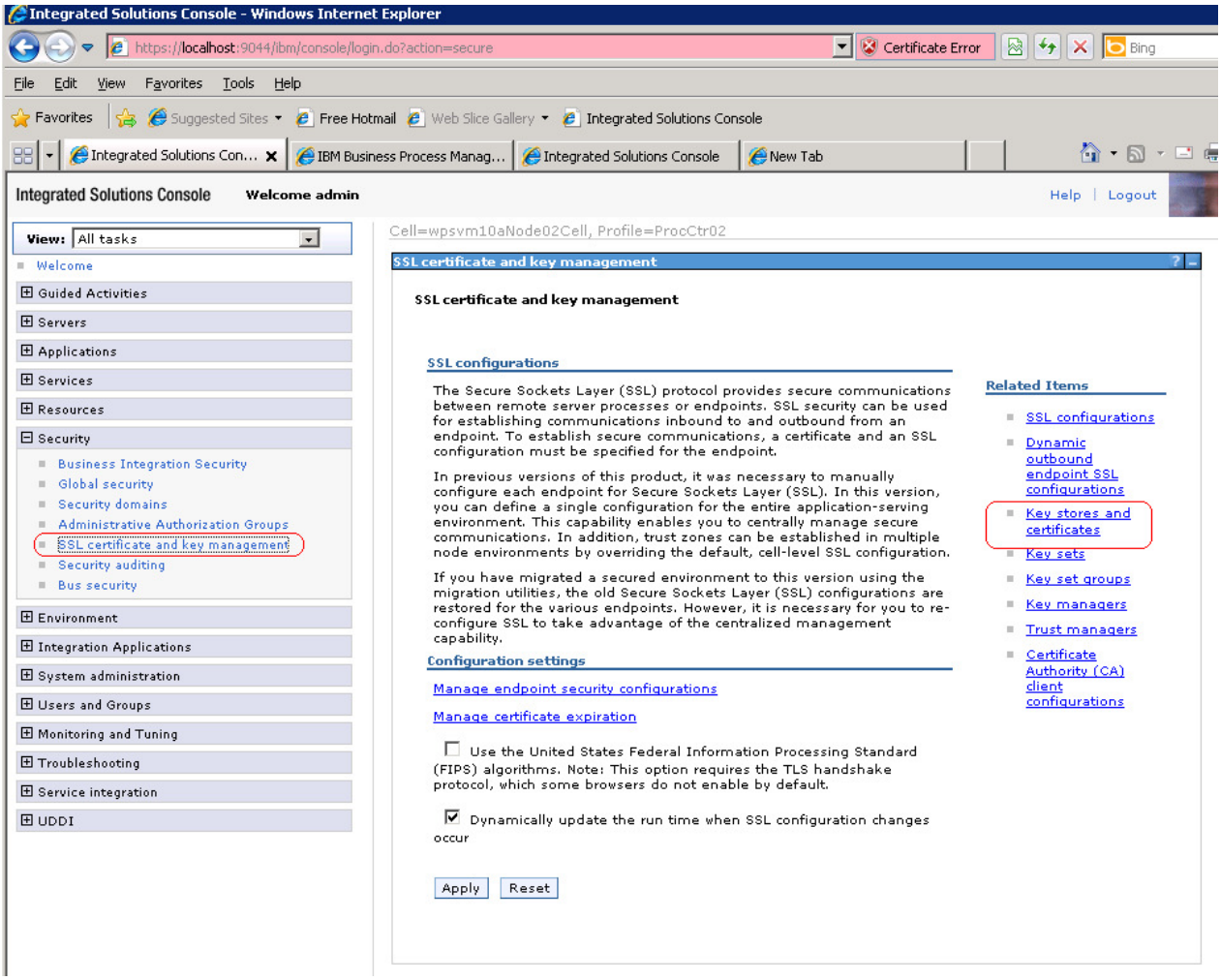
Configuring Secure Socket Layer (SSL) for use with BPM 7.5.x

Configuring Secure Socket Layer (SSL) communication for a standalone environment

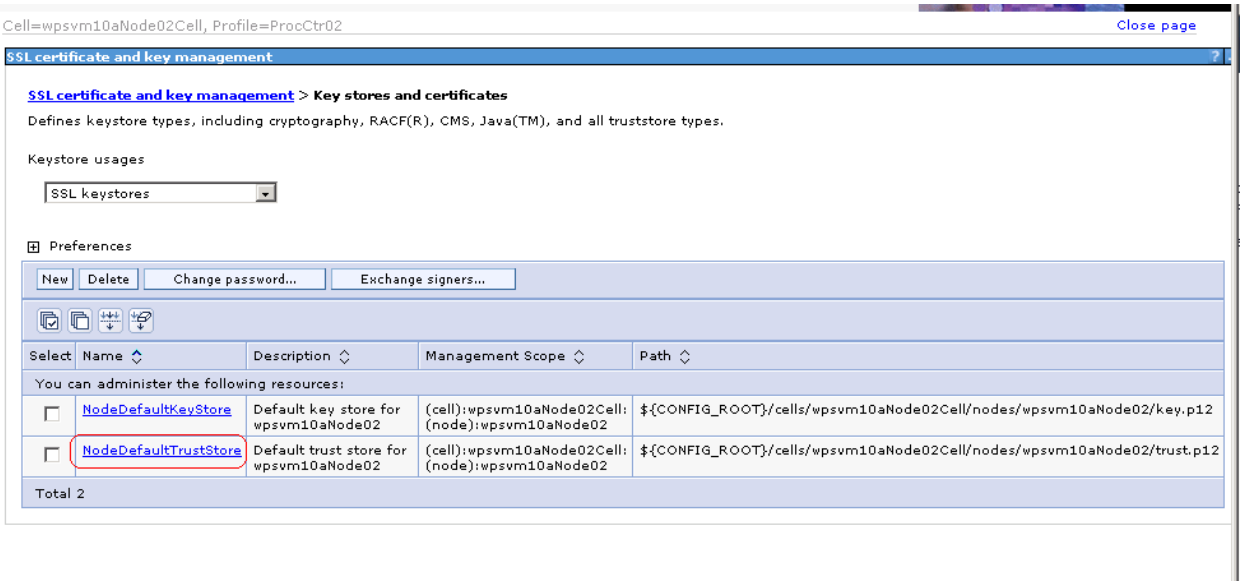
The following steps are required to make the communication between the Process Center and the Process Server work with https in a standalone environment.

Import the Process Server WAS root SSL certificate into Process Center

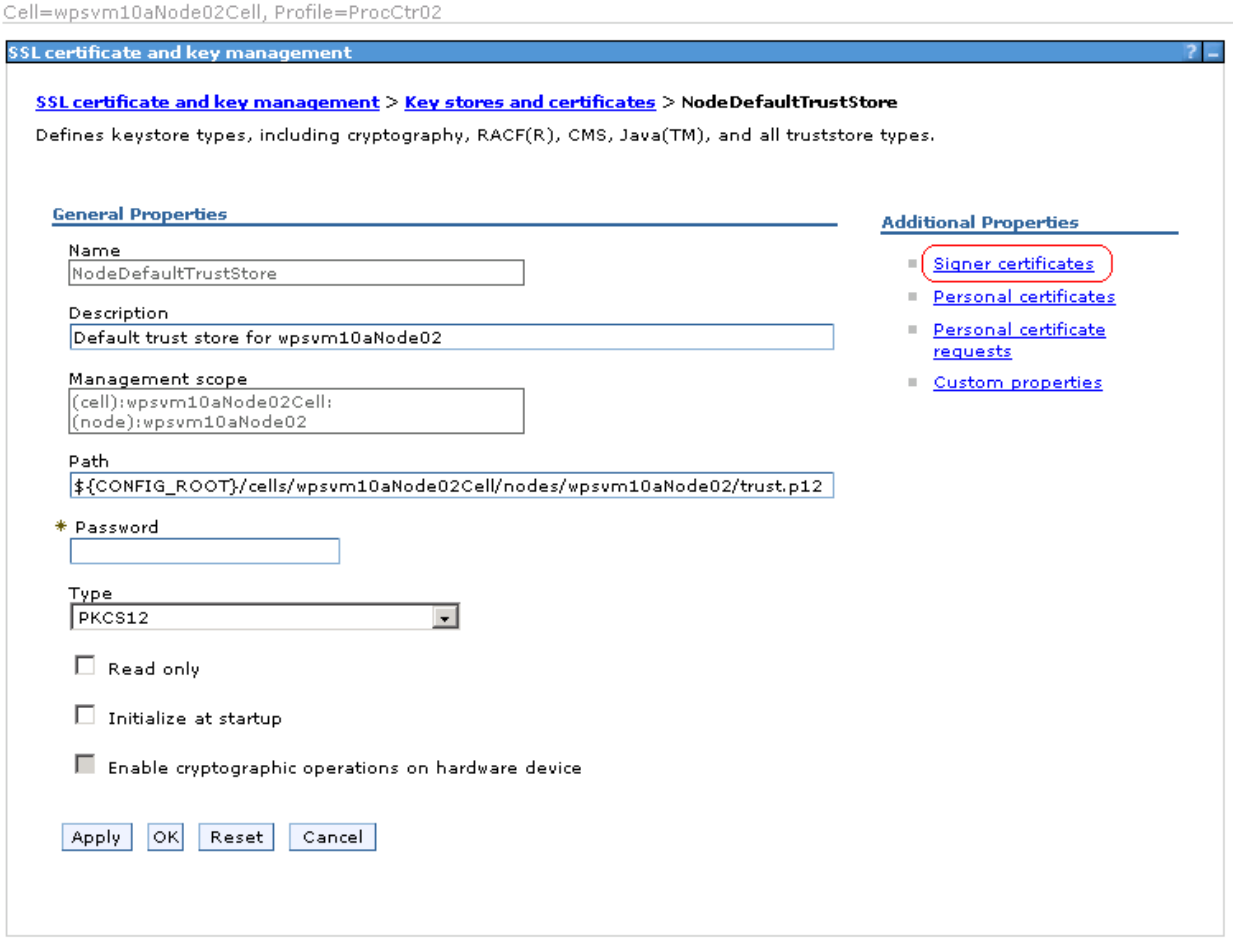
1. On the Process center WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate**.



2. Click **NodeDefaultTrustStore**.

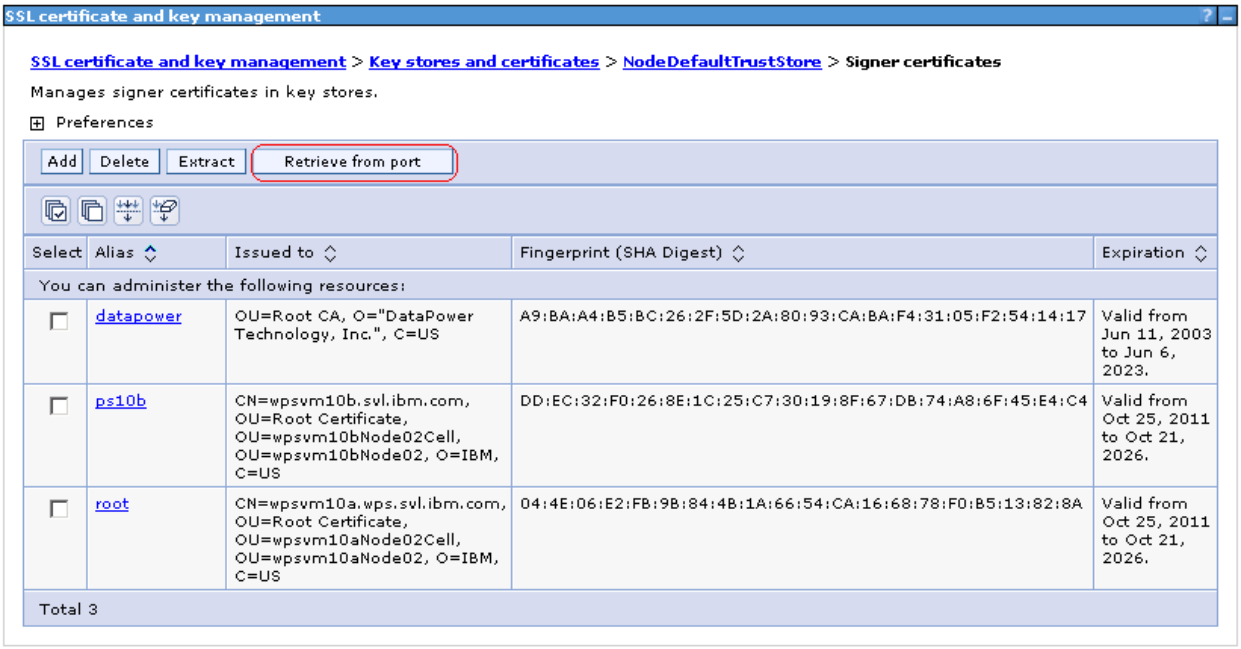


3. Click **Signer certificates**.



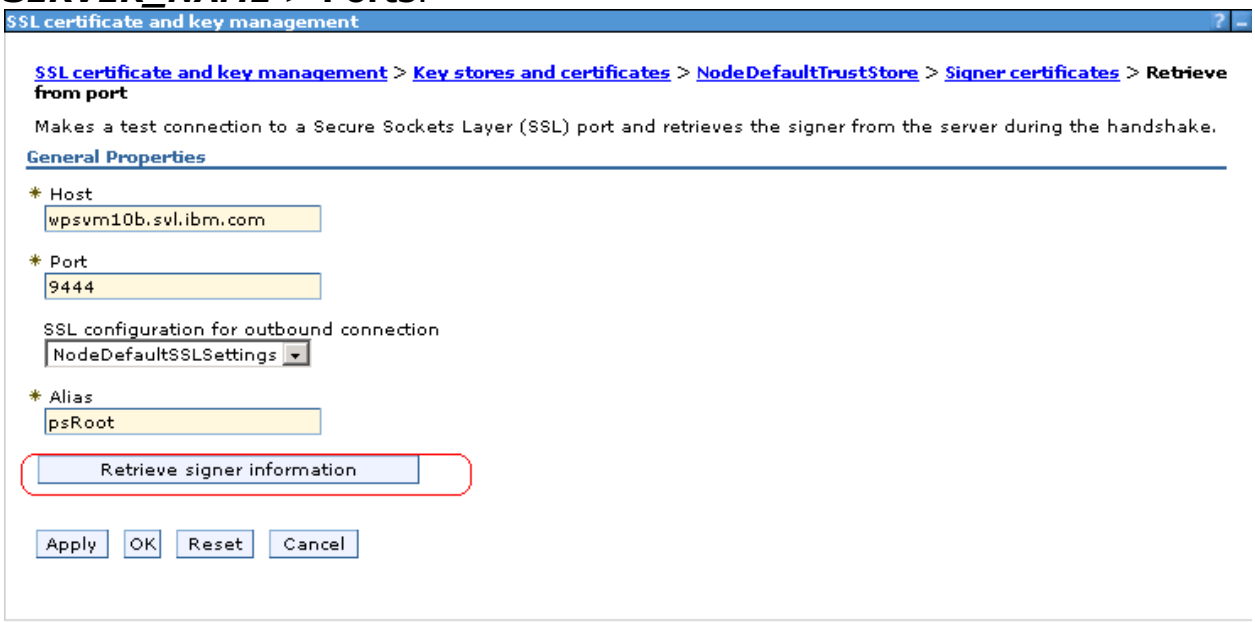
4. Click **Retrieve from port**.

