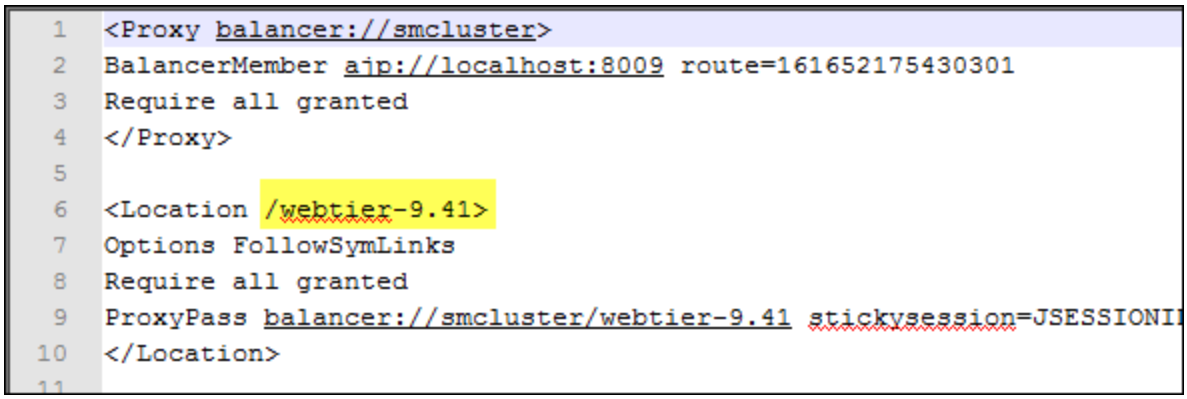
```
<Proxy balancer://smcluster>
BalancerMember ajp://localhost:8009
Order Deny,Allow
```

```
Deny from none
Allow from all
</Proxy>

<Location /webtier-9.41>
Options FollowSymLinks
Allow from all
ProxyPass balancer://smcluster/webtier-9.41stickysession=JSESSIONID|jsessionid
nofailover=On timeout=180
</Location>
```



Note: You must paste `ProxyPass balancer://smcluster/webtier-9.41 stickysession=JSESSIONID|jsessionid nofailover=On timeout=180` in one line as illustrated.

12. This script is set up for the Service Manager webtier in the webtier-9.41 directory (see line 6). If your webtier has another name, update this httpd-proxy_ajp_loadbalanced.conf file with the actual name of your webtier.

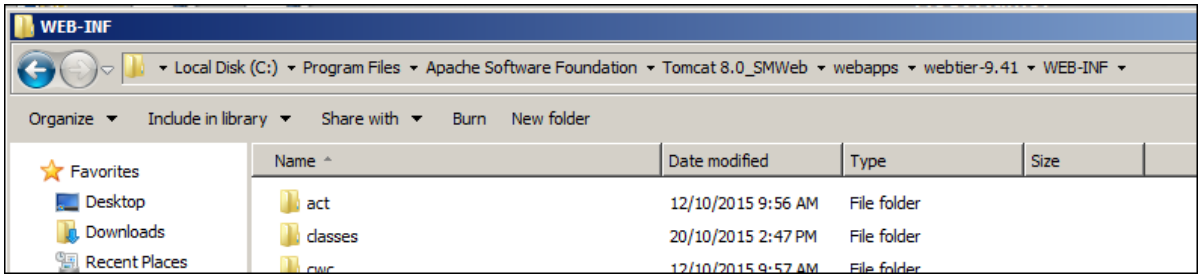


13. Step 3 instructs you to check the `AJP 1.3 Connector` port in the server.xml file. If this port is 8009,

continue with the next step. If the AJP 1.3 Connector is on another port, update line 2 in this httpd-proxy_ajp_loadbalanced.conf file with the other port number.

```
1  <Proxy balancer://smcluster>
2  BalancerMember ajp://localhost:8009 route=161652175430301
3  Require all granted
4  </Proxy>
5
6  <Location /webtier-9.41>
7  Options FollowSymLinks
8  Require all granted
9  ProxyPass balancer://smcluster/webtier-9.41 stickysession=JSESSIONI
10 </Location>
```

14. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\webapps\webtier-9.41\WEB-INF directory.



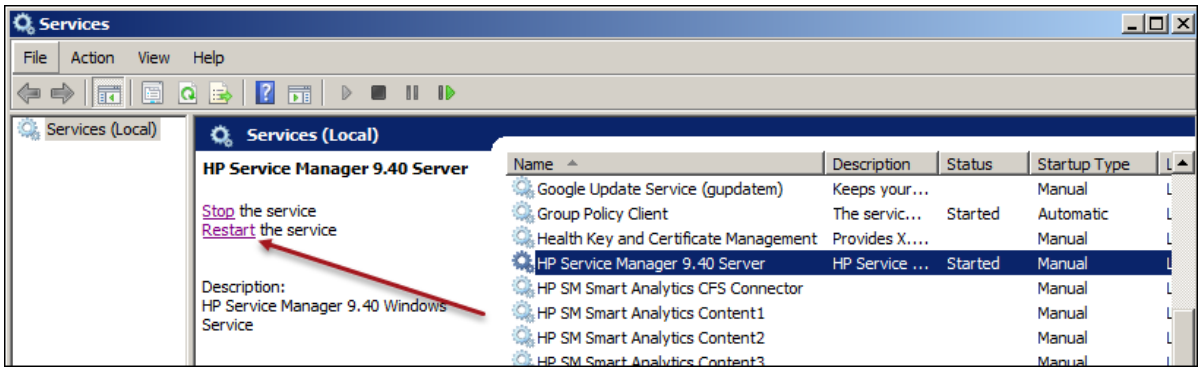
15. Open the web.xml file with a text editor.

16. Locate the `secureLogin` parameter and set it to `true`.

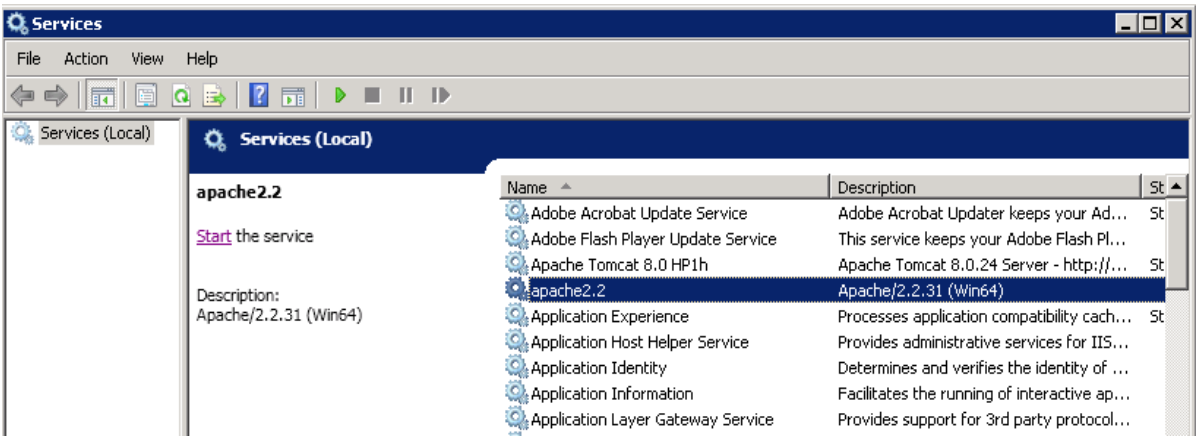
```
129  -->
130  <context-param>
131    <param-name>secureLogin</param-name>
132    <param-value>true</param-value>
133  </context-param>
134  <context-param>
135    <param-name>sslPort</param-name>
```

17. Save your changes and close the web.xml file.

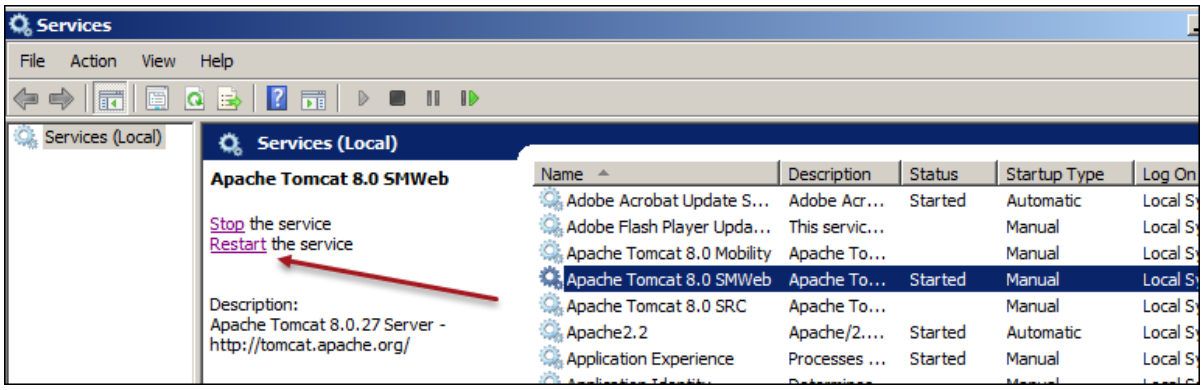
18. Go to Windows Services and restart the **HP Service Manager 9.40 Server** service.



19. Restart the **Apache 2.2** service.

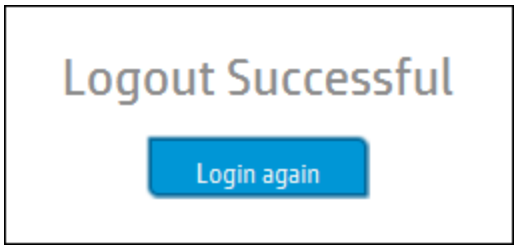


20. Restart the **Tomcat 8.0 SMWeb** service.

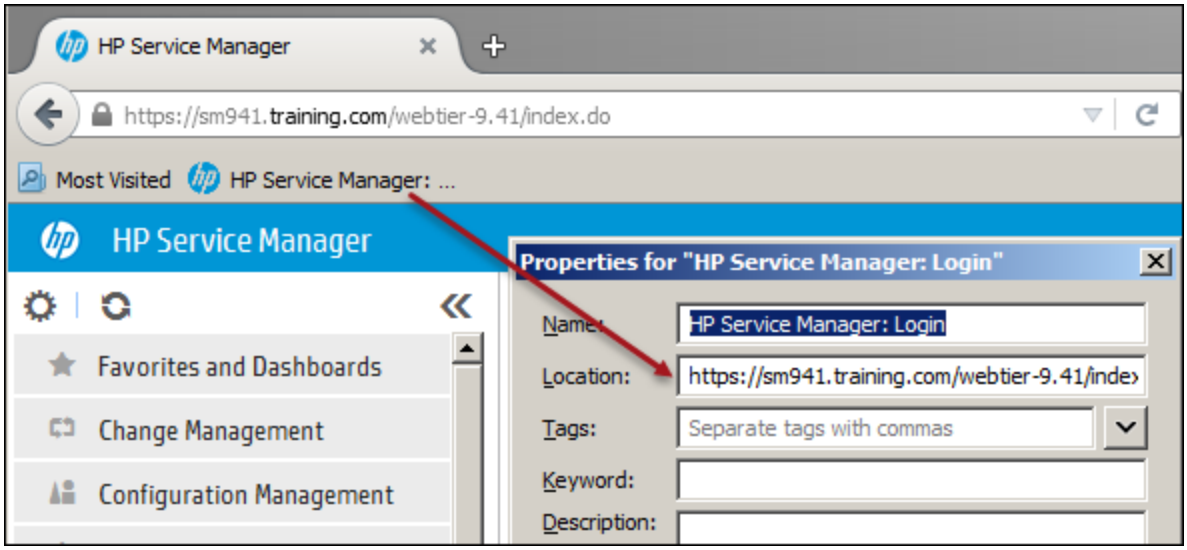


21. Access https://sm941.training.com/webtier-9.41/index.do, and then log on to Service Manager as a system administrator. The system displays the administrator's To Do Queue.