Cell=wpsvm10aNode02Cell, Profile=ProcCtr02

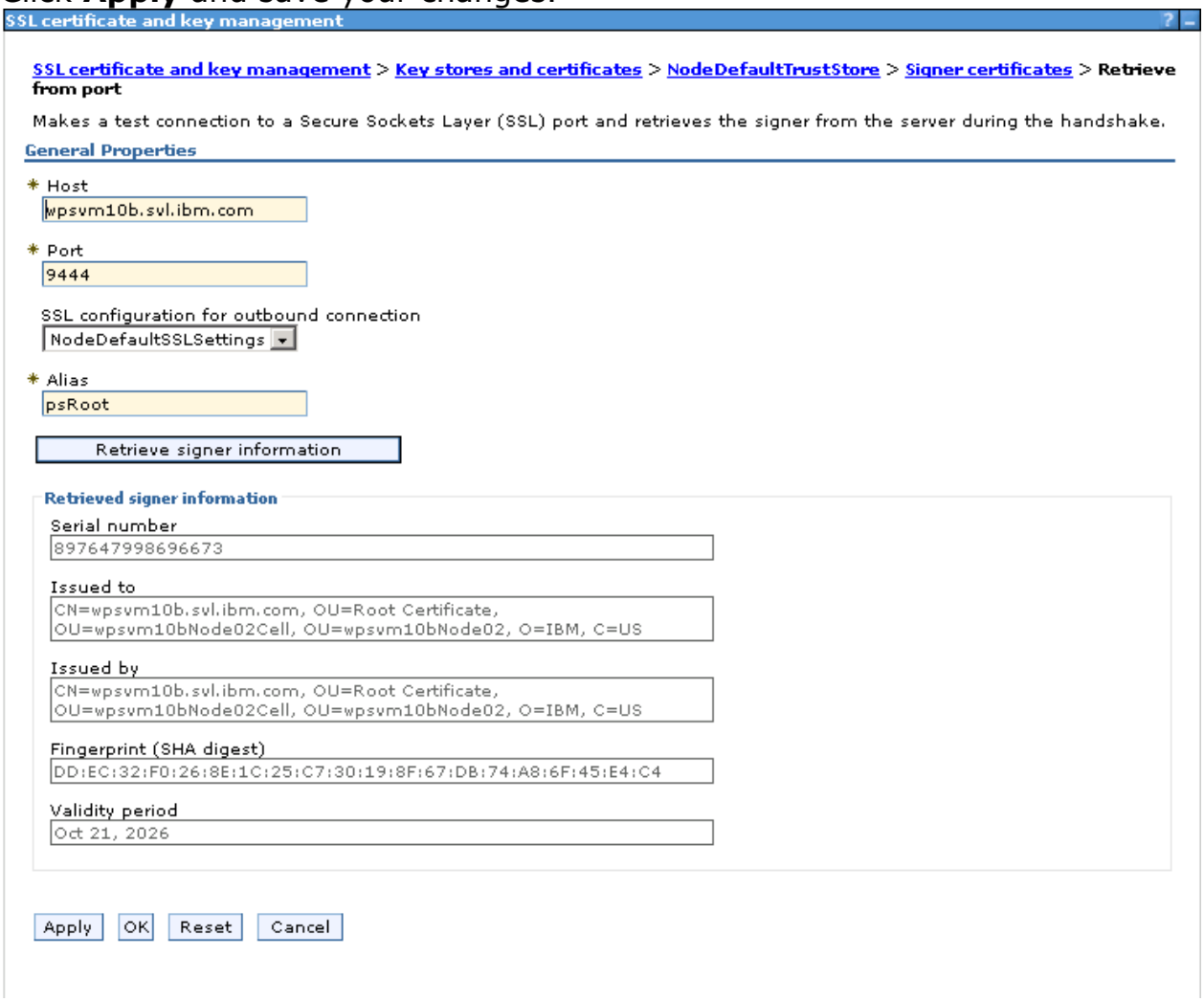


5. Enter the **Host** name, secure **Port** of the Profile (*WC_defaulthost_secure* of Process Server profile), and **Alias**, and click **Retrieve signer information**.

   Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.



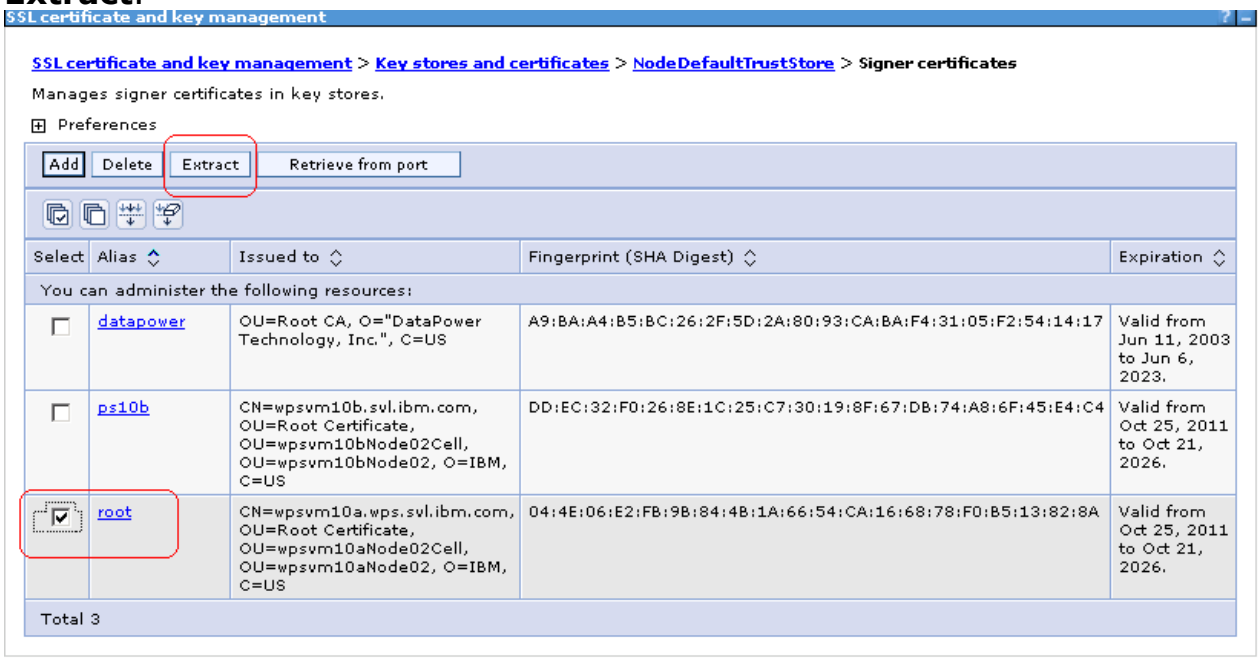
6. Click **Apply** and save your changes.



Export the Process Center root signer certificate

1. On the Process center WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate > NodeDefaultTrustStore > Signer certificates**.

2. From the Signer certificates panel, click the **root** checkbox and select **Extract**.



3. Specify the **File name** path where you want to save the certificate and set the **Data type** to **Binary DER data**. Click **OK**.

4. Copy the extracted Process Center root certificate to the Process Server system.

Import the Process Center root SSL certificate into Process Server

1. On the Process Server WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate > NodeDefaultTrustStore > Signer certificates > Retrieve from port**.

2. Enter the **Host** name, secure **Port** of the Process Center Profile (*WC_defaulthost_secure* of Process Center profile), and **Alias**, and click **Retrieve signer information**.

   Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

3. Click **Apply** and save your changes.

Export the Process Server root signer certificate

1. On the Process Server WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate > NodeDefaultTrustStore > Signer certificates.**

2. From the Signer certificates panel, click on the **Root** checkbox and select **Extract**.

3. Specify the **File name** path where you want to save the certificate and set the **Data type** to **Binary DER data** and click **OK**.

4. Copy the extracted Process Server root certificate to the Process Center system.

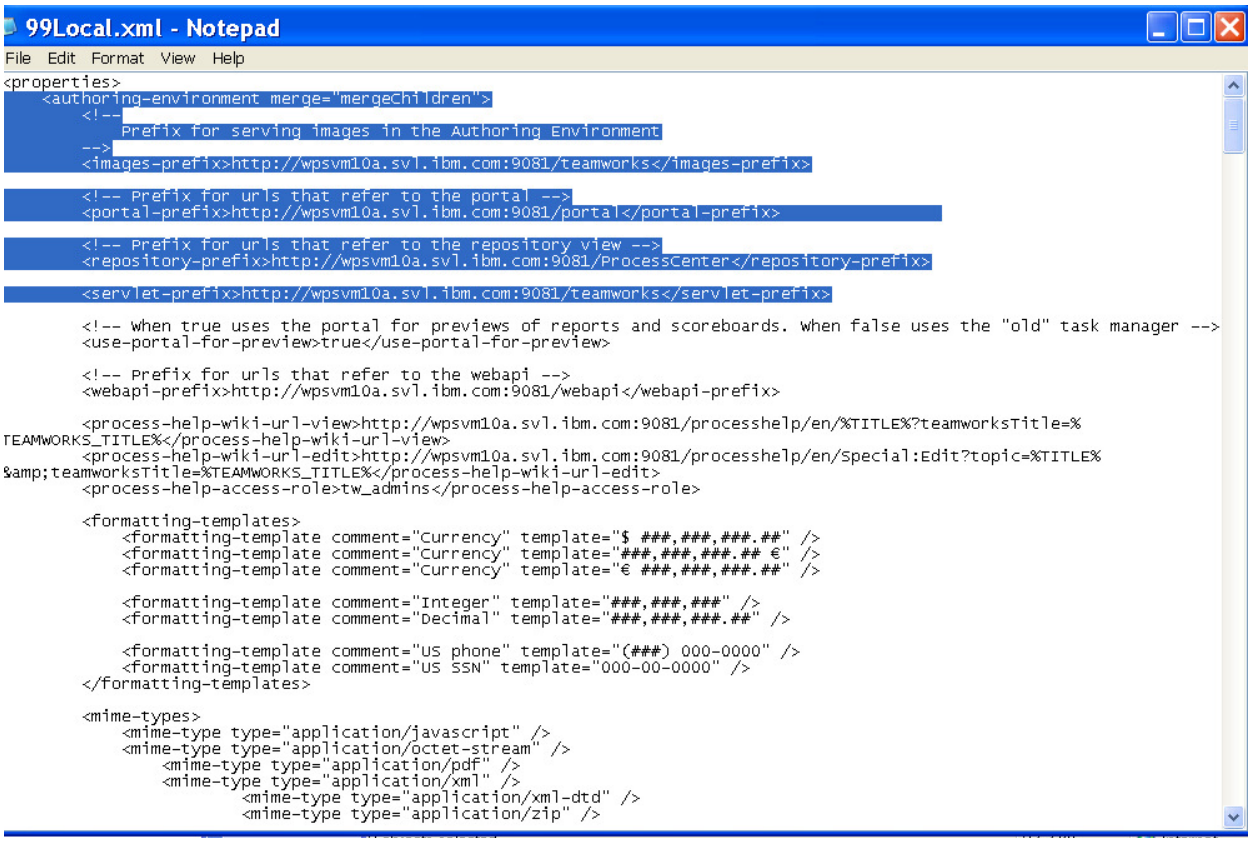
Edit 100Custom.xml on Process Center

1. Edit *WAS_HOME*\profiles*profile name*\config\cells*cell name*\nodes*node name*\servers*server name*\process-center\config\100Custom.xml to overwrite values from 99Local.xml.
   For example:
   c:\BPM\profiles\ProcCtr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-center\config\100Custom.xml.

2. Open *WAS_HOME*\profiles*profile name*\config\cells*cell name*\nodes*node name*\servers*server name*\process-center\config\system\99local.xml.
   For example:

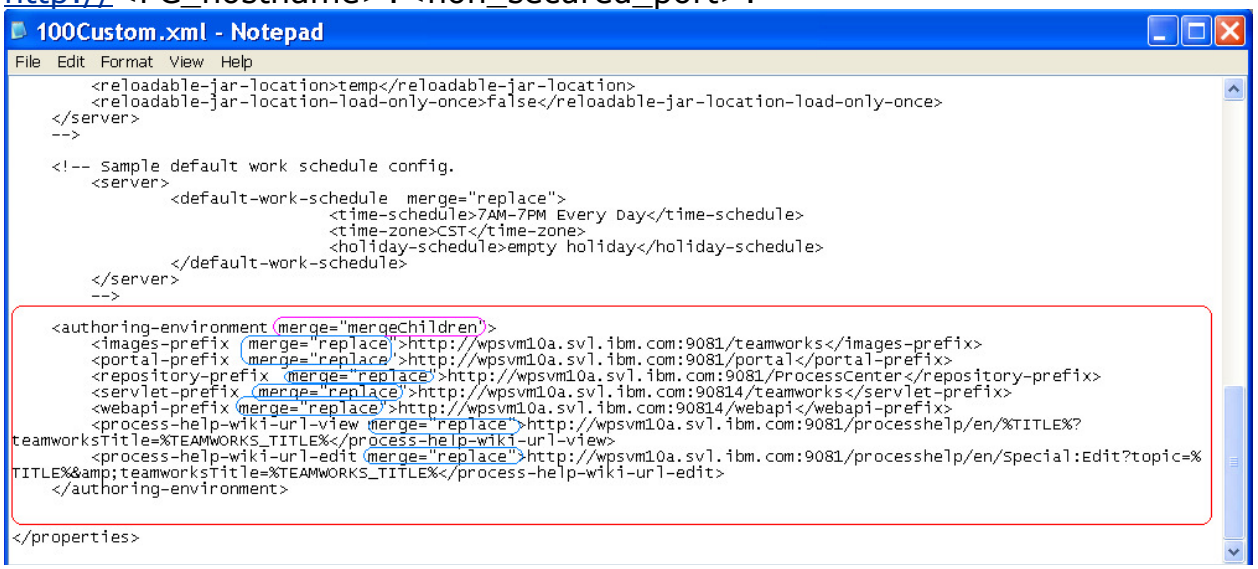
c:\BPM\profiles\ProcCtr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-center\config\system\99local.xml.

3. Copy all occurrences of http://<PC_hostname>:<non_secured_port> in the 99local.xml file, including the enclosing xml tags, and paste them in to the 100Custom.xml file.



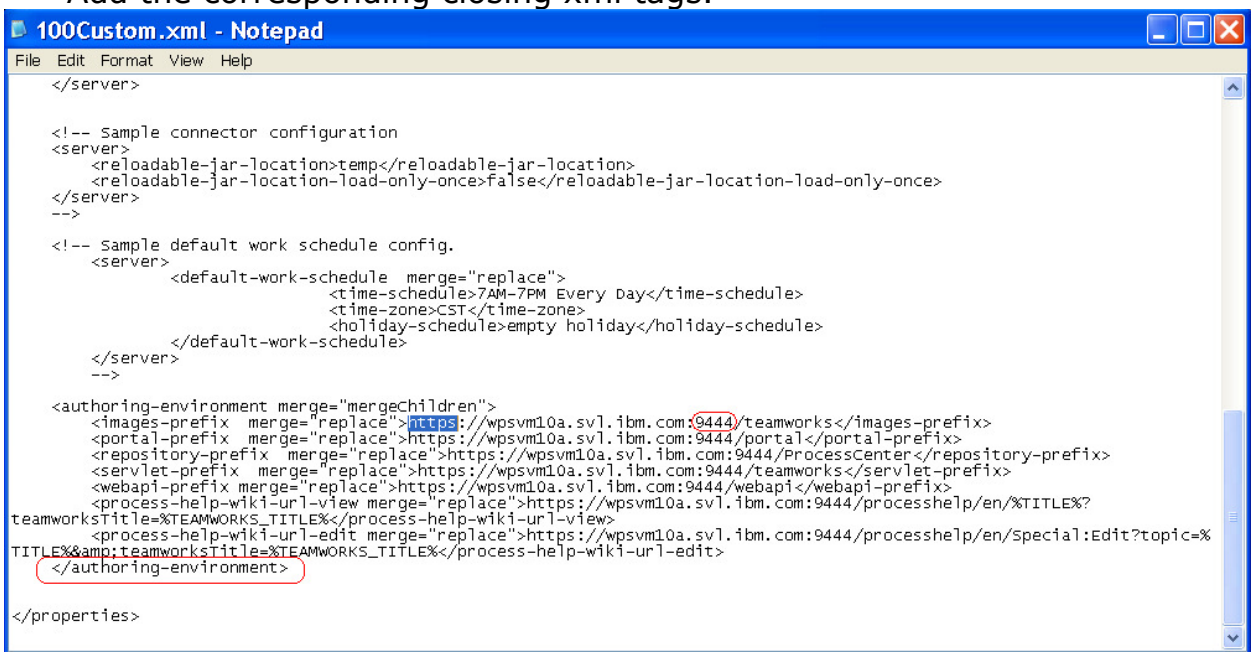
4. Add **merge="mergeChildren"** to the parent xml tags that contain the http://<PC_hostname>:<non_secured_port>.

5. Add **merge="replace"** to the xml tag that contains the http://<PC_hostname>:<non_secured_port>.

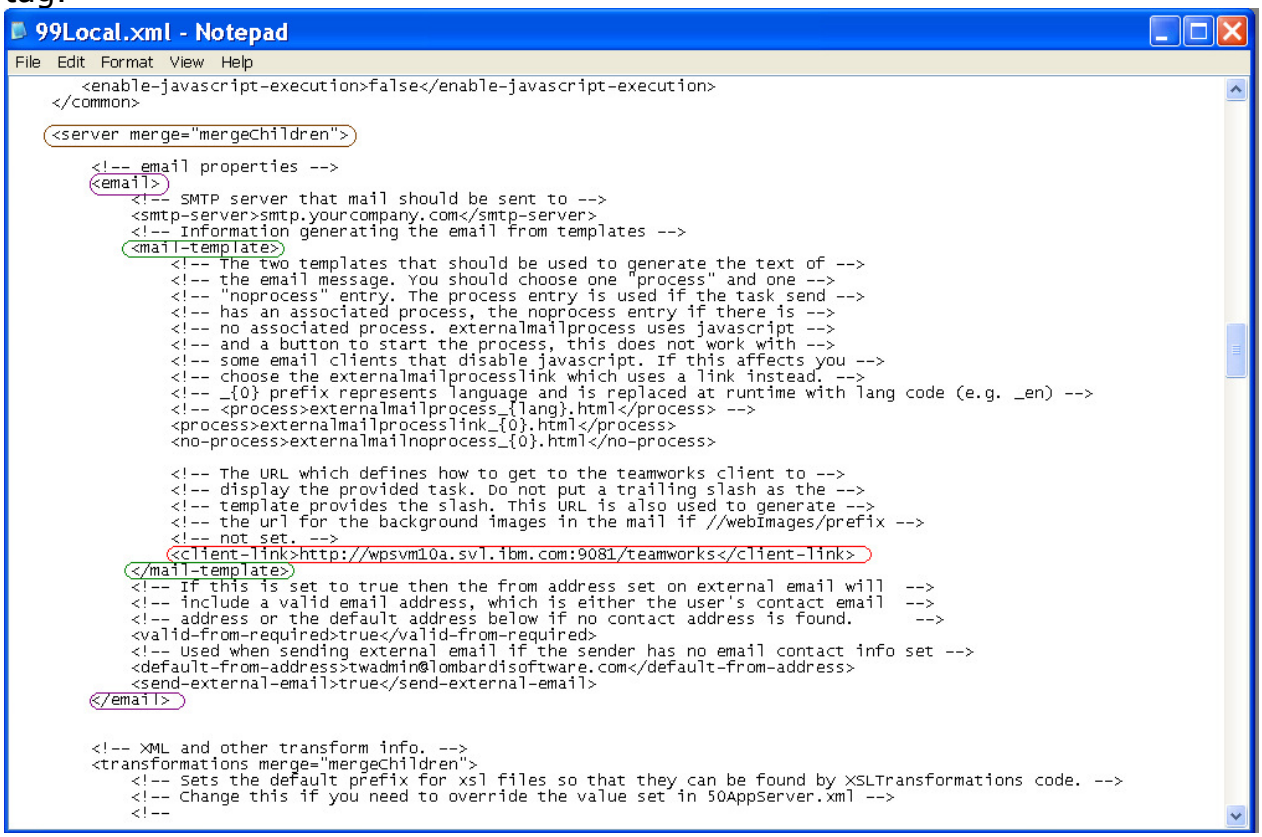


6. Change all occurances of http://<PC_hostname>:<non_secured_port> to https://<PC_hostname>:<secured-port>.

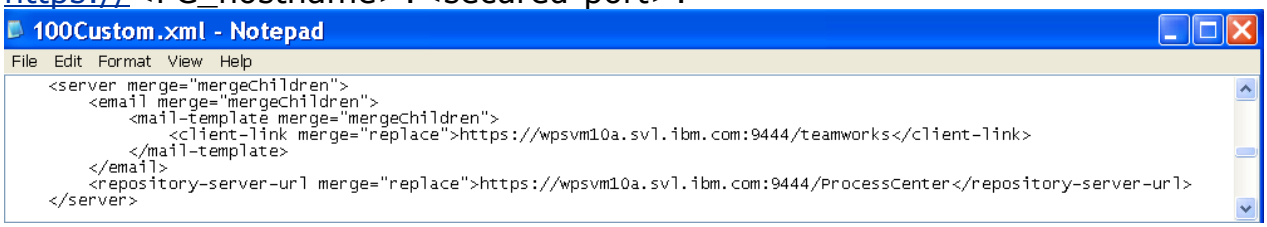
7. Add the corresponding closing xml tags.



8. Copy the parent tags for the <client-link> that contains http://<PC_hostname>:<non_secured_port>, and paste them to the server tag.



9. Add the server section to the 100custom.xml file. Add **merge="mergeChildren"** to the parent xml tags and add **merge="replace"** to the xml tag that contains the http://<PC_hostname>:<non_secured_port>. Then update http://<PC_hostname>:<non_secured_port> to https://<PC_hostname>:<secured-port>.



10. Add the following lines to the <server> section to enable https for deploying the snapshot and specify the correct Process Center secure port:
<deploy-snapshot-using-https merge="replace">true</deploy-snapshot-using-https>
<server-port merge="replace"><*PC WC_defaulthost_secure port*></server-port> (set value to *WC_defaulthost_secure* of Process Center profile)

    Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

11. Open `WAS_HOME\profiles\`*`profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`server name`*`>\process-center\config\system\99Sharepoint.xml`.
For example:
`profiles\ProcCtr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-center\config\system\99Sharepoint.xml`).

12. Copy all occurrences of http://<PC_hostname>:<non_secured_port> from the 99Sharepoint.xml, including its parent xml tags, and paste them to the 100Custom.xml file.

13. Change all occurances of http://<PC_hostname>:<non_secured_port> to https://<PC_hostname>:<secured-port>.

14. Save and close the 100Custom.xml file.

Here is an example of the Process Center 100Custom.xml file:

```
<properties>
```

```
    <!--Properties file for customer cluster scoped properties. -->

 <!-- set unversioned-po-caching-enable to false for clustering
    <common merge="mergeChildren">
        <environment-name merge="replace">My Environment</environment-name>
        <default-unversioned-po-cache-size merge="replace">500</default-unversioned-
po-cache-size>
       <default-versioned-po-cache-size merge="replace">500</default-versioned-po-
cache-size>
        <unversioned-po-caching-enable merge="replace">false</unversioned-po-
caching-enable>
       <default-webapi-userid-cache-size merge="replace">500</default-webapi-userid-
cache-size>
    </common>
    -->

    <!-- Sample connector configuration
    <server>
        <reloadable-jar-location>temp</reloadable-jar-location>
        <reloadable-jar-location-load-only-once>false</reloadable-jar-location-load-
only-once>
    </server>
    -->

    <!-- Sample default work schedule config.
 <server>
       <default-work-schedule  merge="replace">
                   <time-schedule>7AM-7PM Every Day</time-schedule>
                   <time-zone>CST</time-zone>
                   <holiday-schedule>empty holiday</holiday-schedule>
       </default-work-schedule>
 </server>
 -->

    <common merge="mergeChildren">
        <portal-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/portal</portal-prefix>
        <process-admin-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/ProcessAdmin</process-admin-
prefix>
        <teamworks-webapp-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks</teamworks-webapp-
prefix>
        <webservices merge="mergeChildren">
            <base-url
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks/webservices</base-url>
 </webservices>
        <xml-serialization merge="mergeChildren">
            <default-namespace-uri
merge="replace">https://wpsvm10a.svl.ibm.com:9444/schema/</default-namespace-uri>
        </xml-serialization>
        <coach-designer-xsl-url
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks/coachdesigner/transform/
CoachDesigner.xsl</coach-designer-xsl-url>
        <office merge="mergeChildren">
```

```
            <sharepoint merge="mergeChildren">
<default-workspace-site-description merge="replace"><![CDATA[This site has been
automatically generated for managing collaborations and documents
for the Lombardi TeamWorks process instance: <#= tw.system.process.name #> <#=
tw.system.process.instanceId #>

TeamWorks Link:
https://wpsvm10a.svl.ibm.com:9444/portal/jsp/getProcessDetails.do?bpdInstanceId=<#=
tw.system.process.instanceId #>

]]></default-workspace-site-description>
            </sharepoint>
        </office>
    </common>
    <server merge="mergeChildren">
        <email merge="mergeChildren">
            <mail-template merge="mergeChildren">
                <client-link
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks</client-link>
            </mail-template>
        </email>
        <repository-server-url
merge="replace">https://wpsvm10a.svl.ibm.com:9444/ProcessCenter</repository-server-
url>
        <deploy-snapshot-using-https  merge="replace">true</deploy-snapshot-using-
https>
        <server-port  merge="replace">9444</server-port>
    </server>
    <authoring-environment merge="mergeChildren">
        <images-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks</images-prefix>
        <portal-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/portal</portal-prefix>
        <repository-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/ProcessCenter</repository-prefix>
        <servlet-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/teamworks</servlet-prefix>
        <webapi-prefix
merge="replace">https://wpsvm10a.svl.ibm.com:9444/webapi</webapi-prefix>
        <process-help-wiki-url-view
merge="replace">https://wpsvm10a.svl.ibm.com:9444/processhelp/en/%TITLE%?teamworksTi
tle=%TEAMWORKS_TITLE%</process-help-wiki-url-view>
        <process-help-wiki-url-edit
merge="replace">https://wpsvm10a.svl.ibm.com:9444/processhelp/en/Special:Edit?topic=
%TITLE%&amp;teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-edit>
    </authoring-environment>
</properties>
```

Edit 100Custom.xml on Process Server

1. Edit `WAS_HOME\profiles\profile name\config\cells\cell name\nodes\node name\servers\server name\process-server\config\100Custom.xml` to overwrite values from the 99Local.xml file. For example: `c:\BPM\profiles\ProcSrv01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-server\config\100Custom.xml`.

2. Open `WAS_HOME\profiles\profile name\config\cells\cell name\nodes\node name\servers\server name\process-server\config\99local.xml`. For example: `c:\BPM\profiles\ProcSrv01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-server\config\system\99local.xml`.

3. Copy all occurrences of `http://<PS_hostname>:<non_secured_port>` from the 99local.xml file, including its enclosing parent xml tags, and paste the same to the 100Custom.xml file.

4. Add `merge="mergeChildren"` to the parent xml tags that contain `http://<PS_hostname>:<non_secured_port>`.

5. Add `merge="replace"` to the xml tag that contains `http://<PS_hostname>:<non_secured_port>`.

6. Change `http://<PS_hostname>:<non_secured_port>` to `https://<PS_hostname>:<secured-port>`.

7. Add the corresponding closing xml tags.

8. For the `<client-link>` tag that contains `http://<PS_hostname>:<non_secured_port>`, copy its parent tags up to the server tag.

9. Add the server section to the 100Custom.xml file.
   a. Add `merge="mergeChildren"` to the parent xml tags
   b. Add `merge="replace"` to the xml tag that contains `http://<PS_hostname>:<non_secured_port>`.
   c. Change `http://<PS_hostname>:<non_secured_port>` to `https://<PS_hostname>:<secured-port>`.

10. Add the following to the `<server>` section to specify the correct Process Server secure port: `<server-port merge="replace"><PS WC_defaulthost_secure port></server-port>` (set the value to *WC_defaulthost_secure* of Process Server profile).

Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

11. Open `WAS_HOME\profiles\profile name\config\cells\cell name\nodes\node name\servers\server name\process-server\config\system\99Sharepoint.xml`. For example: `c:\BPM\profiles\ProcSrv01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-server\config\system\99Sharepoint.xml`.

12. Copy all occurrences of `http://<PS_hostname>:<non_secured_port>` from the `99Sharepoint.xml` file, including its parent xml tags, and paste them to the `100Custom.xml` file.

13. Change `http://<PS_hostname>:<non_secured_port>` to `https://<PS_hostname>:<secured-port>`.

14. Save and close the 100Custom.xml file.

Here is a sample Process Server 100Custom.xml file:

```
<properties>
    <!--Properties file for customer cluster scoped properties. -->

  <!-- set unversioned-po-caching-enable to false for clustering
    <common merge="mergeChildren">
        <environment-name merge="replace">My Environment</environment-name>
        <default-unversioned-po-cache-size merge="replace">500</default-unversioned-
po-cache-size>
   <default-versioned-po-cache-size merge="replace">500</default-versioned-po-cache-
size>
        <unversioned-po-caching-enable merge="replace">false</unversioned-po-caching-
enable>
   <default-webapi-userid-cache-size merge="replace">500</default-webapi-userid-cache-
size>
    </common>
    -->

    <!-- Sample connector configuration
    <server>
        <reloadable-jar-location>temp</reloadable-jar-location>
        <reloadable-jar-location-load-only-once>false</reloadable-jar-location-load-
only-once>
    </server>
    -->

    <!-- Sample default work schedule config.
  <server>
   <default-work-schedule  merge="replace">
              <time-schedule>7AM-7PM Every Day</time-schedule>
              <time-zone>CST</time-zone>
              <holiday-schedule>empty holiday</holiday-schedule>
```

```
   </default-work-schedule>
  </server>
  -->

    <common merge="mergeChildren">
        <portal-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/portal</portal-prefix>
        <process-admin-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/ProcessAdmin</process-admin-prefix>
        <teamworks-webapp-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks</teamworks-webapp-prefix>
        <webservices merge="mergeChildren">
            <base-url
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks/webservices</base-url>
        </webservices>
        <xml-serialization merge="mergeChildren">
            <default-namespace-uri
merge="replace">https://wpsvm10b.svl.ibm.com:9444/schema/</default-namespace-uri>
        </xml-serialization>
        <coach-designer-xsl-url
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks/coachdesigner/transform/Co
achDesigner.xsl</coach-designer-xsl-url>
        <office merge="mergeChildren">
            <sharepoint merge="mergeChildren">
                <default-workspace-site-description merge="replace"><![CDATA[This site
has been automatically generated for managing collaborations and documents
for the Lombardi TeamWorks process instance: <#= tw.system.process.name #> <#=
tw.system.process.instanceId #>

TeamWorks Link:
https://wpsvm10b.svl.ibm.com:9444/portal/jsp/getProcessDetails.do?bpdInstanceId=<#=
tw.system.process.instanceId #>

]]></default-workspace-site-description>
            </sharepoint>
        </office>
    </common>
    <server merge="mergeChildren">
        <email merge="mergeChildren">
            <mail-template merge="mergeChildren">
                <client-link
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks</client-link>
            </mail-template>
        </email>
        <repository-server-url
merge="replace">https://wpsvm10a.svl.ibm.com:9444/ProcessCenter</repository-server-
url>
        <server-port merge="replace">9444</server-port>
    </server>
    <authoring-environment merge="mergeChildren">
        <images-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks</images-prefix>
        <portal-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/portal</portal-prefix>
```

```
        <repository-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/ProcessCenter</repository-prefix>
        <servlet-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/teamworks</servlet-prefix>
        <webapi-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9444/webapi</webapi-prefix>
        <process-help-wiki-url-view
merge="replace">https://wpsvm10b.svl.ibm.com:9444/processhelp/en/%TITLE%?teamworksTitl
e=%TEAMWORKS_TITLE%</process-help-wiki-url-view>
        <process-help-wiki-url-edit
merge="replace">https://wpsvm10b.svl.ibm.com:9444/processhelp/en/Special:Edit?topic=%T
ITLE%&amp;teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-edit>
    </authoring-environment>
</properties>
```