If you are directed to the Logout Successful page, there may be some issues with the LW-SSO setup. Check all your files from the previous tasks and then try again.



22. Note that from now on, you need to use HTTPS and the fully qualified domain name (FQDN) in the URL when logging on to Service Manager web client. You may wish to update the bookmarks in the bookmark toolbar.



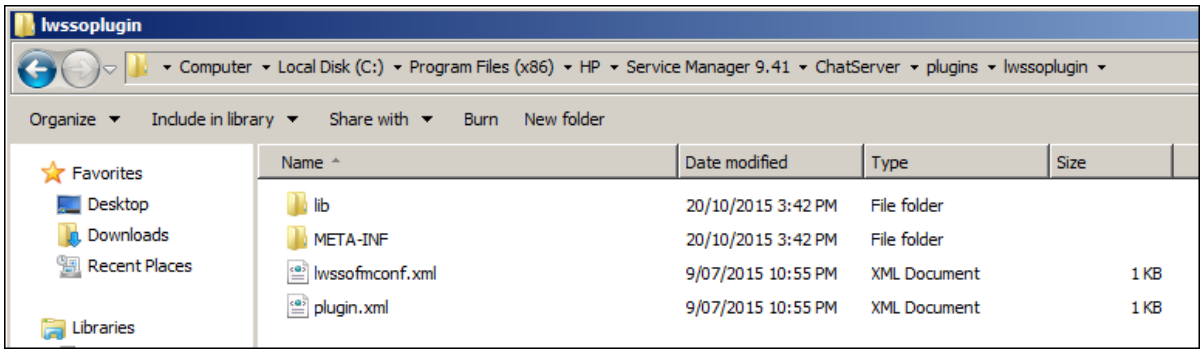
23. Log out from Service Manager.

Task 9: Configure LW-SSO for the chat server

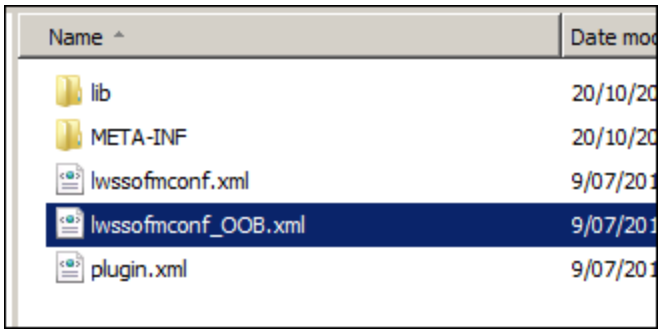
In this task, you will set up LW-SSO for the SM Collaboration Openfire service.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\plugins\lwssoplugin folder.



2. Copy the lwssofmconf.xml file and save it as lwssofmconf_OOB.xml.



3. Open lwssoconf.xml with a text editor.

4. Locate the `domain` parameter and set it to `training.com`.

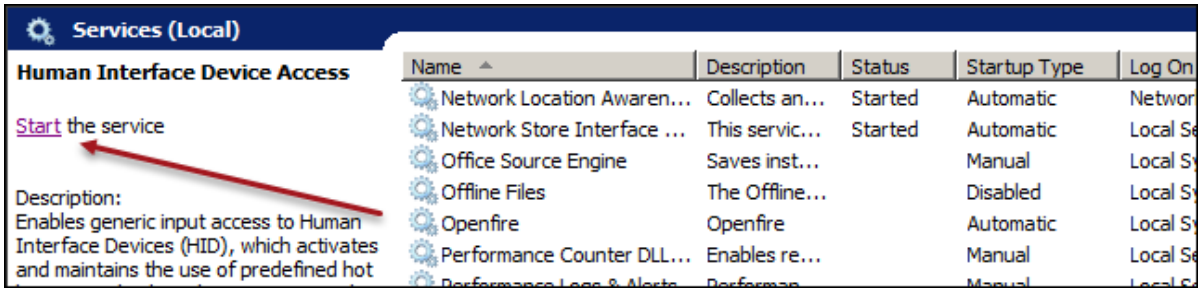
```
11          <in-lwsso>
12              <lwssoValidation>
13              <domain>training.com</domain>
14                  <crypto cipherType="symmetricBlockCipher" engineName="AES"
15                      paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
16                      initString="This is a shared secret passphrase"></crypto>
17              </lwssoValidation>
18          </in-lwsso>
```

5. Locate the `initString` value and set this to `SM941training`.

```
12                  <lwssoValidation>
13                  <domain>training.com</domain>
14                      <crypto cipherType="symmetricBlockCipher" engineName="AES"
15                          paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
16                          initString="SM941training"></crypto>
17                  </lwssoValidation>
18              </in-lwsso>
19          </service>
20      </inbound>
21      <outbound/>
```

6. Save your changes and close the lwssofmconf.xml file.

7. Go to Windows services and start the **Openfire** Windows service.



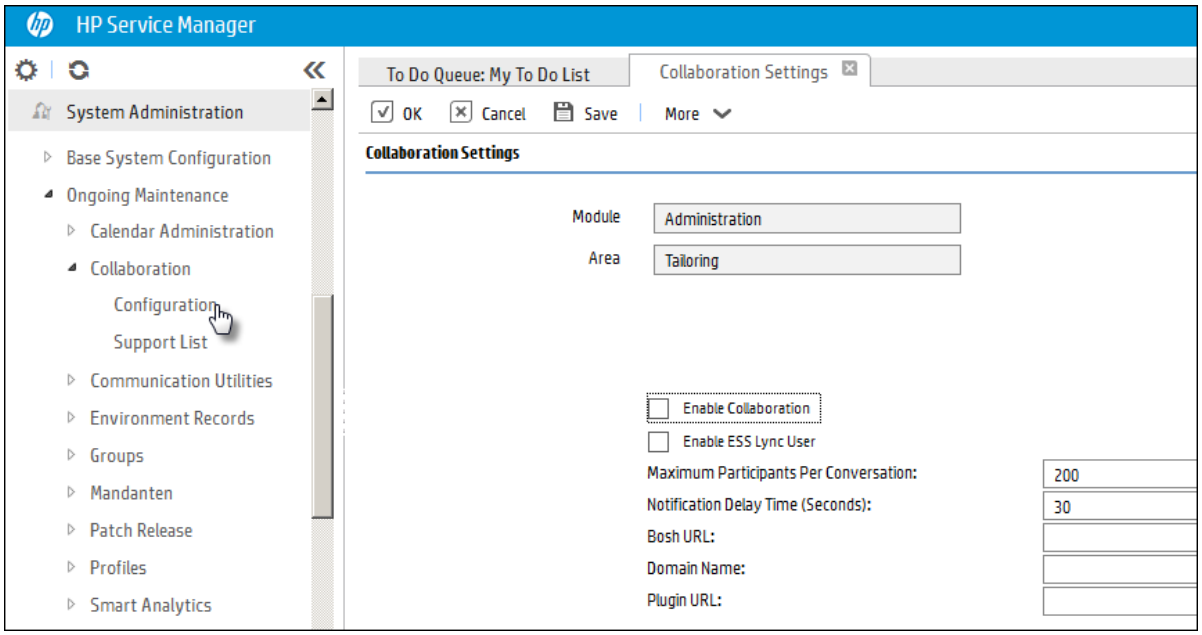
Task 10: Enable Service Manager Collaboration

By default, the HP Service Manager Collaboration feature is disabled after applying Service Manager 9.41 web tier. In this task, you will log on to Service Manager and set up the Collaboration Configuration.

Follow these steps:

1. Access https://sm941.training.com/webtier-9.41/index.do in your web browser, and then log on to Service Manager as a system administrator.

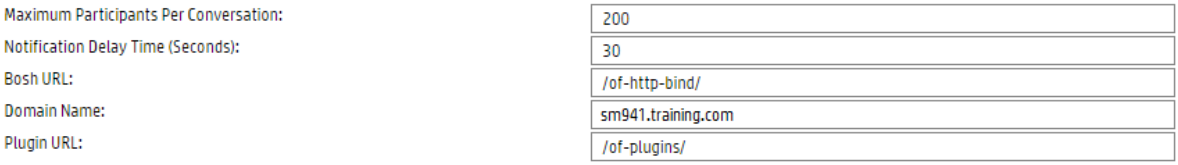
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.



3. Select the **Enable Collaboration** check box to enable Service Manager Collaboration.

4. (Optional) Select the **Enable ESS Lync User** check box so that the Lync users can join Collaboration conversations by using Lync.

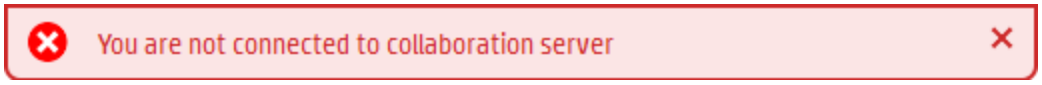
5. Specify the values in the following fields as illustrated:



Field	Value in this task	Description
Maximum Participants Per Conversation	200	The maximum number of participants in a conversation. The default value is 200.

Field	Value in this task	Description
Notification Delay Time (Seconds)	30	The maximum time that an online participant has to wait to receive the live conversation notifications. The default value is 30. Notification delay is disabled if this value is set to 0 or minus.
BOSH URL	`/of-http-bind/`	The HTTP binding (also known as BOSH) path for Openfire to send XMPP messages. In the sample reverse proxy configurations in Task 5: Enable Apache reverse proxy, this path is `/of-http-bind/`. **Note:** ■ Type the path in Apache reverse proxy configurations in this field. Do not type the actual URL. ■ Do not omit the slashes.
Domain Name	sm941.training.com	Domain name of the Openfire server.
Plugin URL	/of-plugins/	The Openfire plugin URL. In the sample reverse proxy configurations in Task 5: Enable Apache reverse proxy, this value is `/of-plugins/`. **Note:** ■ Type the identifier as specified in your reverse proxy configurations in this field. Do not type the actual URL. ■ Do not omit the slashes.

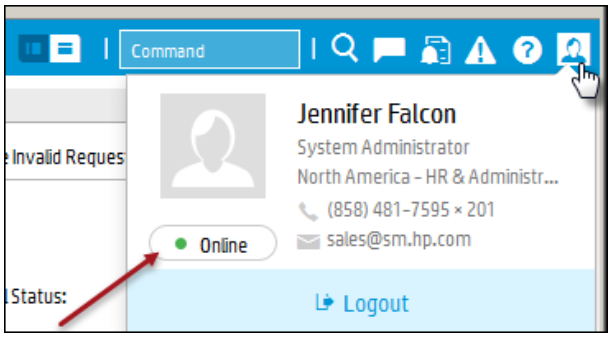
6. Click **Save** and **OK**. It may take a minute for the configurations to take effect.
7. Log out of the web client, and then log on as the system administrator again.
8. When you log in, you should not see the following Collaboration error message on your screen:



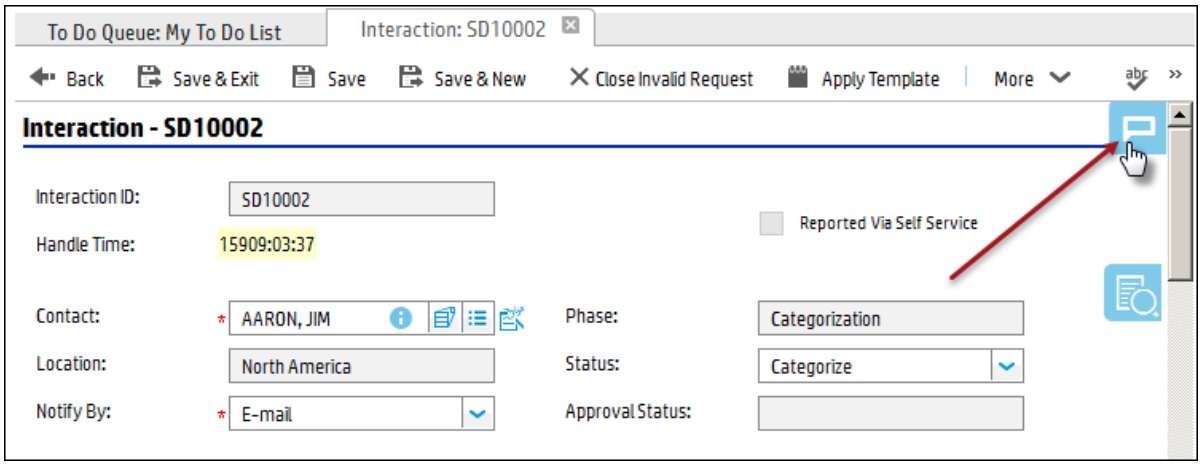
If the system displays this error message, check all your settings and then refer to "Troubleshooting - Failed to connect to the Collaboration server" on page 69.

9. The Chat Notification botton is displayed on the top-right corner of the Service Manager UI. You are not able to click it because the chat notifications are not available yet.

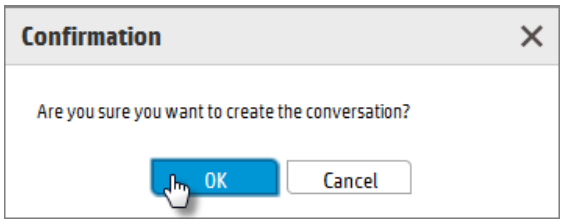
10. Click the User Information button to show your User Basic Information Card. Your presence status is now **Online**.



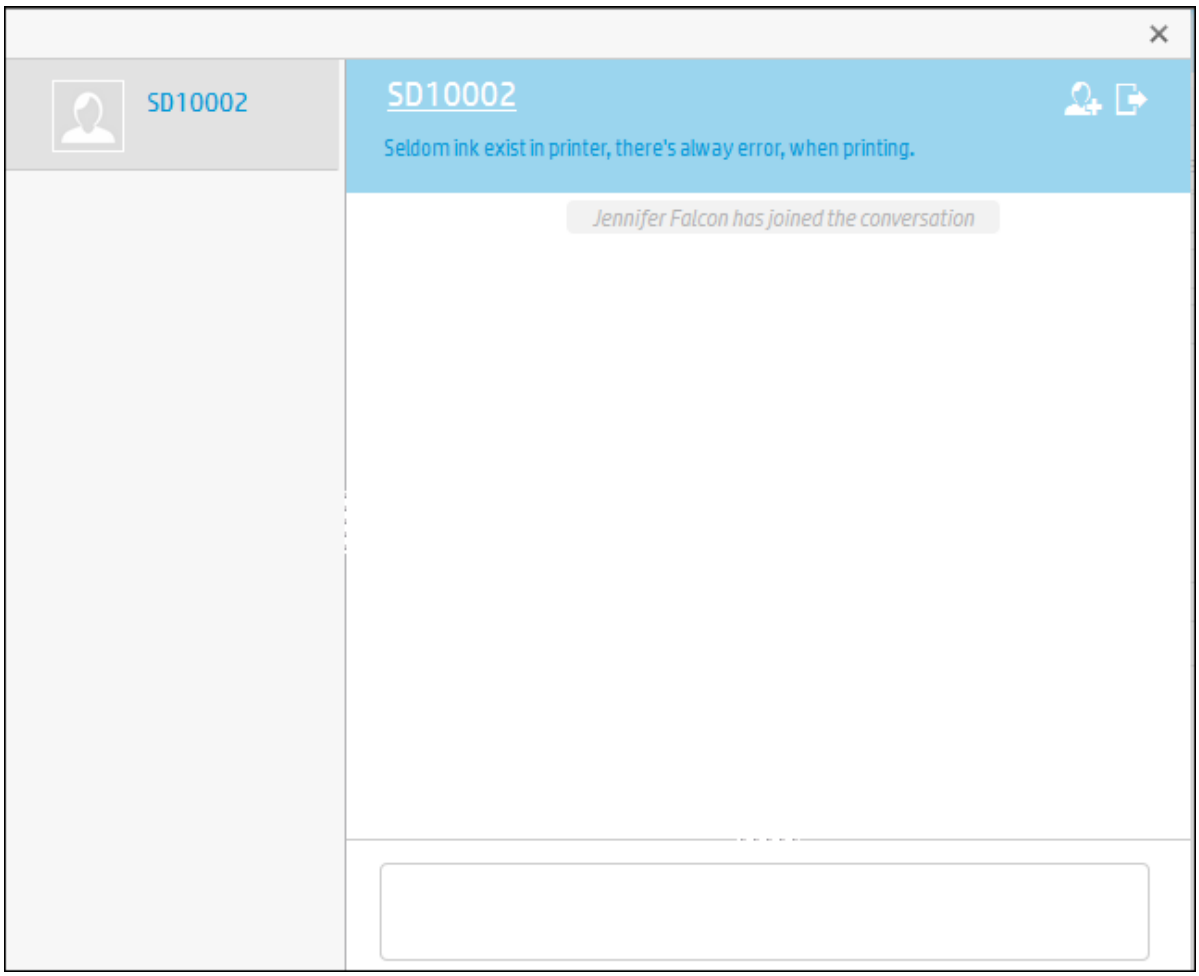
11. Open an interaction record. The **Start Conversation** button floats on the upper-right corner of the detailed view of this record.



12. Click the **Start Conversation** button, and then and then click **OK** in the system confirmation dialog.



13. A conversation starts with the record's ID and title displayed on the header of the conversation window.



Congratulations! You have successfully installed Service Manager Collaboration!

(Optional) Task 11: Integrate with Microsoft Office Lync

HP Service Manager Collaboration provides an out-of-the-box Lync plugin and a Lync agent to integrate with Microsoft Office Lync. When you start a conversation in Service Manager Collaboration, the Lync plugin that is embedded in the Openfire server monitors all the messages. If a participant does not log on to the Openfire server, the Lync plugin will use the participant's email address as his/her Lync account and then send the message to the Lync server. If the user is available to chat, the Lync agent will launch a conversation with the right user, and then forward the message to him/her on Lync. After the Lync user replies, the Lync Agent will push this message back to the Lync plugin. Consequently, the Lync plugin will poll the in-coming Lync message and then forward it to all the other users in the Collaboration conversation.

The following diagram illustrates a sample message exchange architecture between Service Manager Collaboration and the Lync server:

Note:
Lync users cannot start a conversation with Service Manager Collaboration. Instead, they can be invited to Collaboration conversations only.

In this task, you will integrate Service Manager Collaboration with Microsoft Office Lync.

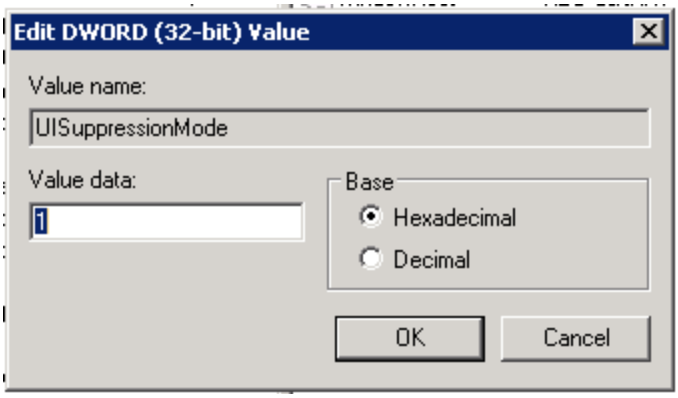
Follow these steps:

1. Download and install Microsoft .NET Framework 4.5 from Microsoft Download Center.
2. Download and install Microsoft Lync 2013 from Microsoft Download Center. Service Manager Collaboration integrates with Microsoft Lync 2013 only.
3. Sign in Lync by using an IT operator's Lync account. This account transfers the communication between the Openfire server and the Lync server, and hence must be effective and timeliness.
4. Click Microsoft Office Lync **Options** > **Personal**, and then select **None** from the **Personal information manager** drop-down menu. Save your changes and then sign out.
5. Create the new UISuppressionMode Windows Registry value.

a. Open Windows Registry Editor, and then navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync.

b. Right-click Lync, and then click **New** > **DWORD (32-bit)** value to create a new registry value.

c. Set the new value name to UISuppressionMode, and then set the value data to 1.



d. Click **OK**, and then close the Windows Registry Editor.