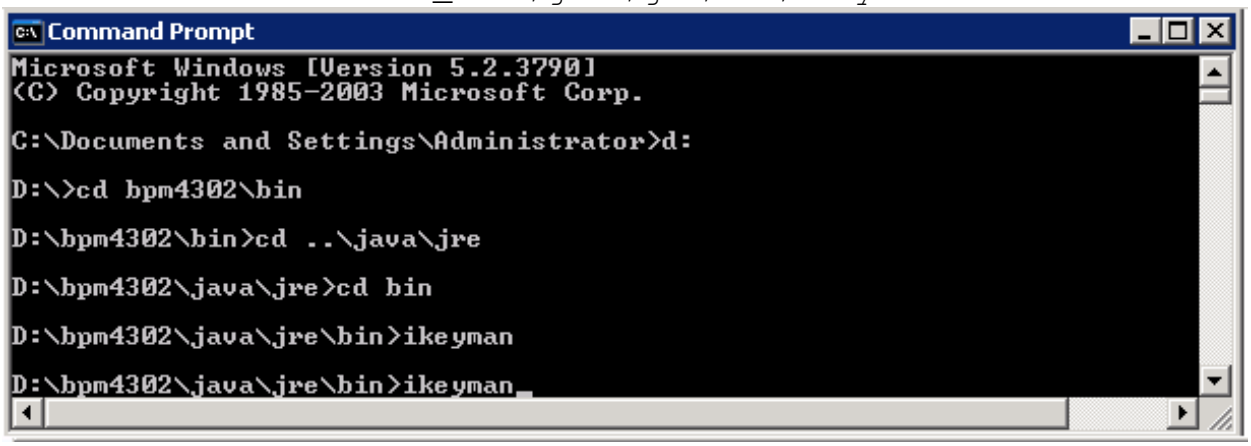
SSL communication between Process Server and Process Center Server

Important: If the Process Center and clustered runtime servers were started before you begin to configure SSL, and the LSW_SERVER table on the Process Center database contains the non-secure port of the Process Server, you must delete the Process Server from the Process Center repository:

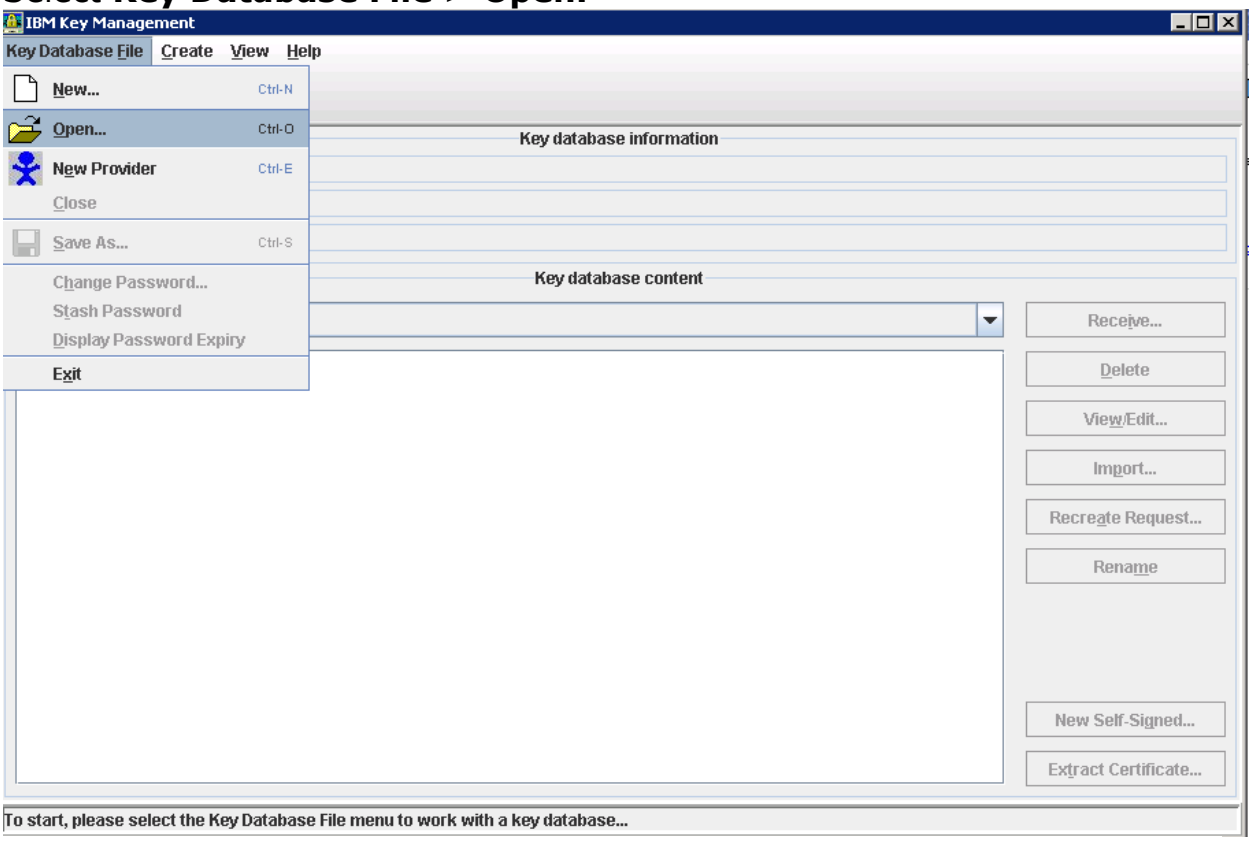
1. Stop Process Server.
2. From the Servers tab on the Process Center Console, delete Process Server from the Process Center repository.
3. Delete the record with the non-secure port from the LSW_SERVER table on the Process Center database.
4. Start Process Server.

Make sure that the SSL communication between the Process Server and the Process Center Server work by adding the certificates to each other's trust store.

1. Install the Process Server signer certificate in to the Process Center trust store.
   a) Invoke Process Center `WAS_HOME/java/jre/bin/ikeyman`.



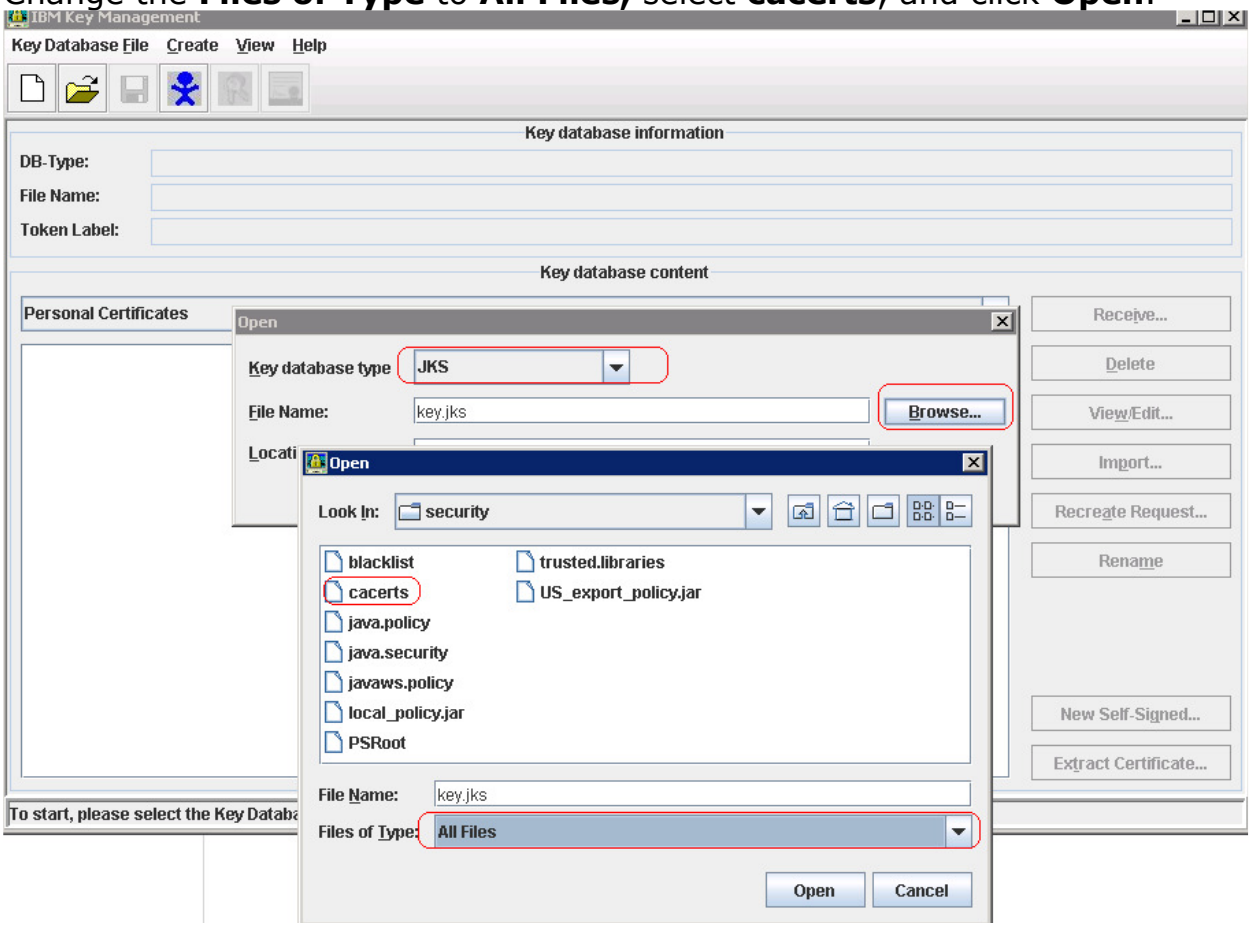
b) Select **Key Database File > Open.**



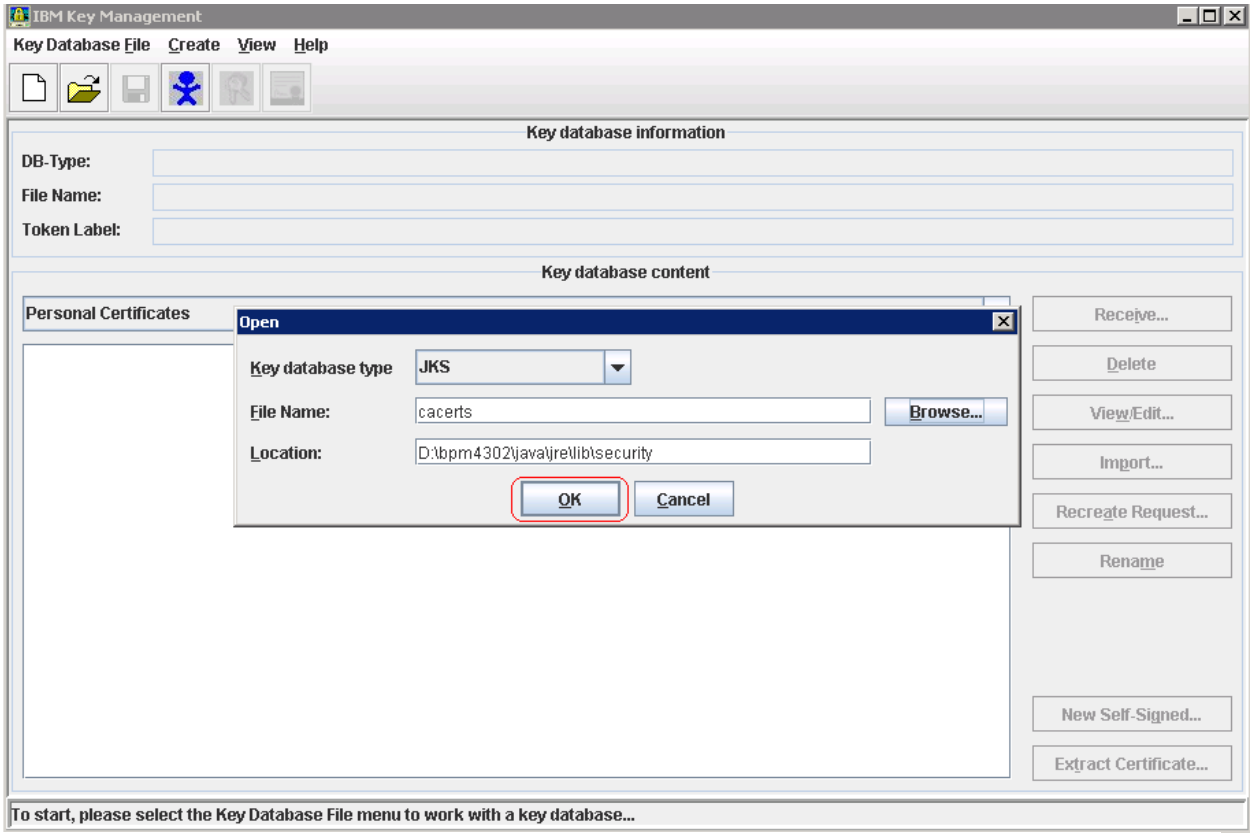
c) Set the Key database type to JKS.

d) Click **Browse** and set the file location to *WAS_HOME*`/java/jre/lib/security`.

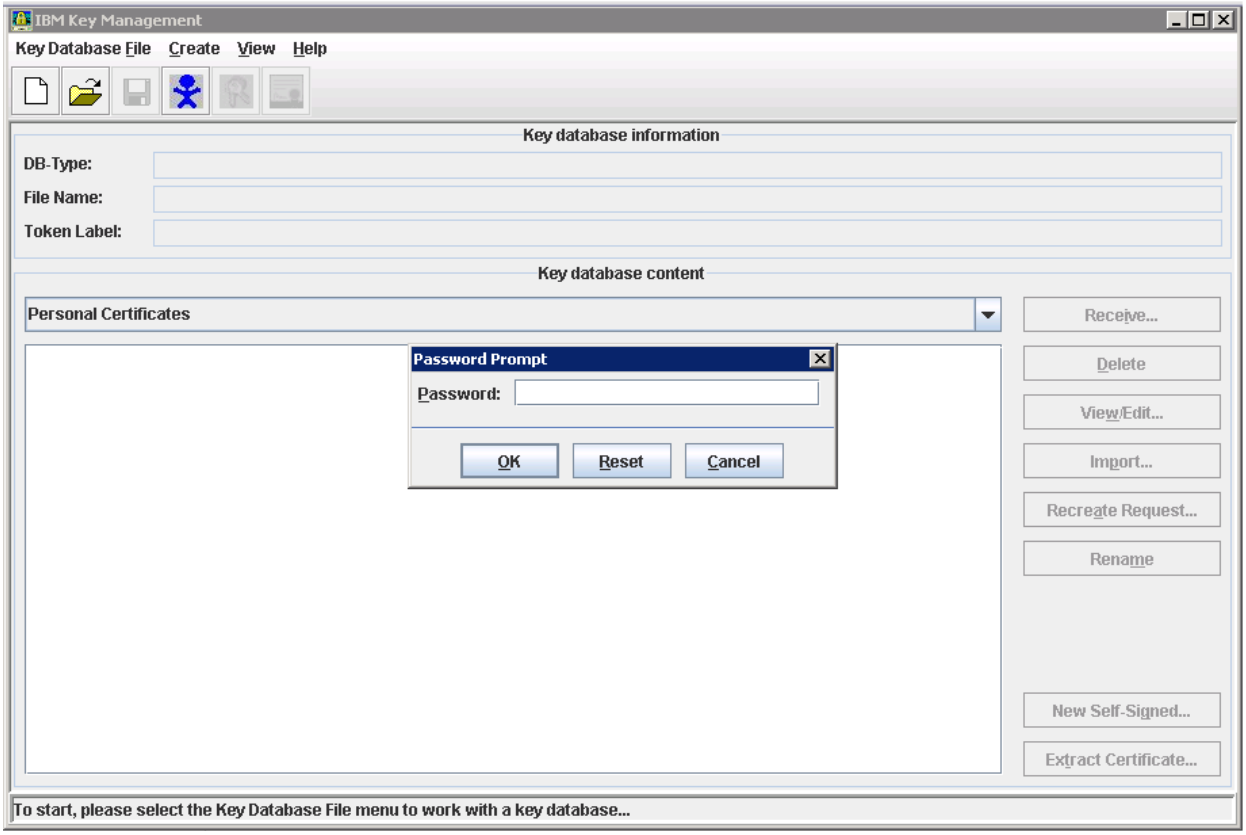
e) Change the **Files of Type** to **All Files,** select **cacerts**, and click **Open**.