6. Encrypt the Lync account and update openfire.xml.

a. Stop the Openfire server.

b. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\conf directory, and then open openfire.xml with a text editor.

c. Locate the `<lyncIntegration>` section.

```
<lyncIntegration>
  <enabled>false</enabled>
  <auth>
    <!-- Put plain lync user name and password here, it will be automatically encrypted
         after server startup and encrypted="true" will be added to the userName and password
         elements. When you change your Lync userName or password, you must remove encrypted="true" and
         replace the encrypted string with the new plain string.
         -->
    <userName/>
    <password/>
  </auth>
  <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

d. Update the `<lyncIntegration>` section as follows:

```
<lyncIntegration>
                <enabled>true</enabled>
                <auth>
                <!-- Put plain lync user name and password here, it will be automatically
encrypted
                after server startup and encrypted="true" will be added to the userName a
password
                elements. When you change your Lync userName or password, you must remove
                encrypted="true" and replace the encrypted string with the new plain stri
-->
                <userName><YourLyncAccountName></userName>
                <password><YourLyncPassword></password>
                </auth>
                <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

Where *<YourLyncAccountName>* and *<YourLyncPassword>* must be same as that used in step 3.

```
<lyncIntegration>
  <enabled>true</enabled>
  <auth>
    <!-- Put plain lync user name and password here, it will be automatically encrypted
         after server startup and encrypted="true" will be added to the userName and password
         elements. When you change your Lync userName or password, you must remove encrypted="true" and
         replace the encrypted string with the new plain string.
         -->
    <userName>trainingmster@hpe.com<userName/>
    <password>samplepassword<password/>
  </auth>
  <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

Note: When the IT operator's Lync password is changed, the *<YourLyncPassword>* value in openfire.xml must be changed accordingly.

e. Save your changes and close this file.

f. Start the Openfire server.

See the following screenshot for an example of the encrypted `<lyncIntegration>` section in openfire.xml:

```
<lyncIntegration>
  <enabled>true</enabled>
  <auth>
    <!-- Put plain lync user name and password here, it will be automatically encrypted
         after server startup and encrypted="true" will be added to the userName and password
         elements. When you change your Lync userName or password, you must remove encrypted="true" and
         replace the encrypted string with the new plain string.
          -->
    <userName encrypted="true">B454FAEED3A2E2118C77759EC9E7F4EFA56E051ADB0AB4451A8F8EB2A2357125</userName>
    <password encrypted="true">BA9F849640CAA40D4A69AE8ABCDBAA16</password>
  </auth>
  <startLyncAgent>true</startLyncAgent>
</lyncIntegration>
```

7. Enable Service Manager Collaboration to communicate with the Lync server.

    a. Log on to Service Manager as a system administrator.

    b. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration** to open the Collaboration Settings form.

    c. Select the **Enable Lync User** check box so that the Service Manager Lync users can join Collaboration conversations by using Lync.

Now you can communicate with the Lync users in a Service Manager Collaboration conversation.

Caution: To integrate with Microsoft Office Lync, follow these steps to specify the log on account for the Openfire service before starting it as a standard Windows service:

1. Right-click the Openfire service in the Windows Services window, and then select **Properties**.
2. Click the **Log On** tab.
3. Select **This account**, and then specify the same IT operator's Lync account as that used in step 3.
4. Click **Apply** and **OK**.

(Optional) Task 12: Migrate data from EC

In this task, you will migrate the existing EC data to Service Manager Collaboration by using the Service Manager Migration Tool.

Follow these steps:

1. Navigate to the C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\smcmigration directory, and then double-click startup.bat to start the Service Manager Migration Tool.
2. Select a language, and then click **Start**.
3. Read through the welcome screen, and then click **Next**.
4. Select the database type of your EC server, specify the server name, database name, user name, and password of your EC database, and then click **Next**.

   Note: If you are working with an Oracle database, download the JDBC driver (for example, ojdbc6.jar) from http://www.oracle.com/technetwork/apps-tech/jdbc-112010-090769.html and then copy this file to the <sm9.41.00xx-ChatServer>\smcmigration\lib directory.

5. Select the database type of your Service Manager server, specify the server name, database name, user name, and password of your Service Manager database, and then click **Migrate**.

   The Service Manager Migration Tool displays a status bar that the visualizes the data migration progress.

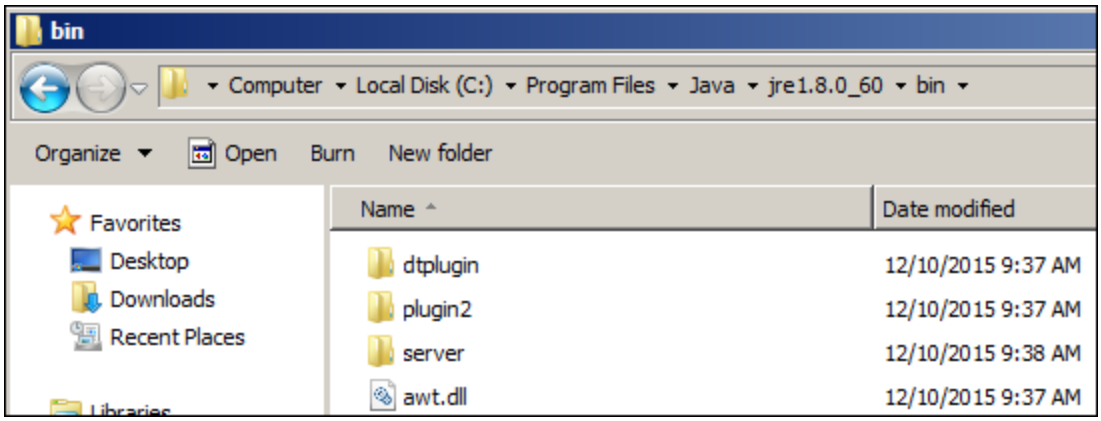
6. When the data migration progress is completed, click **Finish** to quit the tool.

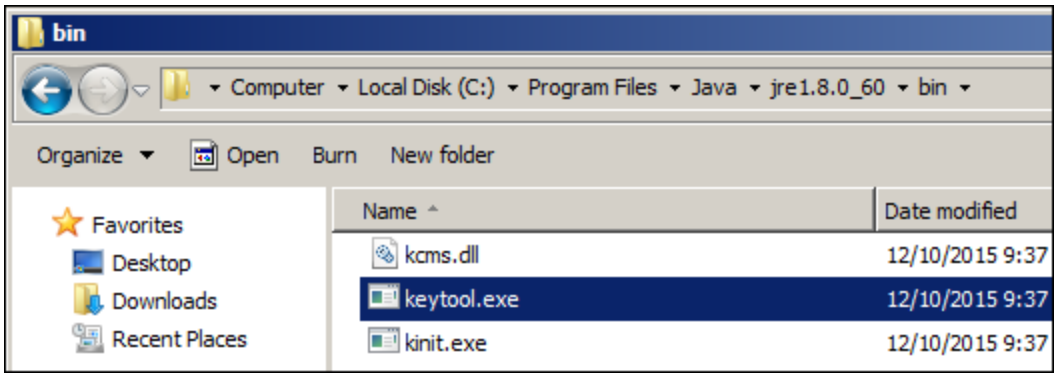
(Optional) Task 13: Configure Tomcat for HTTPS Support

This task is only required if SSL has been configured between Apache and Tomcat. If you are using `mod_jk` for communication between Apache and Tomcat (as described in Task 6: Connect Apache to Tomcat) or proxy balance, then you do not need perform the steps in this task.

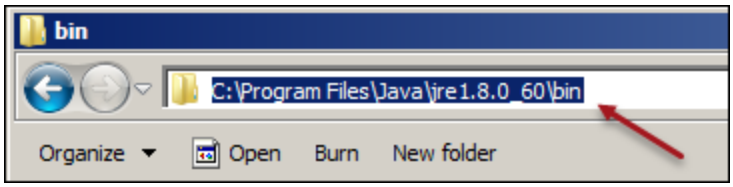
Follow these steps:

1. Navigate to the C:\Program Files\Java\jre1.8.0_60\bin directory, and then confirm keytool.exe is stored in this directory.

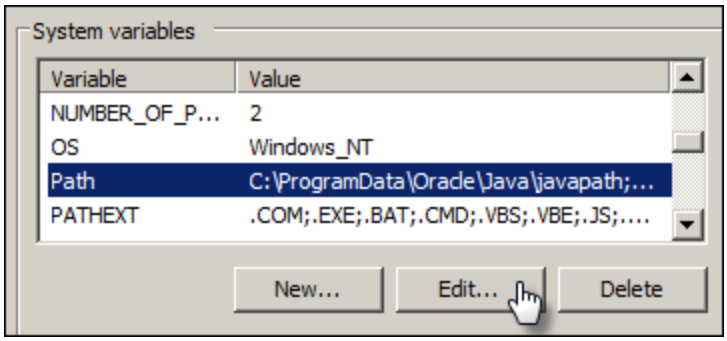




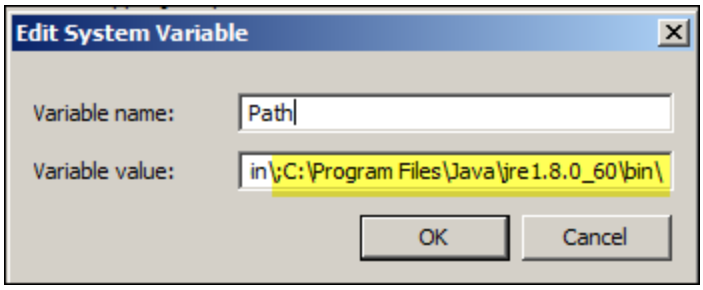
2. Copy the folder location as you will need it in the next steps and keep it in your clipboard or paste it to Notepad.



3. To add this location to the Path environment variable, right-click **Computer** on the Windows desktop and select **Properties**.
4. Click **Advanced system settings**.
5. On the **System Properties** window, click the **Environment Variables** button.
6. Locate the **Path** system variable, and then click **Edit**.



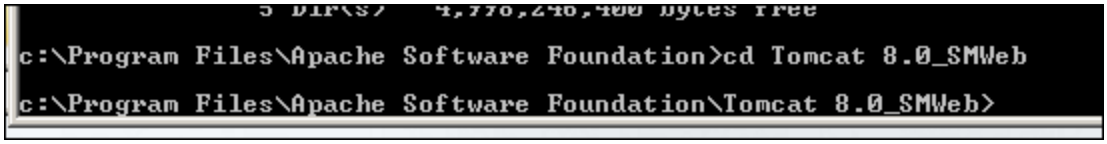
7. Add `;C:\Program Files\Java\jre1.8.0_60\bin\` to the end of the value, and then click **OK**.



8. Click **OK** to close the **Environment Variables** window.

9. Click **OK** to close the **System Properties** window.

10. Open a DOS command prompt and change the directory to C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb.



11. Run the following command to generate the keystore file and set passwords for this keystore file by using the Java keytool:

    keytool -genkey -alias tomcat -keyalg RSA -keystore Chatkeystore -keypass keypasswd -storepass storepasswd -validity 3600

```
c:\Program Files\Apache Software Foundation>cd Tomcat 8.0_SMWeb

c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -genkey -al
ias tomcat -keyalg RSA -keystore Chatkeystore -keypass keypasswd -storepass stor
epasswd -validity 3600_
```

12. The system prompts a series of question, including your first and last name, organizational unit, organization, city, state, and country code. Provide answers to these information and then press Enter, respectively.

13. Finally you are presented with the values for the keytool. Type `yes` and then press Enter.

```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -genkey -al
ias tomcat -keyalg RSA -keystore Chatkeystore -keypass keypasswd -storepass stor
epasswd -validity 3600
Picked up JAVA_TOOL_OPTIONS: -Dfile.encoding=UTF8
What is your first and last name?
  [Unknown]:  Leanne Hanna
What is the name of your organizational unit?
  [Unknown]:  HPSW
What is the name of your organization?
  [Unknown]:  HPE
What is the name of your City or Locality?
  [Unknown]:  Melbourne
What is the name of your State or Province?
  [Unknown]:  VIC
What is the two-letter country code for this unit?
  [Unknown]:  AU
Is CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU correct?
  [no]:  yes
```

The command line returns.