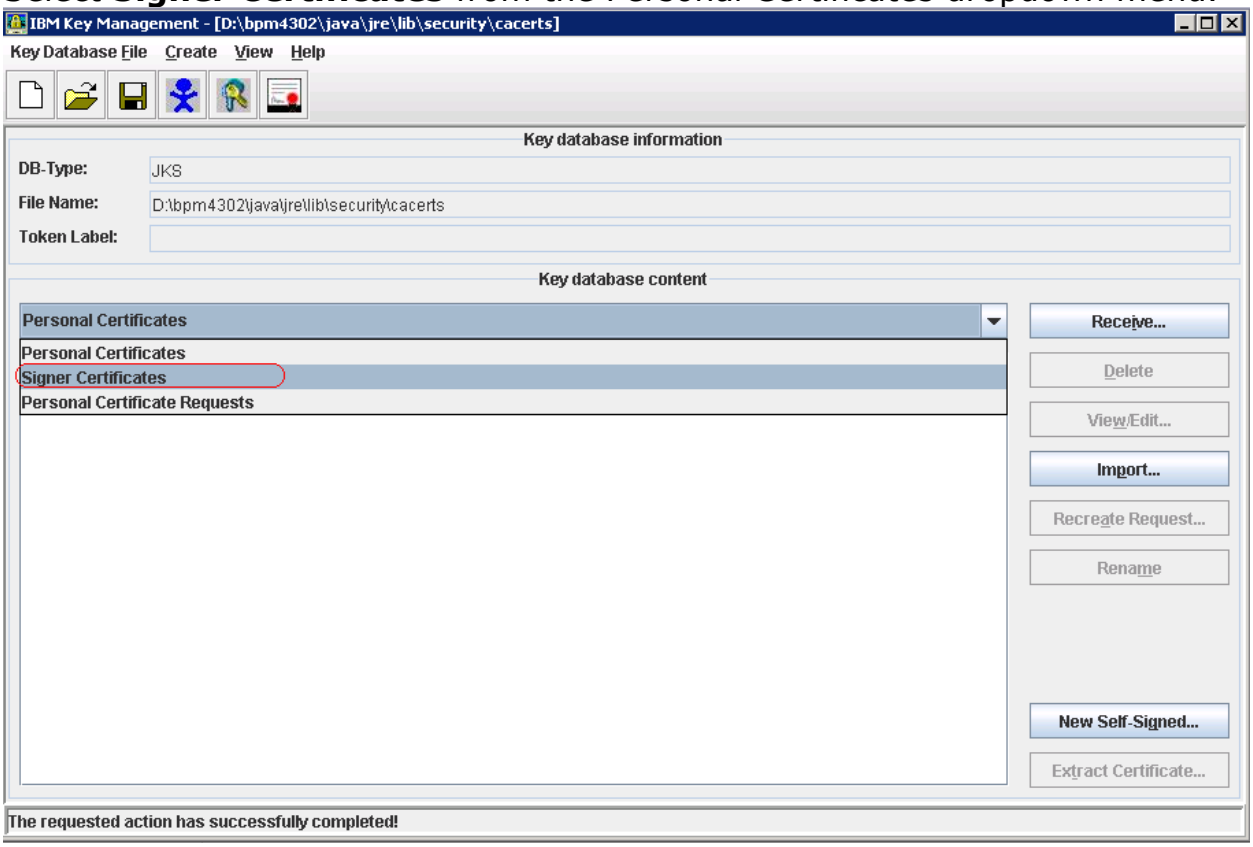
f) Click **OK**.



g) Provide the **Password**. Default is **changeit**.

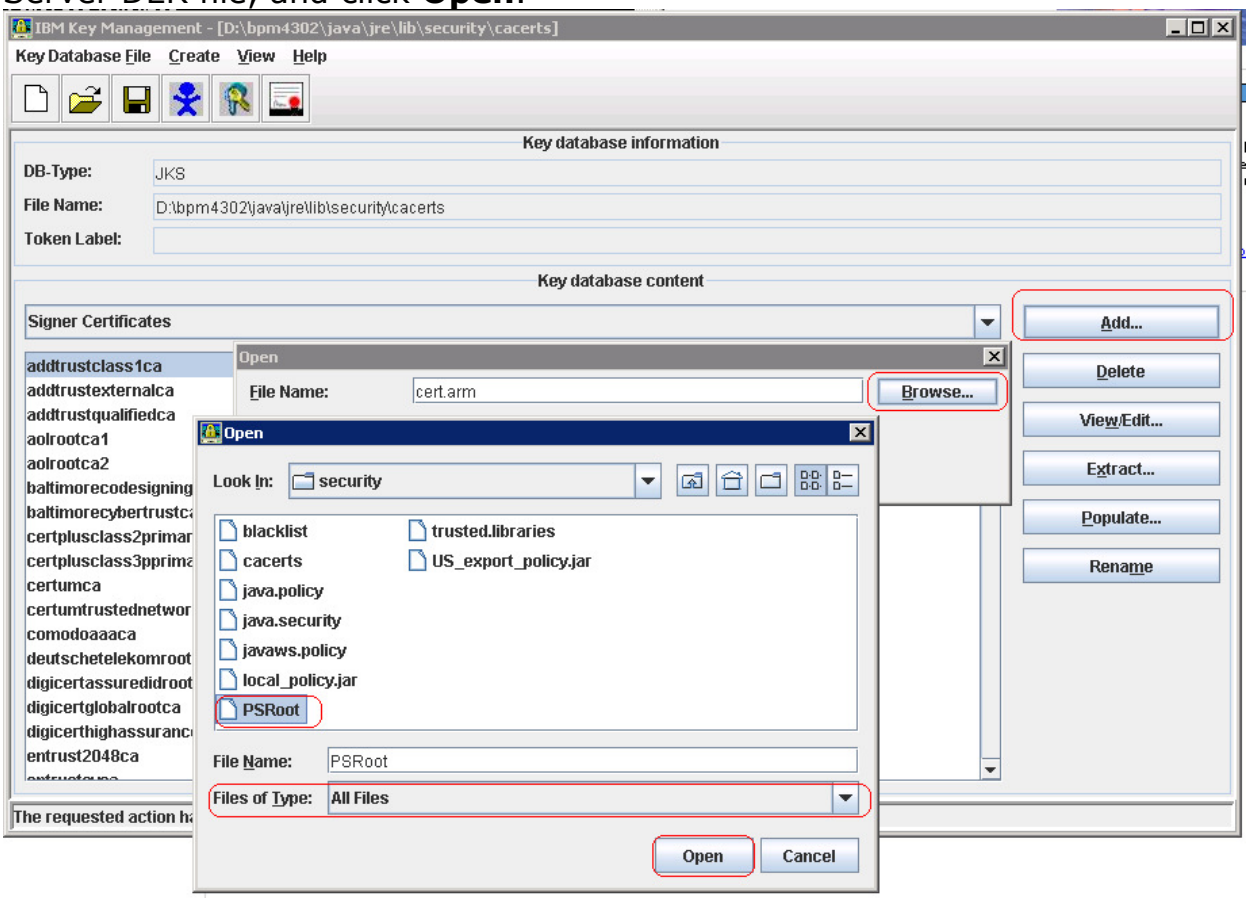


h) Select **Signer Certificates** from the Personal Certificates dropdown menu.

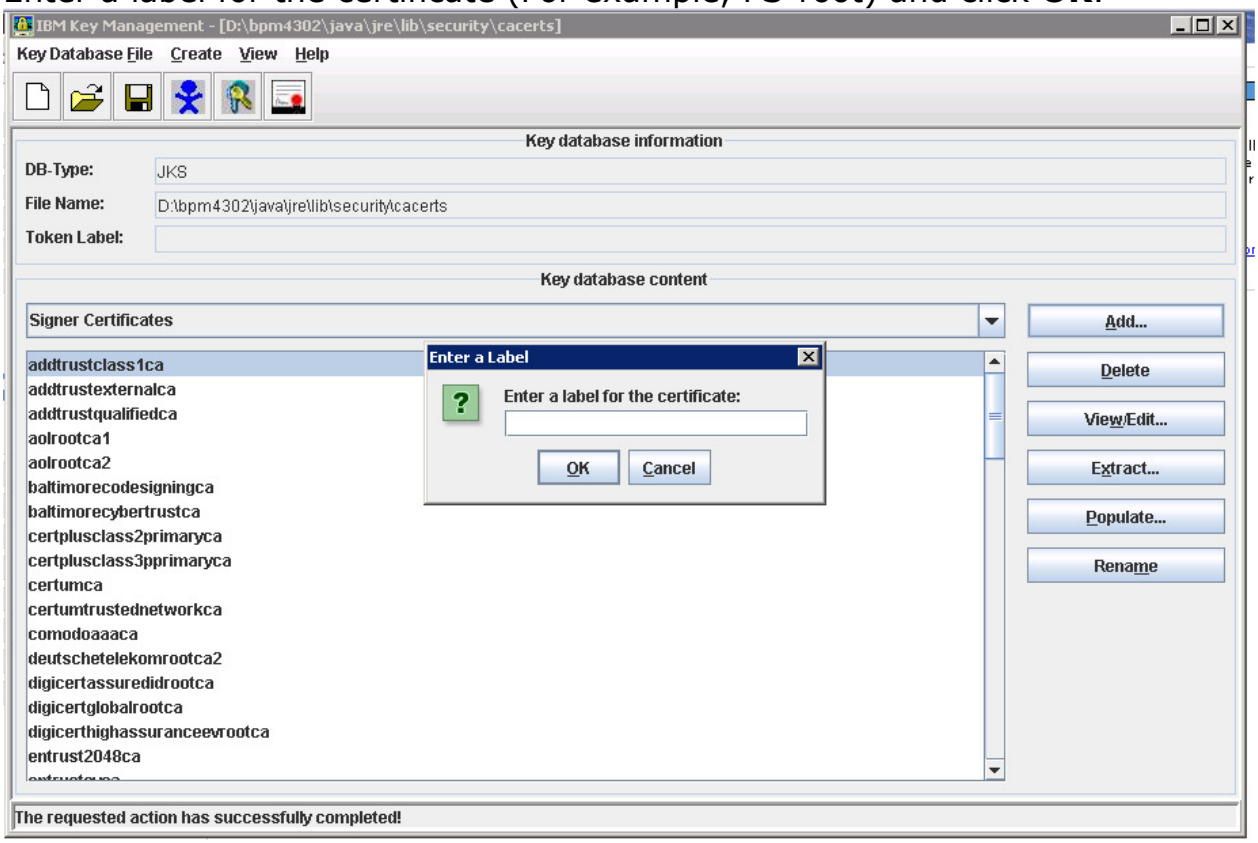


i) Click **Add**.

j) Change the **Files of Type** to **All Files**, select the location of the Process Server DER file, and click **Open**.



k) Enter a label for the certificate (For example, PS-root) and click **OK**.



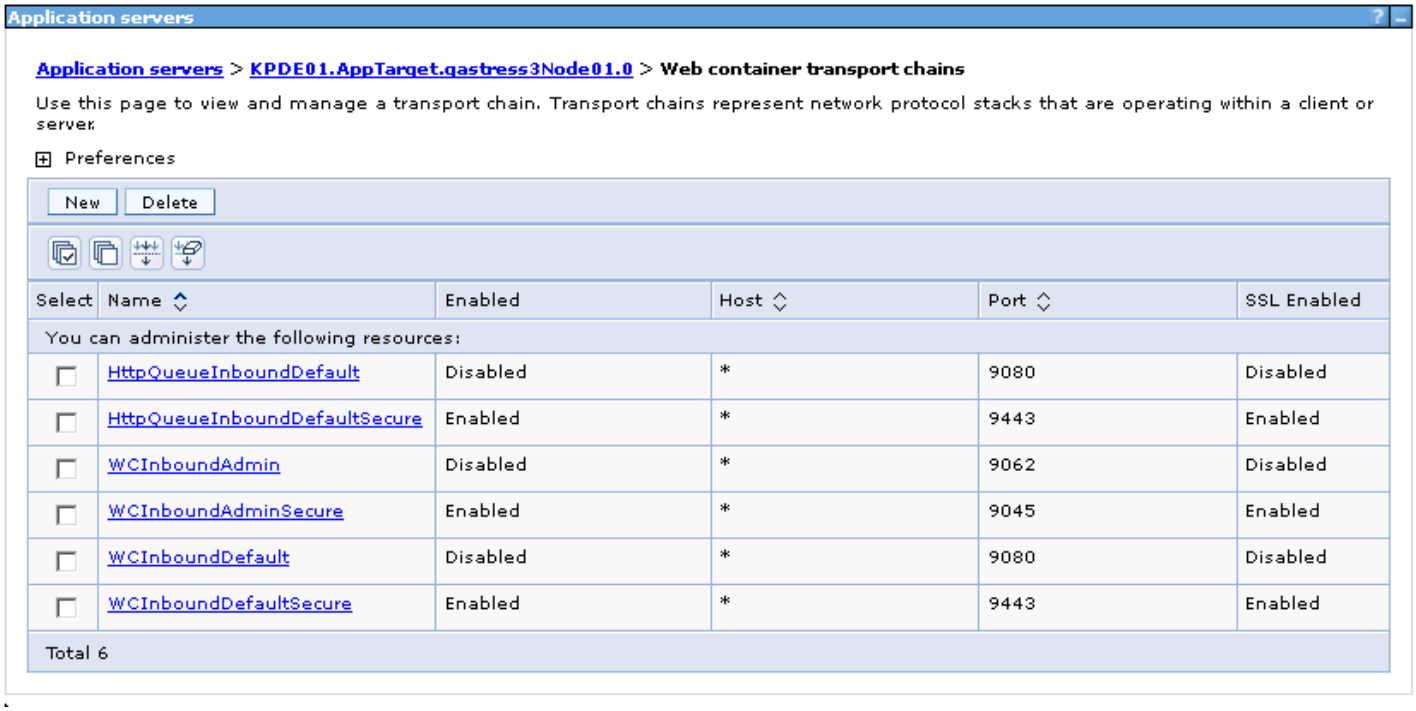
l) Close the ikeyman window.

2. Install the Process Center signer certificate in to the Process Server trust store.
   a) Invoke Process Server *WAS_HOME*/java/jre/bin/ikeyman.
   b) Set the Key database type to JKS.
   c) Click **Browse** and set the file location to *WAS_HOME*/java/jre/lib/security.
   d) Change the **Files of Type** to **All Files,** select **cacerts**, and click **Open**.
   e) Click **OK**.
   f) Provide the **Password**. Default is **changeit**.
   g) Select **Signer Certificates** from the Personal Certificates dropdown menu.
   h) Click **Add**.
   i) Change the **Files of Type** to **All Files**, select the location of the Process Center DER file, and click **Open**.
   j) Enter a label for the certificate (For example, Process Center-root) and click **OK**.
   k) Close the ikeyman window.

3. Restart the Process Server and Process Center servers.

Disable all unsecured ports on all Process Center and Process Server servers.

1. Log in to the WebSphere administrative console and navigate to **Servers > Server Types > WebSphere Application Servers**.
2. For each server, click on the server link, then go to **Container Settings > Web Container Settings > Web container transport chains**.
3. Click on each link for the unsecured port, for example, **HttpQueueInboundDefault**, and deselect the **Enabled** checkbox.
4. Repeat these steps for all Application Servers and all Nodes.



Verify the Process Server `100Custom.xml` file changes in the server

1. Open the `TeamWorksConfiguration.running.xml` file, which is located in the *`WAS_HOME`*`\profiles\`*`profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`server name`*`\process-server\` directory. Note: The TeamWorksConfiguration.running.xml file may not be available in every environment.
   Confirm the changes in the 100Custom.xml file. For example:
   `c:\BPM\profiles\ProcSrv01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-server\TeamWorksConfiguration.running.xml`

Verify the Process Center `100Custom.xml` file changes in the server

1. Open the `TeamWorksConfiguration.running.xml` file, which is located in the *`WAS_HOME`*`\profiles\`*`profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`server name`*`\process-center\` directory. Confirm the changes in the 100Custom.xml. For example:
   `c:\BPM\profiles\ProcCtr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\process-`

```
center\TeamWorksConfiguration.running.xml
```

*Note:
Depending on your environment, you may need to repeat the following steps for the personal certificate:
- Export the Process Center **root signer certificate**
- Export the Process Server **root signer certificate**
- Install Process Center signer certificate in Process Server trust store
- Install Process Server signer certificate in Process Center trust store

Verify your configuration

1. Log in to the Process Center console using an https connection.
2. From the Server tab, select **runtime server**, and click **configure server**. Confirm that it is opened in a secure browser with https.

Restart the Process Server and Process Center servers

1. Use admin console to stop the clusters.
2. Stop the node agent and deployment manager.
3. Re-start the node agent.
4. Re-start the deployment manager.
5. Use Admin console to start the clusters.

Importing an SSL security certificate into Integration Designer

In order to connect to an HTTPS enabled server, you need to import the SSL security certificate (X509Certificate) for the server. The steps described in this procedure are performed using Internet Explorer.

1. Launch your web browser and enter https://hostname:secure_port/ProcessCenter/login.jsp where hostname is the fully-qualified domain name of the process center server, and secure_port is the process center secure SSL port number.
2. On the Security Alert window, click View Certificate.
3. On the Certificate window, click the Details tab.
4. Click Copy to File to specify where to save the certificate file on your system.
5. In the wizard, click Next, accept the default values, and then click Next again.
6. Enter a file name for the security certificate, for example, pc_cert.cer, and click Next.
7. Click Finish. After you have created the SSL certificate, you can import it into the Java JRE that you will be using for Integration Designer.
8. Copy the certificate to IIDInstall\jdk\jre\bin where IIDInstall is the directory where you installed Integration Designer.

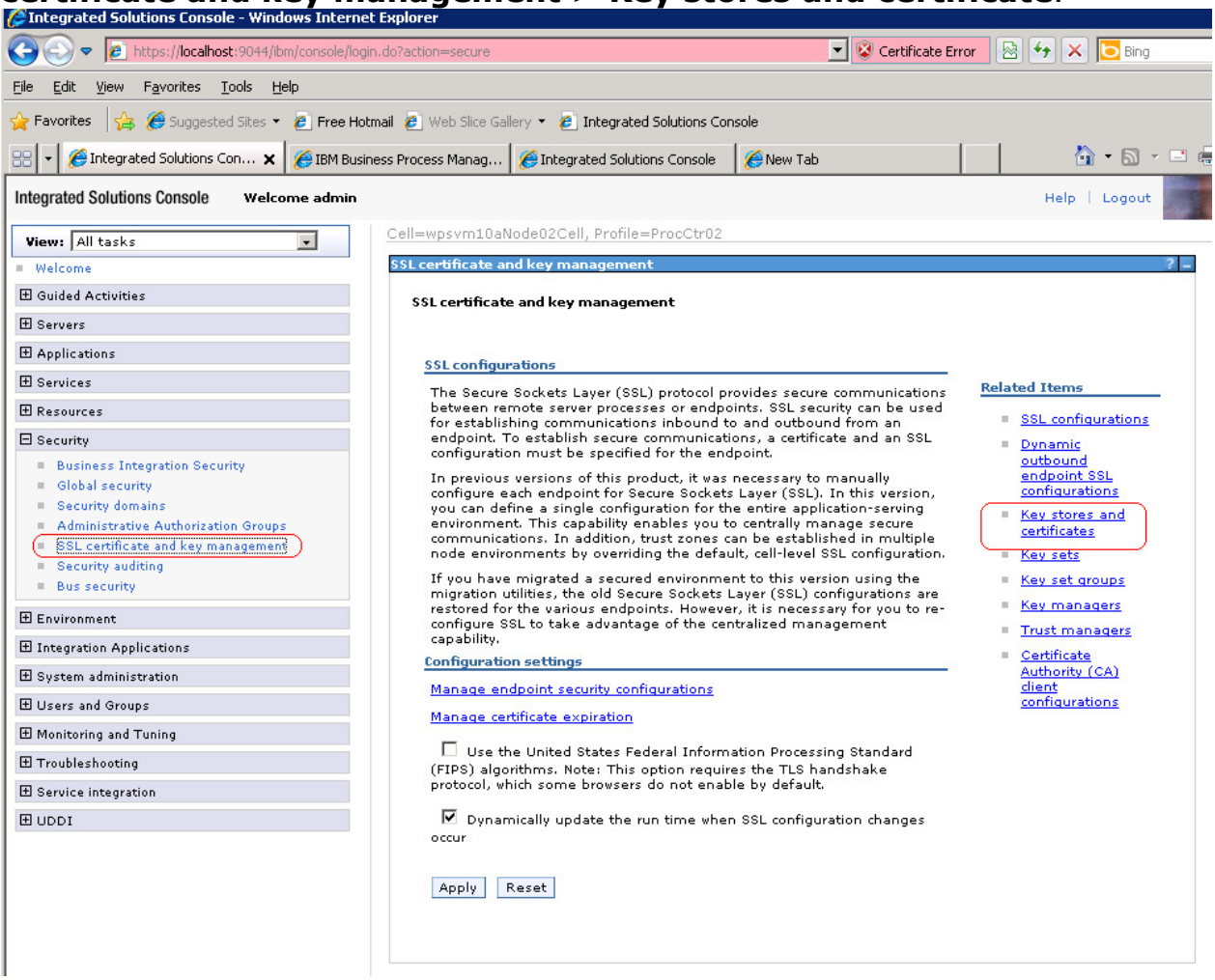
9. Switch to the same location in the command line and run the keytool command line as follows:
   a. keytool.exe -import -v -file <certificate file> -keystore ..\lib\security\cacerts
   If you previously imported SSL certificates into the Integration Designer, add the -alias <key name> parameter to specify a different key name to avoid name conflicts. The default value is mykey.
   b. Enter the keystore password: changeit (this is usually the default password).
   c. Enter y at the prompt to trust the certificate.

Configuring Secure Socket Layer (SSL) communication for a Network Deployment environment

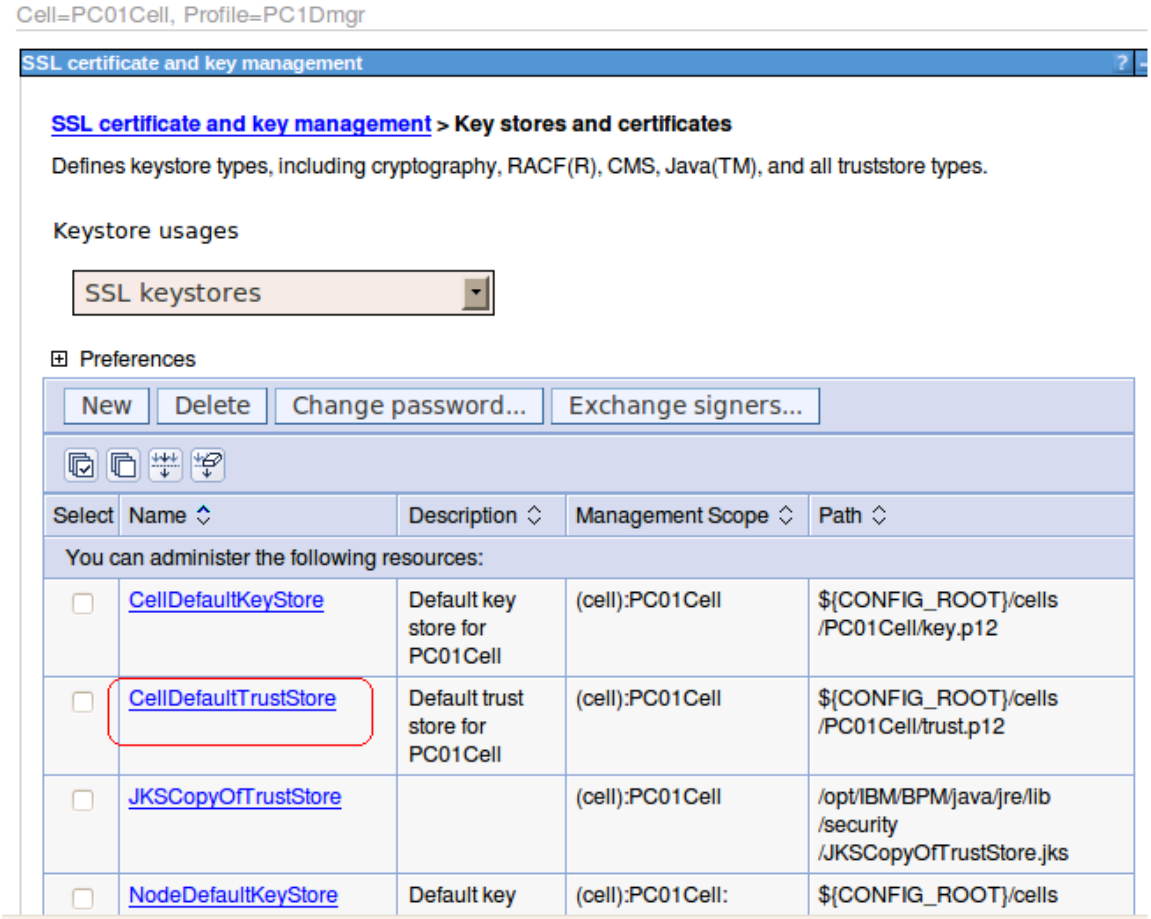
The following steps are required to make the communication between the Process Center and the Process Server work with https in a Network Deployment environment.

Import the Process Server WAS root SSL certificate into Process Center

1. On the Process center WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate**.

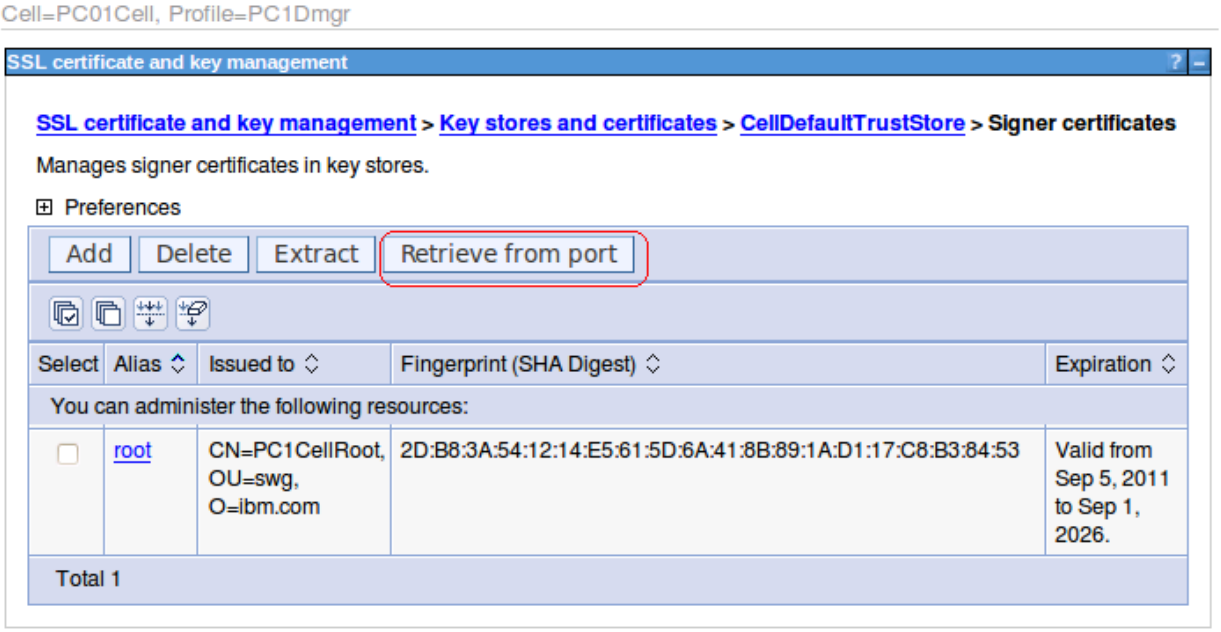


2. Click **CellDefaultTrustStore**.



3. Click **Signer certificates**.

4. Click **Retrieve from port**.



5. Enter the **Host** name, secure **Port** of the Profile (*WC_defaulthost_secure* of Process Server profile), and **Alias**, and click **Retrieve signer information**. You can retrieve the signer information for any of the servers listed.

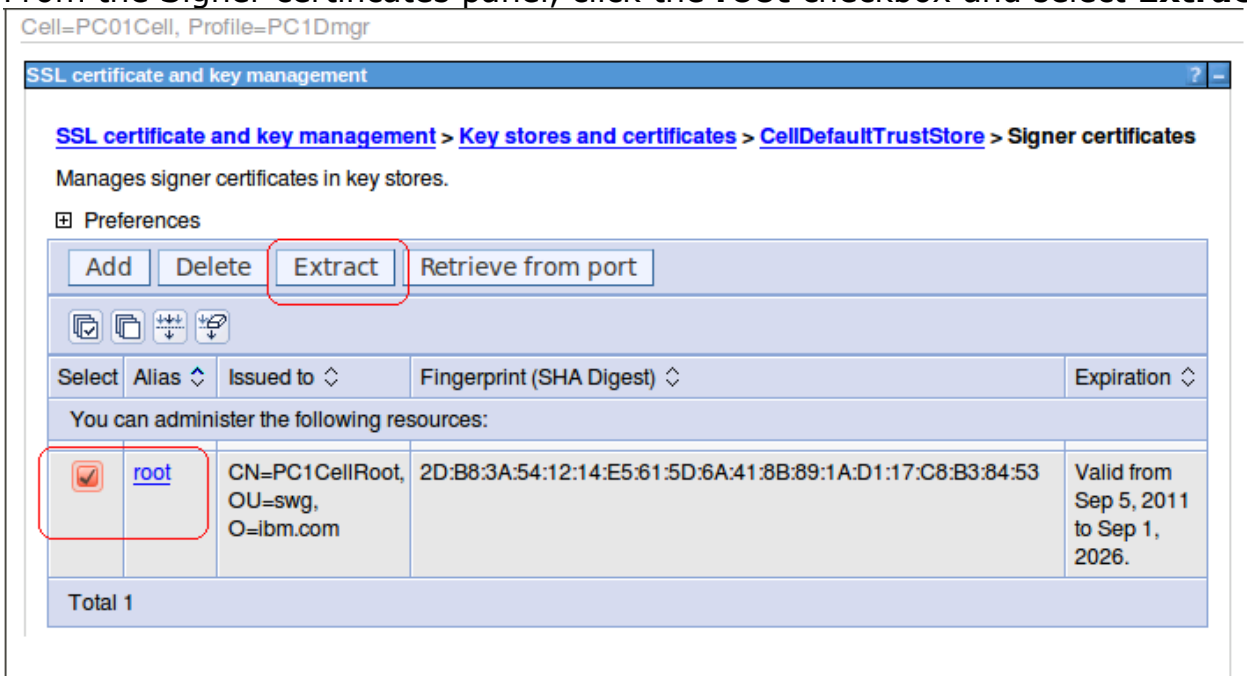
Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

6. Click **Apply** and save your changes.

Export the Process Center root signer certificate

1. On the Process center WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificate > CellDefaultTrustStore > Signer certificates**.