```
  [Unknown]:  AU
Is CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU correct?
  [no]:  yes


c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>
```

14. Run the following command to generate the certificate file for the keystore:

    keytool -export -trustcacerts -alias tomcat -file server.cer -keystore Chatkeystore -storepass storepasswd

```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -export -tr
ustcacerts -alias tomcat -file server.cer -keystore Chatkeystore -storepass stor
epasswd_
```

15. The server.cer certificate file is generated.

```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -export -tr
ustcacerts -alias tomcat -file server.cer -keystore Chatkeystore -storepass stor
epasswd
Picked up JAVA_TOOL_OPTIONS: -Dfile.encoding=UTF8
Certificate stored in file <server.cer>

c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>
```

16. Run the following command to import the self-signed certificate to the Java security folder:

    keytool -import -trustcacerts -alias tomcat -file server.cer -keystore "C:\Program Files\Java\jre1.8.0_60\lib\security\cacerts" -storepass changeit

```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -import -tr
ustcacerts -alias tomcat -file server.cer -keystore "C:\Program Files\Java\jre1.
8.0_60\lib\security\cacerts" -storepass changeit
```

    The system starts to the certificate and prompts you to answer a number of questions.

    Note: The certificate password for cacerts is changeit.

17. The system asks if you trust this certificate. Type `yes` and then press Enter:

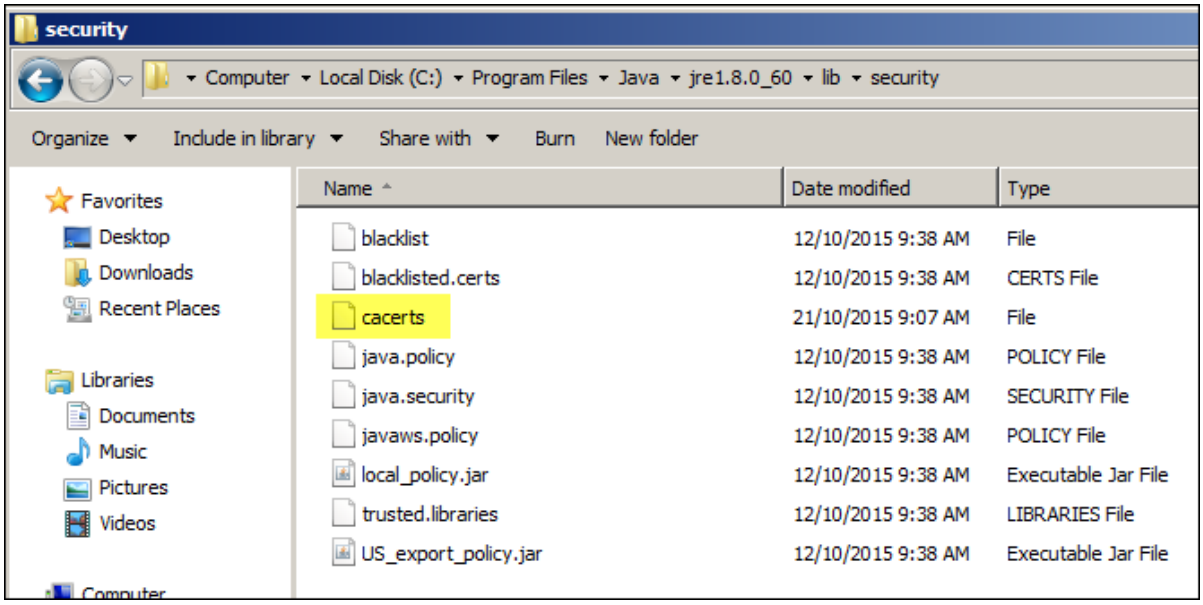
```
c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>keytool -import -tr
ustcacerts -alias tomcat -file server.cer -keystore "C:\Program Files\Java\jre1.
8.0_60\lib\security\cacerts" -storepass changeit
Picked up JAVA_TOOL_OPTIONS: -Dfile.encoding=UTF8
Owner: CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU
Issuer: CN=Leanne Hanna, OU=HPSW, O=HPE, L=Melbourne, ST=VIC, C=AU
Serial number: 52305d8c
Valid from: Wed Oct 21 08:55:28 AEDT 2015 until: Fri Aug 29 07:55:28 AEST 2025
Certificate fingerprints:
         MD5:  EF:89:72:2E:76:44:9C:60:0F:1A:60:BE:EB:18:F5:43
         SHA1: 1F:1C:09:3E:1F:67:17:09:6C:55:D5:C2:01:EA:B7:0D:39:D1:BD:8E
         SHA256: 6F:3C:AE:C0:DC:5B:4E:AE:68:31:1C:B3:5C:A6:06:7C:F9:65:C8:97:EC:
DB:98:7E:B7:EF:94:C6:00:19:98:AE
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 00 F2 CF 80 A5 C5 E5 6E   05 5B DE BB 5B 02 B2 13  .......n.[..[...
0010: 67 9C 5D 65                                        g.]e
]
]

Trust this certificate? [no]:  yes
```

    The certificate is added to the keystore:

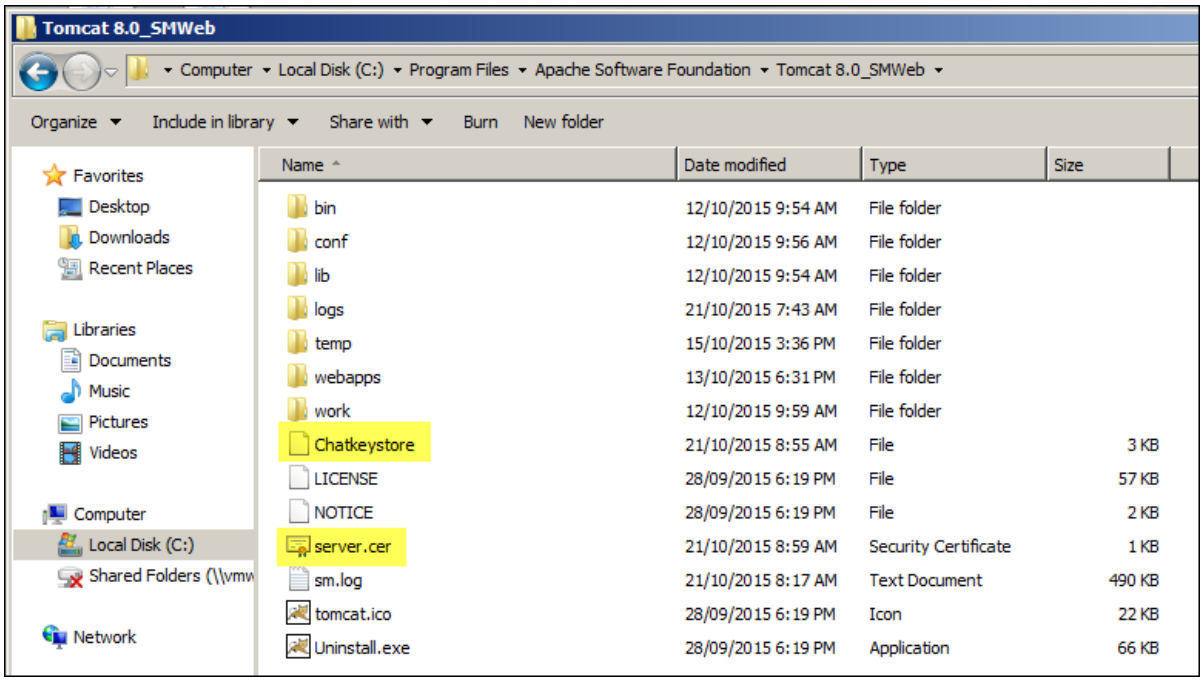
```
Trust this certificate? [no]:  yes
Certificate was added to keystore

c:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb>_
```

18. Close the DOS command window.

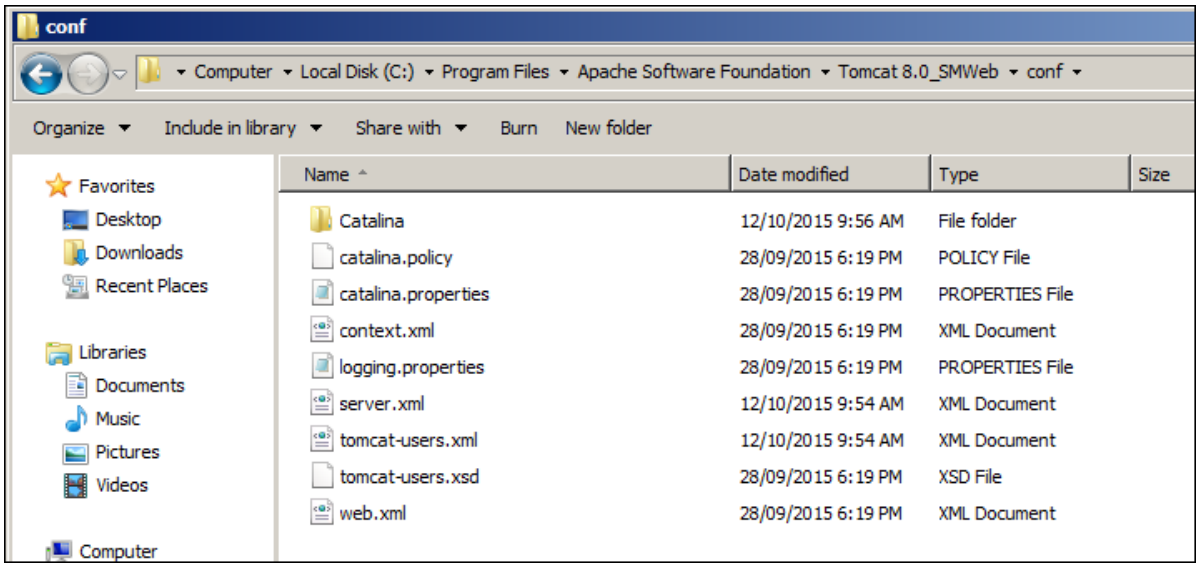
19. Navigate to the C:\Program Files\Java\jre1.8.0_60\lib\security directory to see the cacerts file.



20. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb directory to see the Chatkeystore and server.cer files.



21. Navigate to the C:\Program Files\Apache Software Foundation\Tomcat 8.0_SMWeb\conf directory.



22. Copy the server.xml file and save it as server_OOB.xml.

23. Open the server.xml file with a text editor.

24. Browse to the bottom of the file and insert a few blank lines above `</Host>`.