2. From the Signer certificates panel, click the **root** checkbox and select **Extract**.



3. Specify the **File name** path where you want to save the certificate and set the **Data type** to **Binary DER data**. Click **OK**.

4. Copy the extracted Process Center root certificate to the Process Server system

Import the Process Center WAS root SSL certificate into Process Server

1. On the Process server WAS admin console, navigate to **Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates > Retrieve from port**.

2. Enter the **Host** name, secure **Port** of the Profile (*WC_defaulthost_secure* of Process Center profile), and **Alias**, and click **Retrieve signer information**. You

can retrieve the signer information for any of the servers listed.

Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

3. Click **Apply** and save your changes.

Export the Process Server root signer certificate

1. On the Process server WAS admin console**, go to Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates**.

2. From the Signer certificates panel, click on the **Root** checkbox and select **Extract**.

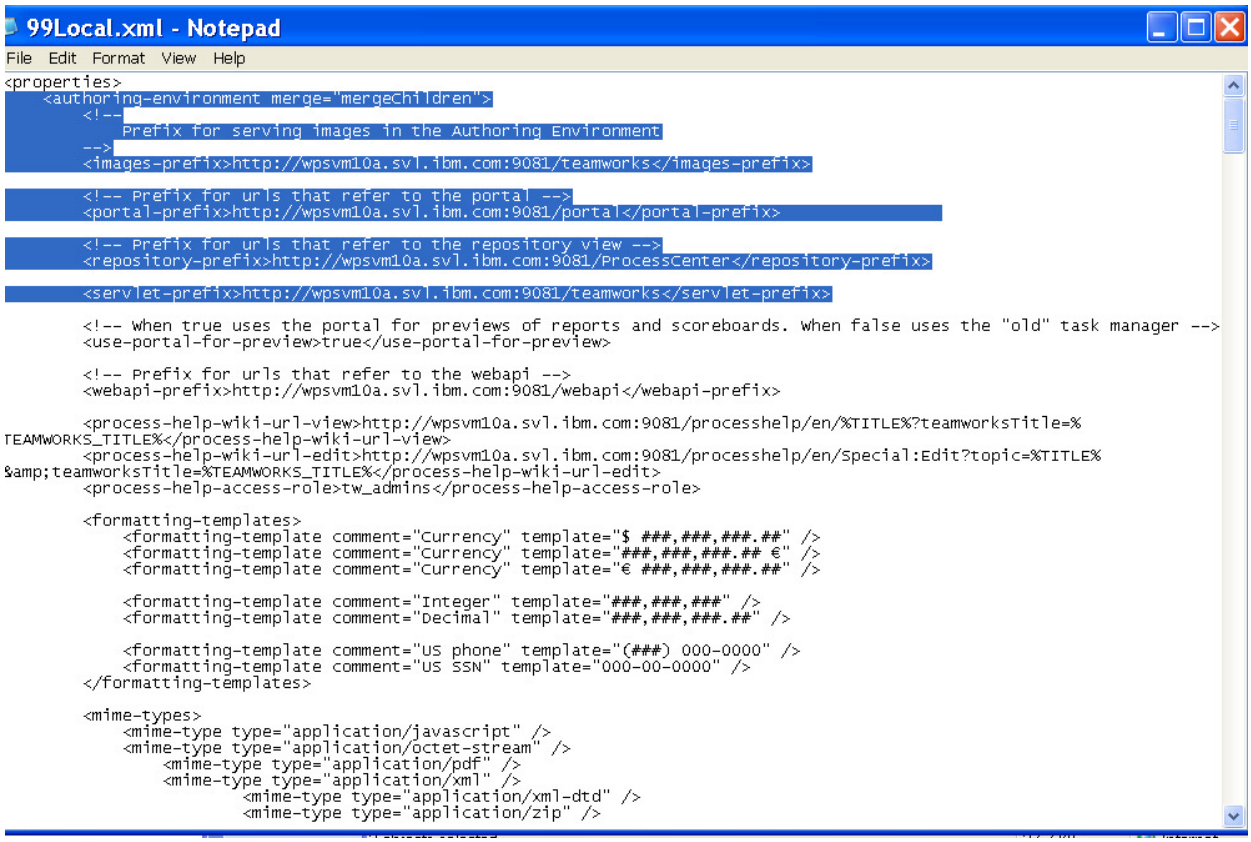
3. Specify the **File name** path where you want to save the certificate and set the **Data type** to **Binary DER data** and click **OK**.

Edit 100Custom.xml on Process Center

1. Edit `WAS_HOME\profiles\PC dmgr profile name\config\cells\cell name\nodes\node name\servers\app target server name\process-center\config\100Custom.xml` to overwrite values from the 99Local.xml file. For example: `c:\BPM\profiles\PCDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PC1.AppTarget.PC1Node1.0\process-center\config\100Custom.xml`.

2. Open `WAS_HOME\profiles\PC dmgr profile name\config\cells\cell name\nodes\node name\servers\app target server name\process-center\config\99local.xml`. For example: `c:\BPM\profiles\PCDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PC1.AppTarget.PC1Node1.0\process-center\config\system\99local.xml`.

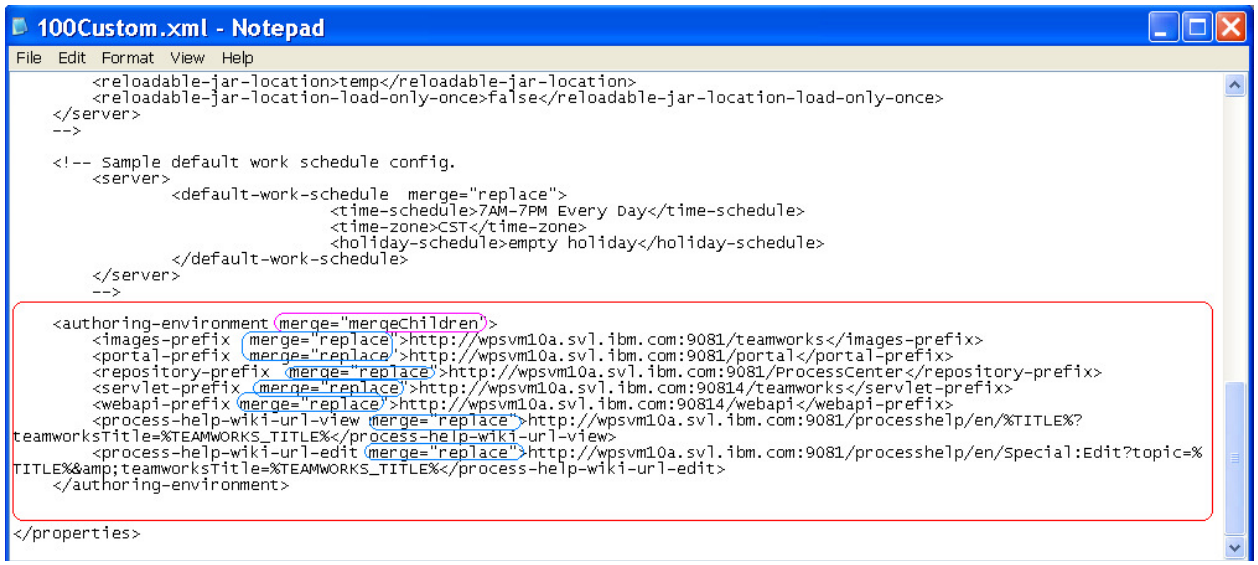
3. Copy all occurrences of `http://<PC_hostname>:<non_secured_port>` from the 99local.xml file, including its enclosing parent xml tags, and paste the same to the 100Custom.xml file.



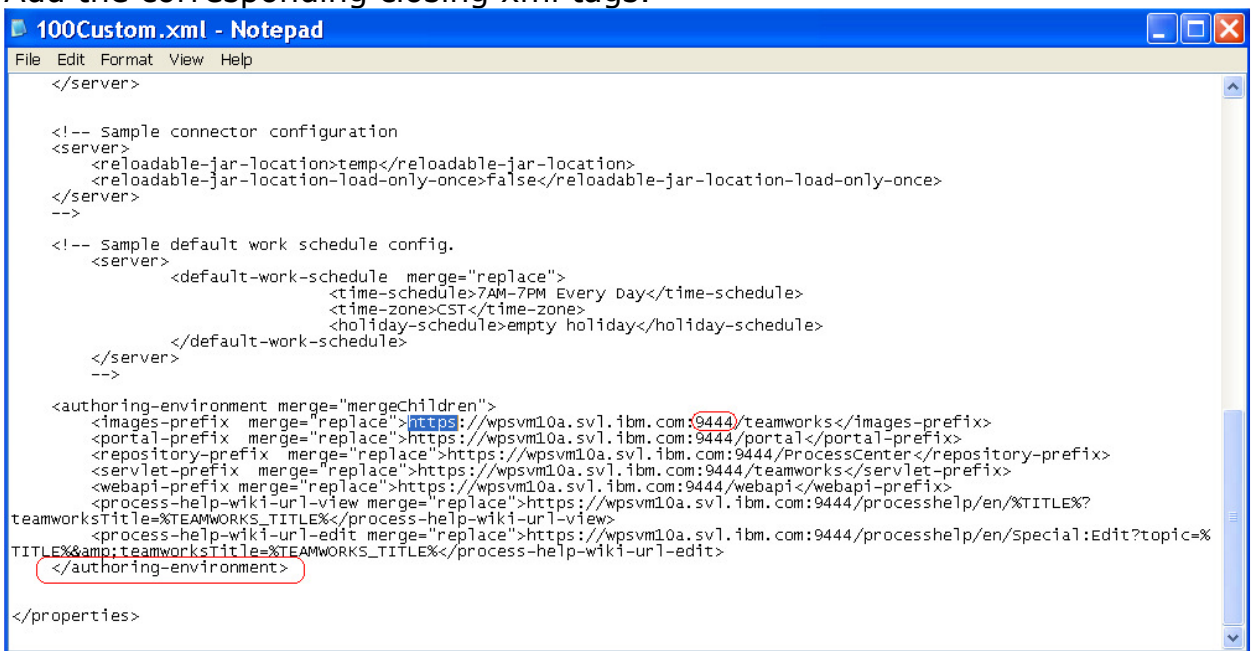
4. Add `merge="mergeChildren"` to the parent xml tags that contain `http://<PC_hostname>:<non_secured_port>`.

5. Add `merge="replace"` to the xml tag that contains `http://<PC_hostname>:<non_secured_port>`.

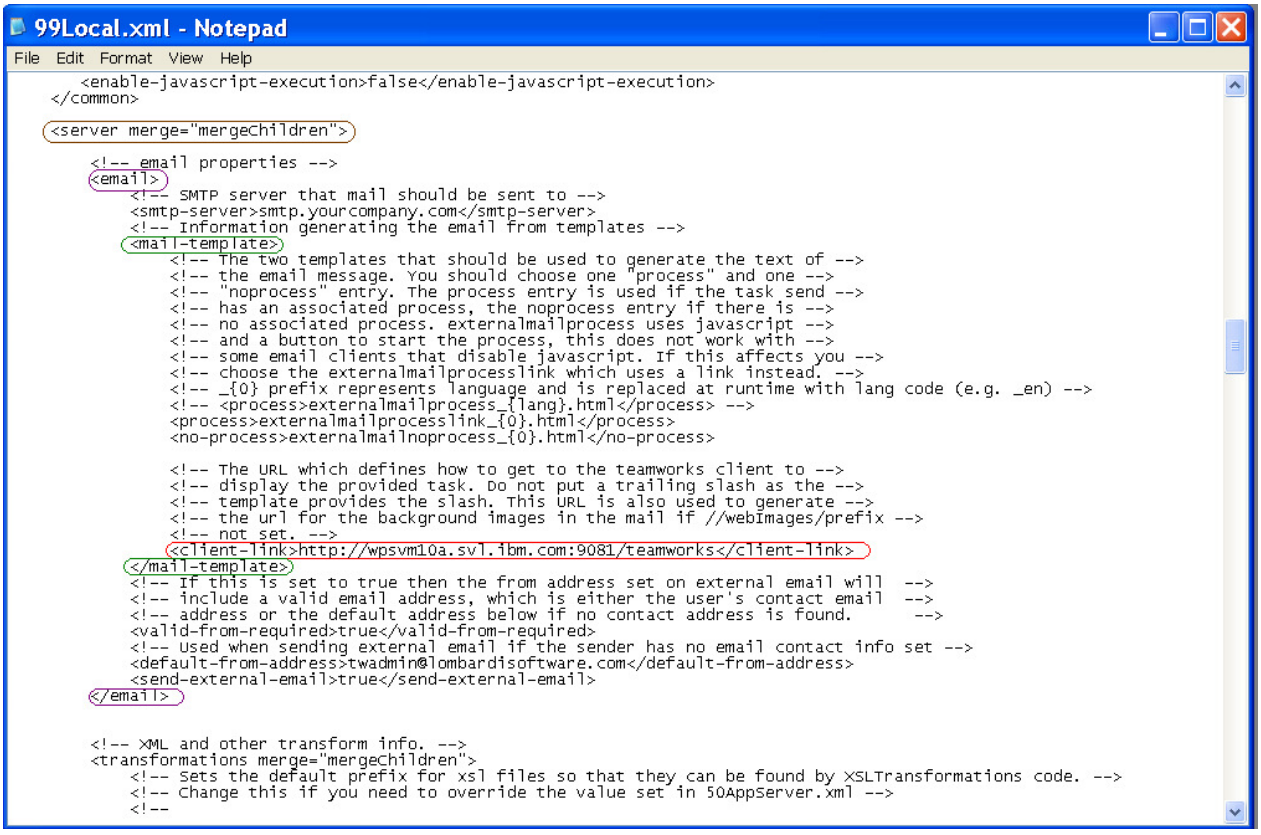
6. Change `http://<PC_hostname>:<non_secured_port>` to `https://<PC_hostname>:<secured-port>`.



7. Add the corresponding closing xml tags.



8. For the `<client-link>` tag that contains `http://<PC_hostname>:<non_secured_port>`, copy its parent tags up to the server tag.



9. Add the server section to the 100Custom.xml file.
   a. Add `merge="mergeChildren"` to the parent xml tags
   b. Add `merge="replace"` to the xml tag that contains `http://<PC_hostname>:<non_secured_port>`.