```
134             Note: The pattern used is equivalent to using pattern="common" -->
135         <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
136                prefix="localhost_access_log" suffix=".txt"
137                pattern="%h %l %u %t &quot;%r&quot; %s %b" />
138
139
140
141       </Host>
142     </Engine>
143   </Service>
```

25. Insert the following codes above `</Host>`:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="Chatkeystore"
keystorePass="storepasswd"/>
```

```
137                pattern="%h %l %u %t &quot;%r&quot; %s %b" />
138
139         <Connector protocol="org.apache.coyote.http11.Http11Protocol"
140         port="8443" minSpareThreads="5" maxSpareThreads="75"
141         enableLookups="true" disableUploadTimeout="true"
142         acceptCount="100" maxThreads="200"
143         scheme="https" secure="true" SSLEnabled="true"
144         clientAuth="false" sslProtocol="TLS"
145         keystoreFile="Chatkeystore"
146         keystorePass="storepasswd"/>
147
148
149       </Host>
150     </Engine>
151   </Service>
```

26. Save your changes and close the server.xml file.

Troubleshooting

This section provides information that can assist you in troubleshooting issues that are associated with Service Manager Collaboration.

Troubleshooting - Openfire restart failure

Description

Failed to restart the Openfire chat server.

Root cause

Some related processes still exist.

Solution

Check the openfire.exe process, the LyncAgent.exe process, and the Lync.exe process in Windows Task Manager when restarting the Openfire chat server. If these processes still exist after the Openfire service is stopped, you must end these processes manually before starting the Openfire chat server.

> **Note:**
> The LyncAgent.exe process and the Lync.exe process exist only when you have integrated HP Service Manager Collaboration with Microsoft Office Lync.

Troubleshooting - Microsoft Lync 2013 client memory leak

Description

Microsoft Lync 2013 client memory increases continuously and never decreases.

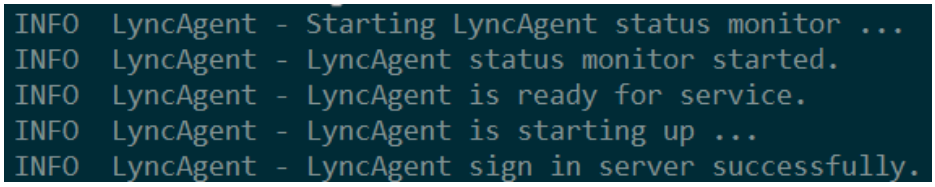
Root cause

This is a Lync 2013 client known issue.

Solution

Follow these steps to restart Lync and the Lync agent when the Lync.exe process's memory exceeds 2G. Do not change the order when ending the process manually.

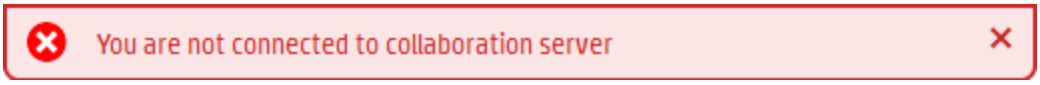
1. End the Lync.exe process in Windows Task Manager.
2. End the LyncAgent.exe process in Windows Task Manager.
3. The LyncAgent.exe process restarts automatically.
4. Wait for several minutes, and then check <ChatServer_HOME>\lyncagent\log.txt to make sure that it contains the log information as illustrated in the following screen shot :



Troubleshooting - Failed to connect to the Collaboration server

Description

When you log on to the Service Manager web client by using https, the system displays the following error message:



Root cause

The Openfire service is not started, or Service Manager Collaboration is not properly configured.

Solution

See the following suggestions:

- "Ensure the Openfire Windows service is started"
- "Verify the Service Manager Collaboration configurations"
- "Reinstall Openfire"

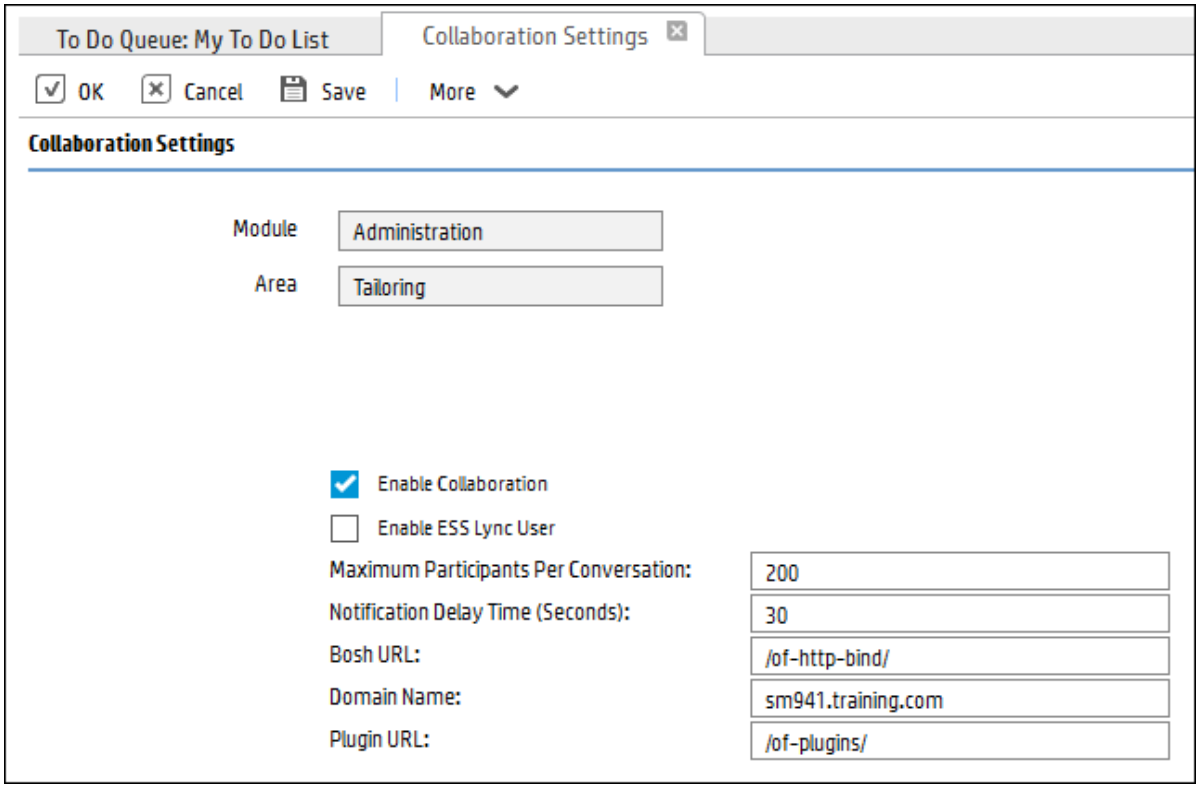
Ensure the Openfire Windows service is started

Delete this text and replace it with your own content.

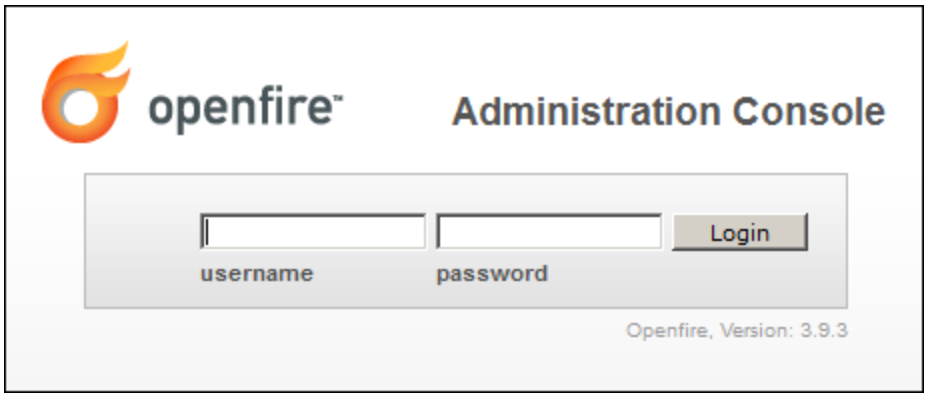
Verify the Service Manager Collaboration configurations

Follow these steps to verify the the Service Manager Collaboration configurations:

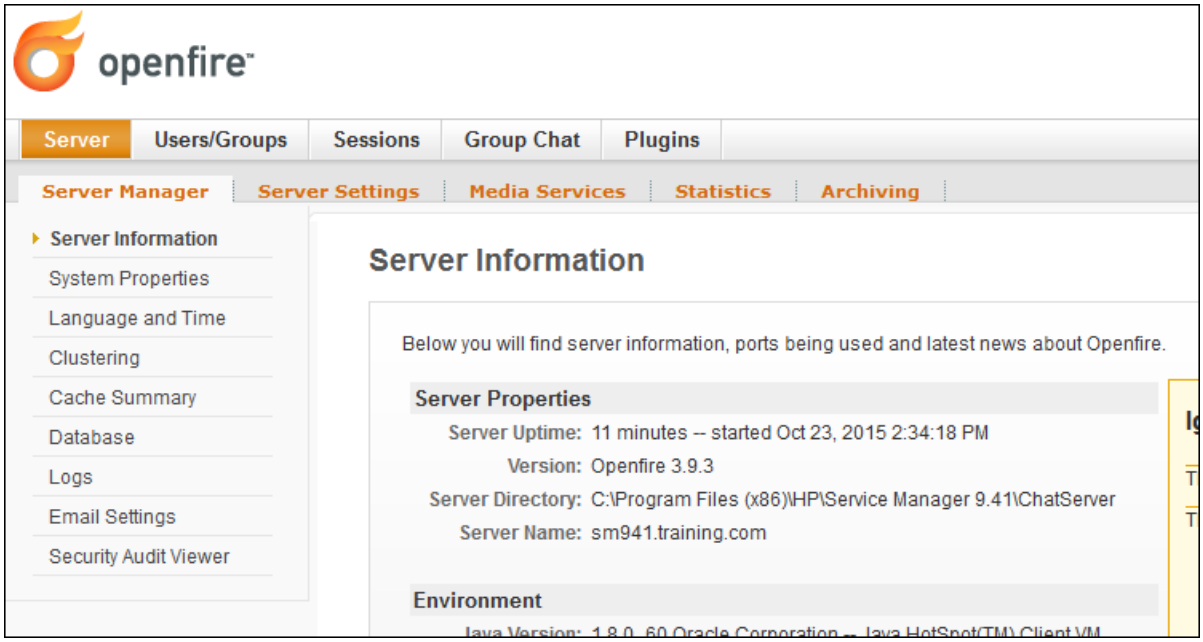
1. Log on to Service Manager as a system administrator.
2. Click **System Administration** > **Ongoing Maintenance** > **Collaboration** > **Configuration**.



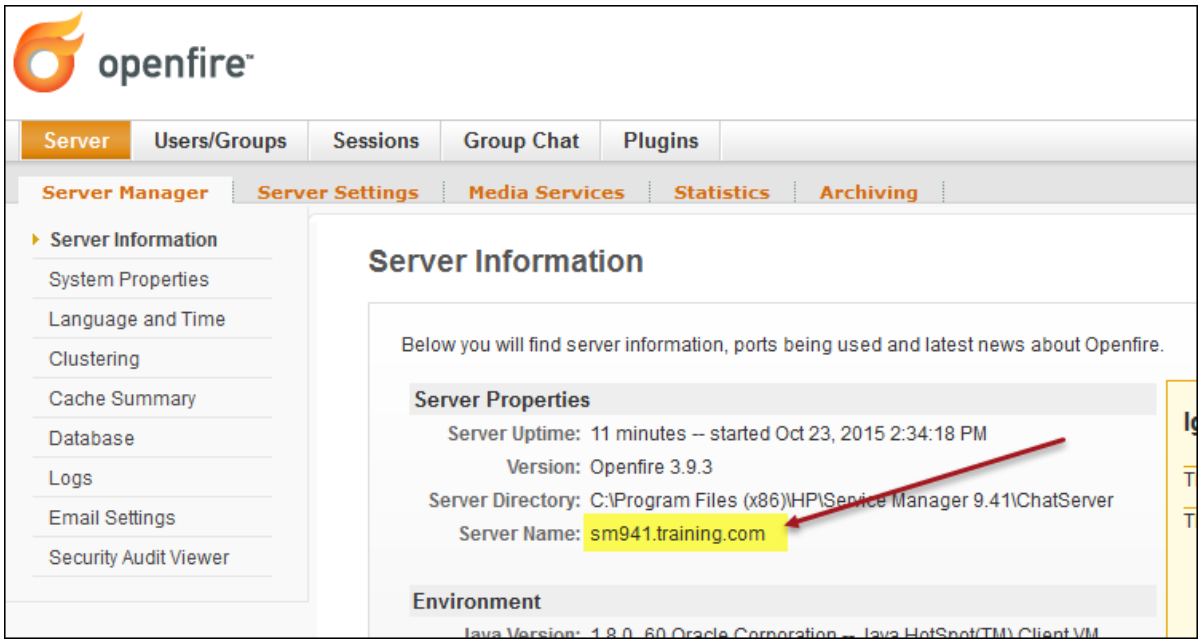
3. Ensure the **Bosh URL** is set to /of-http-bind/.
4. Ensure the **Plugin URL** is set to /of-plugins/.
5. Ensure the **Domain Name** is set to the Openfire Domain you set up in "Task 5: Deploy the chat server " on page 20.
6. Log out from Service Manager.
7. To double-check your Openfire configurations, go to your web browser and access https://localhost:9091. The Openfire Administration Console page opens.



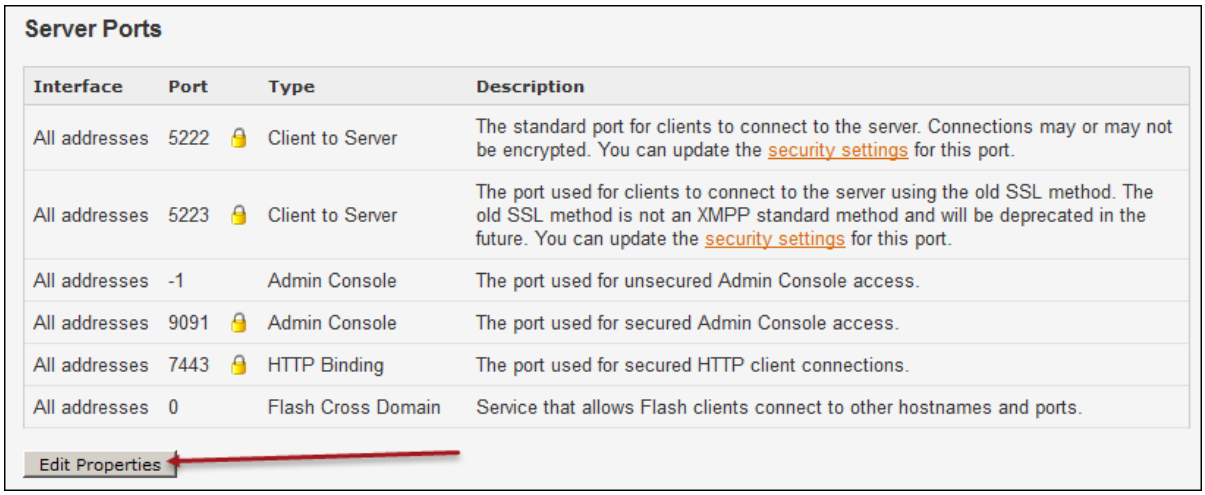
8. Log in with username of `admin` and password of `SM941training`. The system displays the Server Information page.



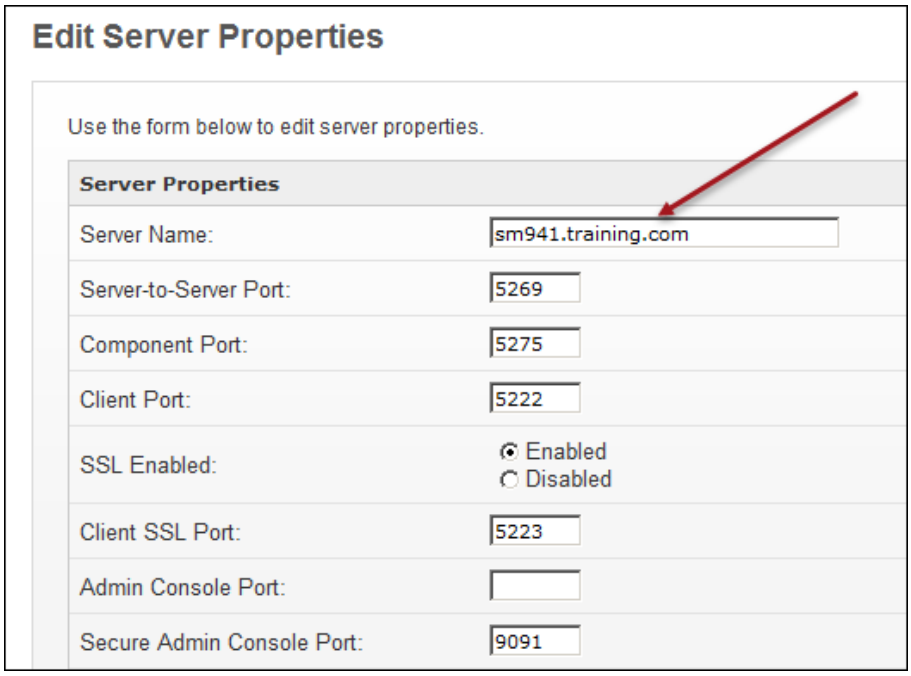
9. On this Server Information page, verify the Server Name (domain name) of the Openfire server.



10. To update the server name, go to the bottom of this page and click **Edit Properties**.

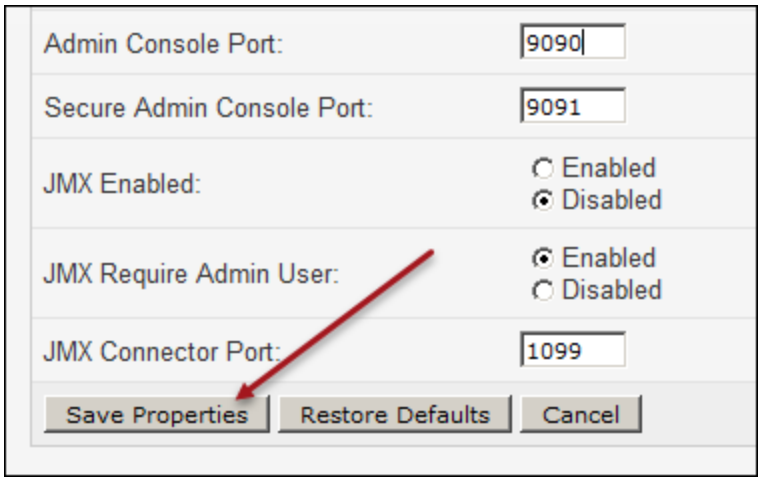


11. Edit the Server Name as appropriate.

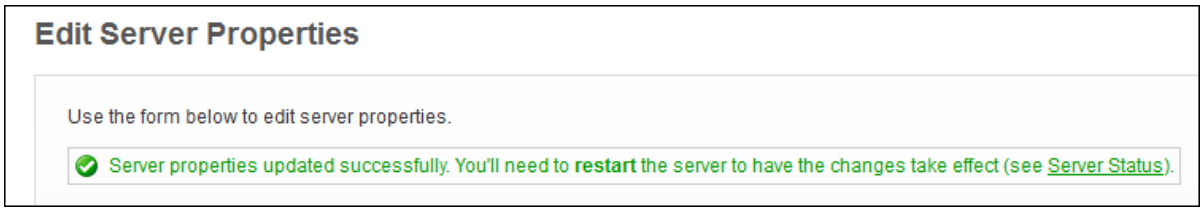


Note:
The **Admin Console Port** field is empty on this page. Set the value to 9090 if you want to take the default value or to the value you choose.

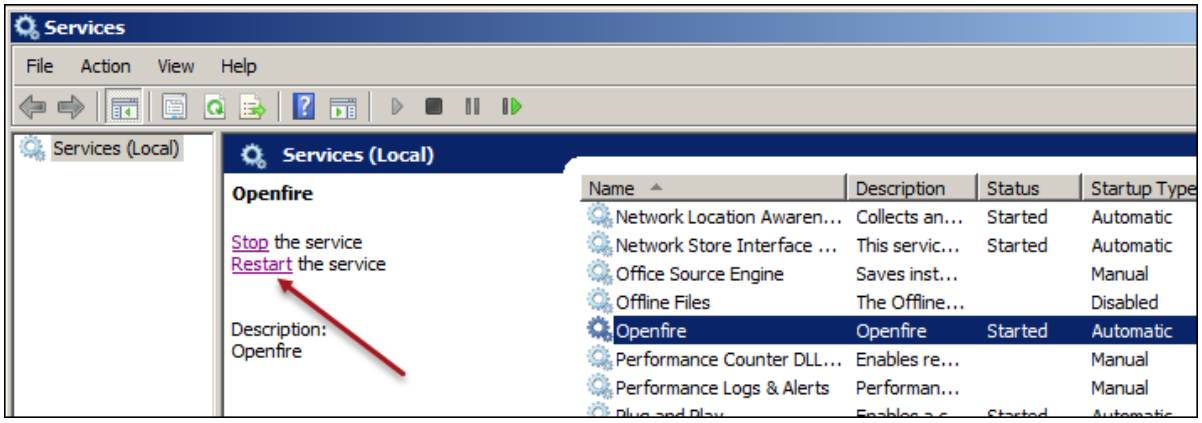
12. Click **Save Properties**.



13. Ensure you receive the message that the server properties were successfully updated.



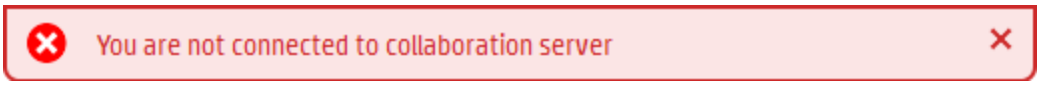
14. Restart the Openfire service in Windows services.



15. Log on to Service Manager again to check whether Collaboration works.

Reinstall Openfire

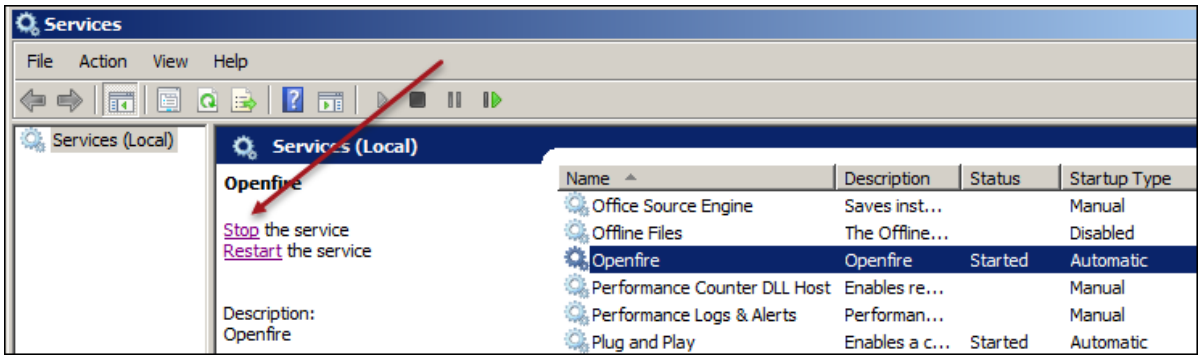
You may need to reinstall Openfire if you have checked all your settings in the entire exercise but still see the following error message:



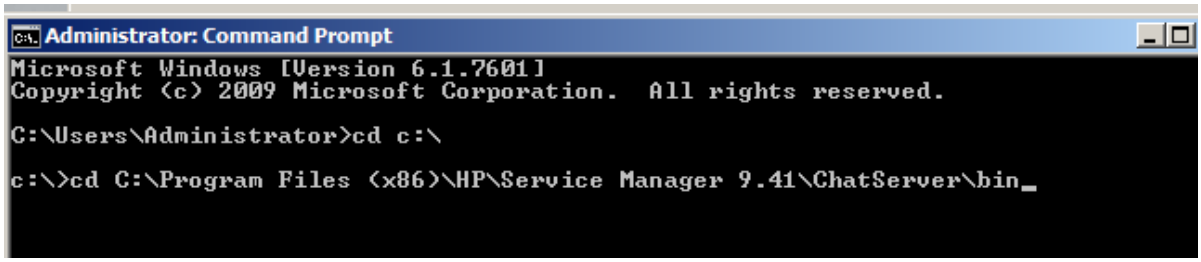
Follow these steps to reinstall Openfire:

1. Log out from Service Manager.

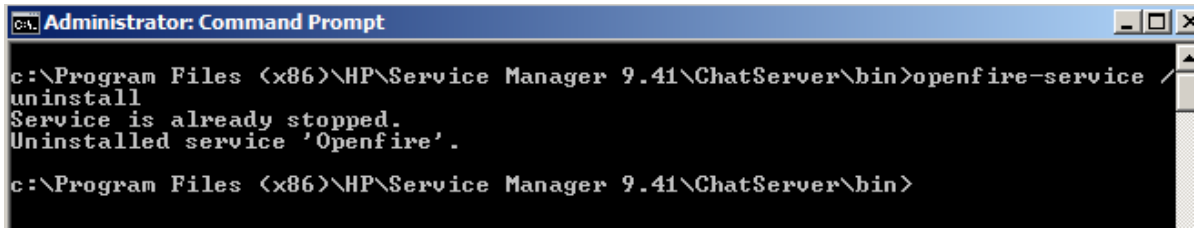
2. Stop the Openfire service.



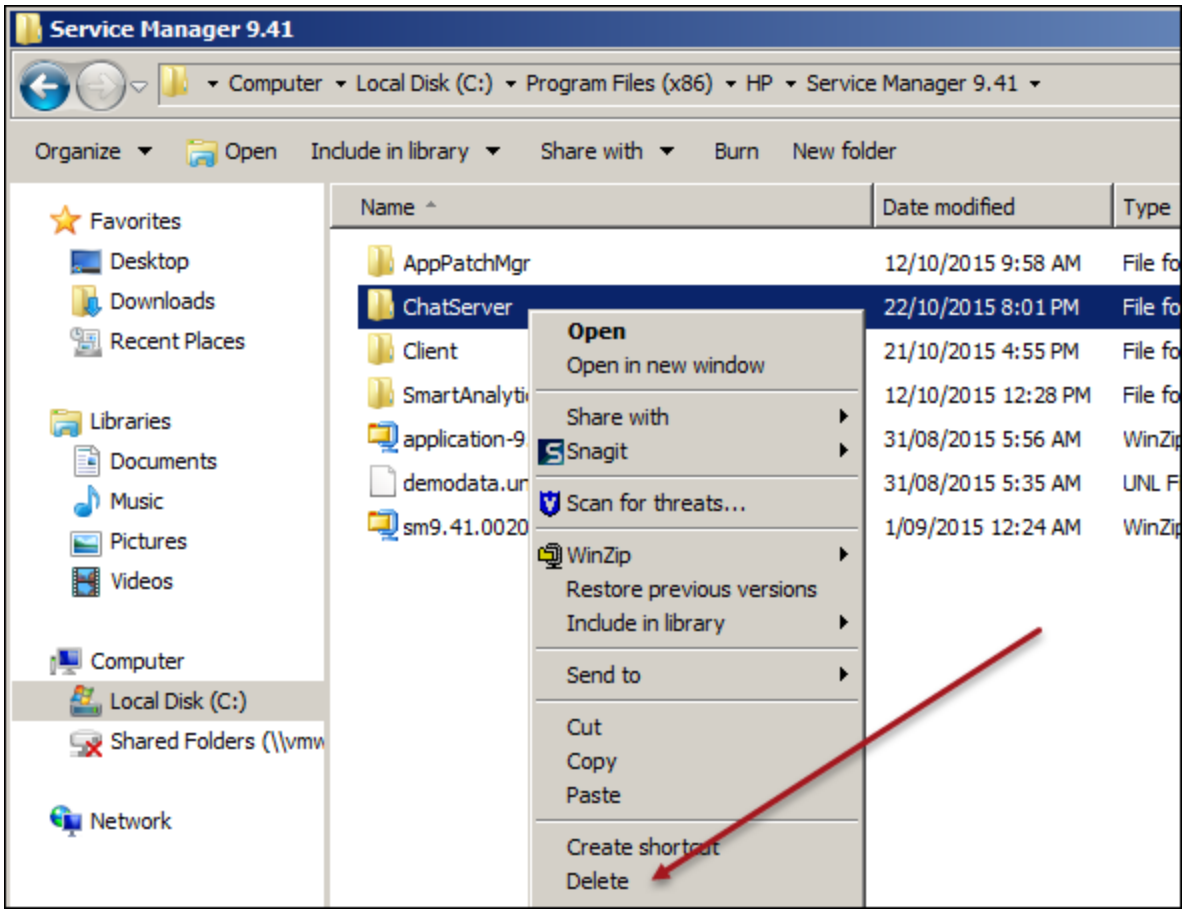
3. Open a DOS command prompt and change the directory to C:\Program Files (x86)\HP\Service Manager 9.41\ChatServer\bin.



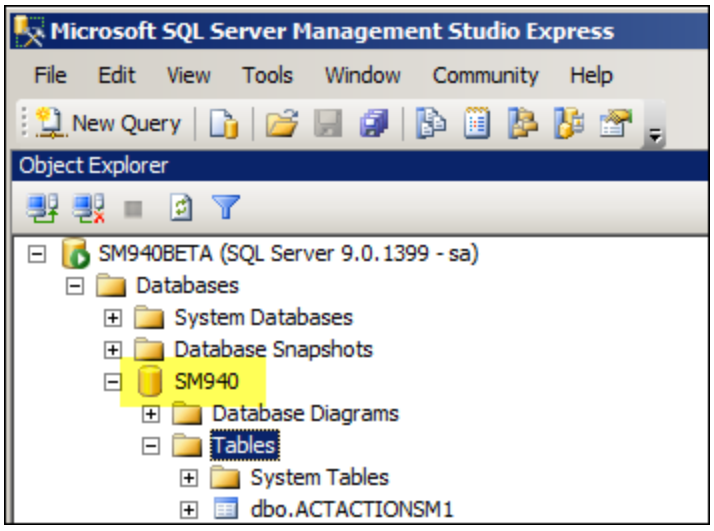
4. Run the **openfire-service /uninstall** command to uninstall the Windows service:



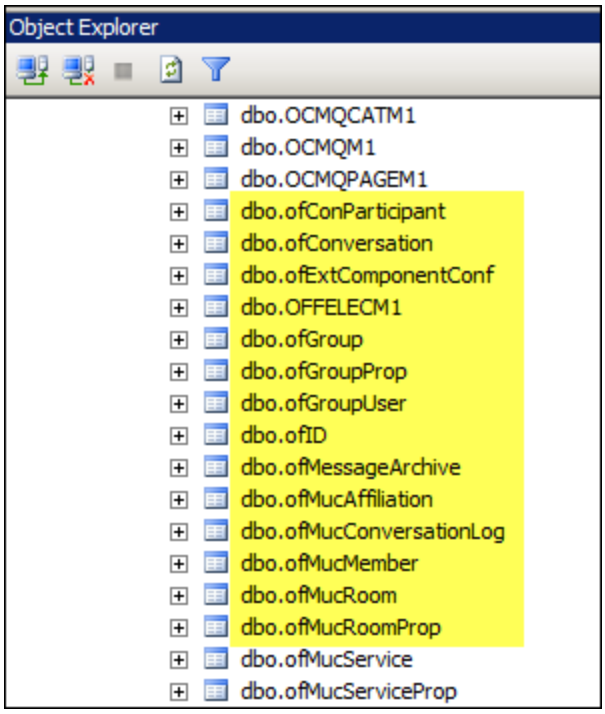
5. Navigate to the C:\Program Files(x86)\HP\Service Manager 9.41 directory by using Windows File Manager, and then remove the ChatServer directory.



6. Log on to your Service Manager database and list the tables.

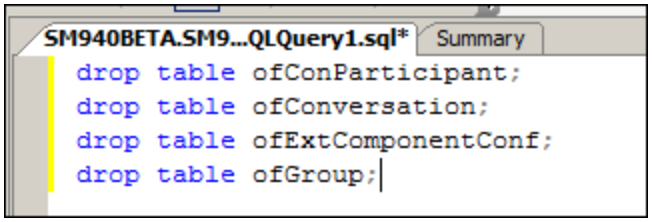


7. Locate the the tables prefixed with **of** in the list.



All of these tables prefixed with lowercase **of** need to be dropped.

8. Drop the tables until all tables prefixed with **of** have been removed.



9. Go to "Task 5: Deploy the chat server " on page 20 and install the Openfire chat server again.

10. Go to "Task 9: Configure LW-SSO for the chat server " on page 49 and configure LW-SSO for the chat server.

11. Log on to Service Manager again to check whether Collaboration works.