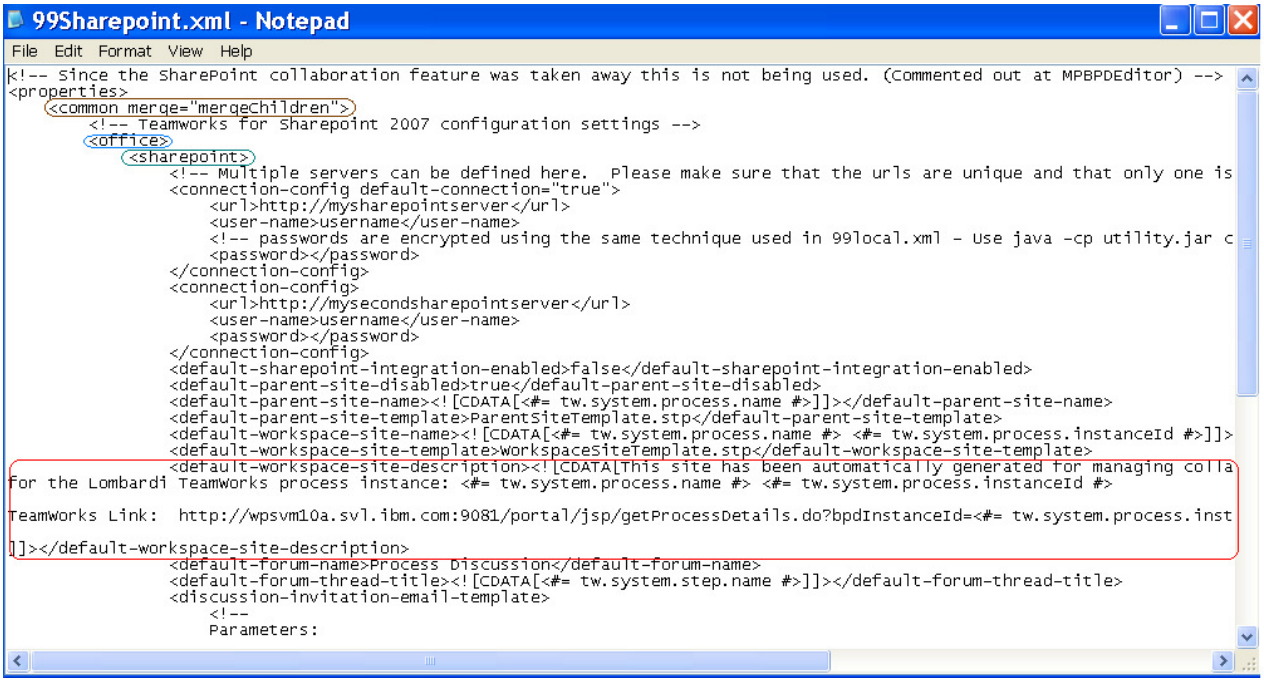
c. Change http://<PS_hostname>:<non_secured_port> to https://<PS_hostname>:<secured-port>.

10. Add the following to the <server> section to specify the correct Process Center secure port:
<server-port merge="replace"><*PC WC_defaulthost_secure port*></server-port> (set the value to *WC_defaulthost_secure* of Process Center profile).

Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

11. Open WAS_HOME\profiles*PC dmgr profile name*\config\cells*cell name*\nodes*node name*\servers*app target server name*\process-center\config\ system\99Sharepoint.xml. For example: c:\BPM\profiles\PCDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PC1.AppTarget.PC1Node1.0\process-center\config\system\99Sharepoint.xml.

12. Copy all occurrences of http://<PC_hostname>:<non_secured_port> from the 99Sharepoint.xml file, including its parent xml tags, and paste them to the 100Custom.xml file.



13. Change http://<PC_hostname>:<non_secured_port> to https://<PC_hostname>:<secured-port>.

14. Save and close the 100Custom.xml file.

Here is a sample Process Center 100Custom.xml file:

```
<properties>
    <!--Properties file for customer cluster scoped properties. -->

 <!-- set unversioned-po-caching-enable to false for clustering
    <common merge="mergeChildren">
        <environment-name merge="replace">My Environment</environment-name>
        <default-unversioned-po-cache-size merge="replace">500</default-unversioned-
po-cache-size>
       <default-versioned-po-cache-size merge="replace">500</default-versioned-po-
cache-size>
        <unversioned-po-caching-enable merge="replace">false</unversioned-po-
caching-enable>
       <default-webapi-userid-cache-size merge="replace">500</default-webapi-userid-
cache-size>
    </common>
    -->

    <!-- Sample connector configuration
    <server>
        <reloadable-jar-location>temp</reloadable-jar-location>
        <reloadable-jar-location-load-only-once>false</reloadable-jar-location-load-
only-once>
    </server>
    -->

    <!-- Sample default work schedule config.
```

```
 <server>
       <default-work-schedule  merge="replace">
                   <time-schedule>7AM-7PM Every Day</time-schedule>
                   <time-zone>CST</time-zone>
                   <holiday-schedule>empty holiday</holiday-schedule>
       </default-work-schedule>
 </server>
 -->
    <authoring-environment merge="mergeChildren">
        <images-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks</images-prefix>

        <portal-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/portal</portal-prefix>

        <repository-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/ProcessCenter</repository-
prefix>

        <servlet-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks</servlet-prefix>

        <webapi-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/webapi</webapi-prefix>

        <process-help-wiki-url-view
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/processhelp/en/%TITLE%?teamw
orksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-view>
        <process-help-wiki-url-edit
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/processhelp/en/Special:Edit?
topic=%TITLE%&amp;teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-edit>

    </authoring-environment>

    <common merge="mergeChildren">
        <portal-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/portal</portal-prefix>

        <process-admin-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/ProcessAdmin</process-admin-
prefix>

        <teamworks-webapp-prefix
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks</teamworks-webapp-
prefix>
        <webservices merge="mergeChildren">
            <base-url
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks/webservices</base-
url>
        </webservices>

        <xml-serialization merge="mergeChildren">
            <default-namespace-uri
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/schema/</default-namespace-
uri>
```

```
        </xml-serialization>
        <coach-designer-xsl-url
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks/coachdesigner/tran
sform/CoachDesigner.xsl</coach-designer-xsl-url>
        <office merge="mergeChildren">
            <sharepoint merge="mergeChildren">
                <default-workspace-site-description merge="replace"><![CDATA[This
site has been automatically generated for managing collaborations and documents
for the Lombardi TeamWorks process instance: <#= tw.system.process.name #> <#=
tw.system.process.instanceId #>

TeamWorks Link:
https://qastress3.eng1.svl.ibm.com:9443/portal/jsp/getProcessDetails.do?bpdInstanceI
d=<#= tw.system.process.instanceId #>

]]></default-workspace-site-description>
            </sharepoint>
        </office>
    </common>

    <server merge="mergeChildren">
        <email merge="mergeChildren">
            <mail-template merge="mergeChildren">
                <client-link
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/teamworks</client-link>
            </mail-template>
        </email>
        <repository-server-url
merge="replace">https://qastress3.eng1.svl.ibm.com:9443/ProcessCenter</repository-
server-url>
        <deploy-snapshot-using-https merge="replace">true</deploy-snapshot-using-
https>
        <server-port merge="replace">9443</server-port>

 </server>

</properties>
```

Edit 100Custom.xml on Process Server

1. Edit `WAS_HOME\profiles\`*`PS dmgr profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`app target server name`*`\process-server\config\100Custom.xml` to overwrite values from the 99Local.xml file. For example: `c:\BPM\profiles\PSDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\server1\PS1.AppTarget.PS1Node1.0\config\100Custom.xml`.

2. Open `WAS_HOME\profiles\`*`PS dmgr profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`app target server name`*`\process-server\config\99local.xml`. For example:

`c:\BPM\profiles\PSDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PS1.AppTarget.PS1Node1.0\process-server\config\system\99local.xml`.

3. Copy all occurrences of `http://<PS_hostname>:<non_secured_port>` from the 99local.xml file, including its enclosing parent xml tags, and paste the same to the 100Custom.xml file.

4. Add `merge="mergeChildren"` to the parent xml tags that contain `http://<PS_hostname>:<non_secured_port>`.

5. Add `merge="replace"` to the xml tag that contains `http://<PS_hostname>:<non_secured_port>`.

6. Change `http://<PS_hostname>:<non_secured_port>` to `https://<PS_hostname>:<secured-port>`.

7. Add the corresponding closing xml tags.

8. For the `<client-link>` tag that contains `http://<PS_hostname>:<non_secured_port>`, copy its parent tags up to the server tag.

9. Add the server section to the 100Custom.xml file.
   a. Add `merge="mergeChildren"` to the parent xml tags
   b. Add `merge="replace"` to the xml tag that contains `http://<PS_hostname>:<non_secured_port>`.
   c. Change `http://<PS_hostname>:<non_secured_port>` to `https://<PS_hostname>:<secured-port>`.

10. Search for *`repository-server-url`* in the server section of the 99local.xml file and copy it to the server section in the 100Custom.xml.

11. Change `http://<PC_hostname>:<non_secured_port>` to `https://<PC_hostname>:<secured-port>`.

12. Add the following to the `<server>` section to specify the correct Process Server secure port:
    `<server-port merge="replace">`*`<PS WC_defaulthost_secure port>`*`</server-port>` (set the value to *`WC_defaulthost_secure`* of Process Server profile).

    Note: The *WC_defaulthost_secure* is located in the WAS admin console. Navigate to **Servers > Server Types > WebSphere Application Servers > *SERVER_NAME* > Ports**.

13. Open WAS_HOME\profiles*PS dmgr profile name*\config\cells*cell name*\nodes*node name*\servers*app target server name*\process-server\config\system\99Sharepoint.xml. For example: c:\BPM\profiles\PSDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PS1.AppTarget.PS1Node1.0\process-server\config\system\99Sharepoint.xml).

14. Copy all occurrences of http://<PS_hostname>:<non_secured_port> in the 99Sharepoint.xml file, including its parent xml tags, to the 100Custom.xml file.

15. Change http://<PS_hostname>:<non_secured_port> to https://<PS_hostname>:<secured-port>.

16. Save and close the 100Custom.xml file.

Here is a sample Process Server 100Custom.xml file:

```
<properties>
    <!--Properties file for customer cluster scoped properties. -->


 <!-- set unversioned-po-caching-enable to false for clustering
    <common merge="mergeChildren">
        <environment-name merge="replace">My Environment</environment-name>
        <default-unversioned-po-cache-size merge="replace">500</default-unversioned-
po-cache-size>
       <default-versioned-po-cache-size merge="replace">500</default-versioned-po-
cache-size>
        <unversioned-po-caching-enable merge="replace">false</unversioned-po-
caching-enable>
       <default-webapi-userid-cache-size merge="replace">500</default-webapi-userid-
cache-size>
    </common>
    -->
<xml-serialization merge="mergeChildren">
     <default-namespace-uri
merge="replace">https://wpsvm10b.svl.ibm.com:9443/schema/</default-namespace-uri>
</xml-serialization>
    <!-- Sample connector configuration
    <server>
        <reloadable-jar-location>temp</reloadable-jar-location>
        <reloadable-jar-location-load-only-once>false</reloadable-jar-location-load-
only-once>
    </server>
    -->

    <!-- Sample default work schedule config.
 <server>
       <default-work-schedule  merge="replace">
                  <time-schedule>7AM-7PM Every Day</time-schedule>
                  <time-zone>CST</time-zone>
```

```
                <holiday-schedule>empty holiday</holiday-schedule>
        </default-work-schedule>
 </server>
 -->

    <authoring-environment merge="mergeChildren">
        <images-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks</images-prefix>

        <portal-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/portal</portal-prefix>

        <repository-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/ProcessCenter</repository-prefix>

        <servlet-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks</servlet-prefix>

        <use-portal-for-preview merge="replace">true</use-portal-for-preview>

        <webapi-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/webapi</webapi-prefix>

        <process-help-wiki-url-view
merge="replace">https://wpsvm10b.svl.ibm.com:9443/processhelp/en/%TITLE%?teamworksTi
tle=%TEAMWORKS_TITLE%</process-help-wiki-url-view>
        <process-help-wiki-url-edit
merge="replace">https://wpsvm10b.svl.ibm.com:9443/processhelp/en/Special:Edit?topic=
%TITLE%&amp;teamworksTitle=%TEAMWORKS_TITLE%</process-help-wiki-url-edit>
    </authoring-environment>

    <common merge="mergeChildren">
        <portal-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/portal</portal-prefix>

        <process-admin-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/ProcessAdmin</process-admin-
prefix>

        <teamworks-webapp-prefix
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks</teamworks-webapp-
prefix>

        <webservices merge="mergeChildren">
            <base-url
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks/webservices</base-url>
        </webservices>
        <coach-designer-xsl-url
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks/coachdesigner/transform/
CoachDesigner.xsl</coach-designer-xsl-url>

        <office merge="mergeChildren">
            <sharepoint merge="mergeChildren">
                <default-workspace-site-description merge="replace"><![CDATA[This
site has been automatically generated for managing collaborations and documents
```

```
for the Lombardi TeamWorks process instance: <#= tw.system.process.name #> <#=
tw.system.process.instanceId #>

TeamWorks Link:
https://wpsvm10b.svl.ibm.com:9443/portal/jsp/getProcessDetails.do?bpdInstanceId=<#=
tw.system.process.instanceId #>

]]></default-workspace-site-description>
            </sharepoint>
        </office>
    </common>

    <server merge="mergeChildren">

        <!-- email properties -->
        <email merge="mergeChildren">
            <mail-template merge="mergeChildren" >
                <client-link
merge="replace">https://wpsvm10b.svl.ibm.com:9443/teamworks</client-link>
            </mail-template>
        </email>

        <repository-server-url
merge="replace">https://qastress3.svl.ibm.com:9443/ProcessCenter</repository-server-
url>
        <server-port merge="replace">9443</server-port>
    </server>

</properties>
```

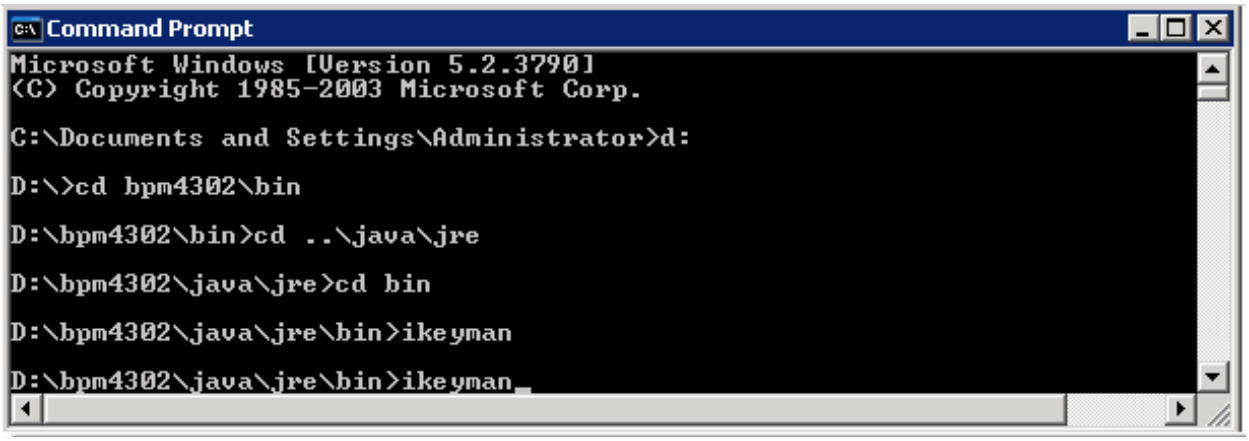
SSL communication between Process Server and Process Center Server

Make sure that the SSL communication between the Process Server and the Process Center Server work by adding the certificates to each other's trust store.

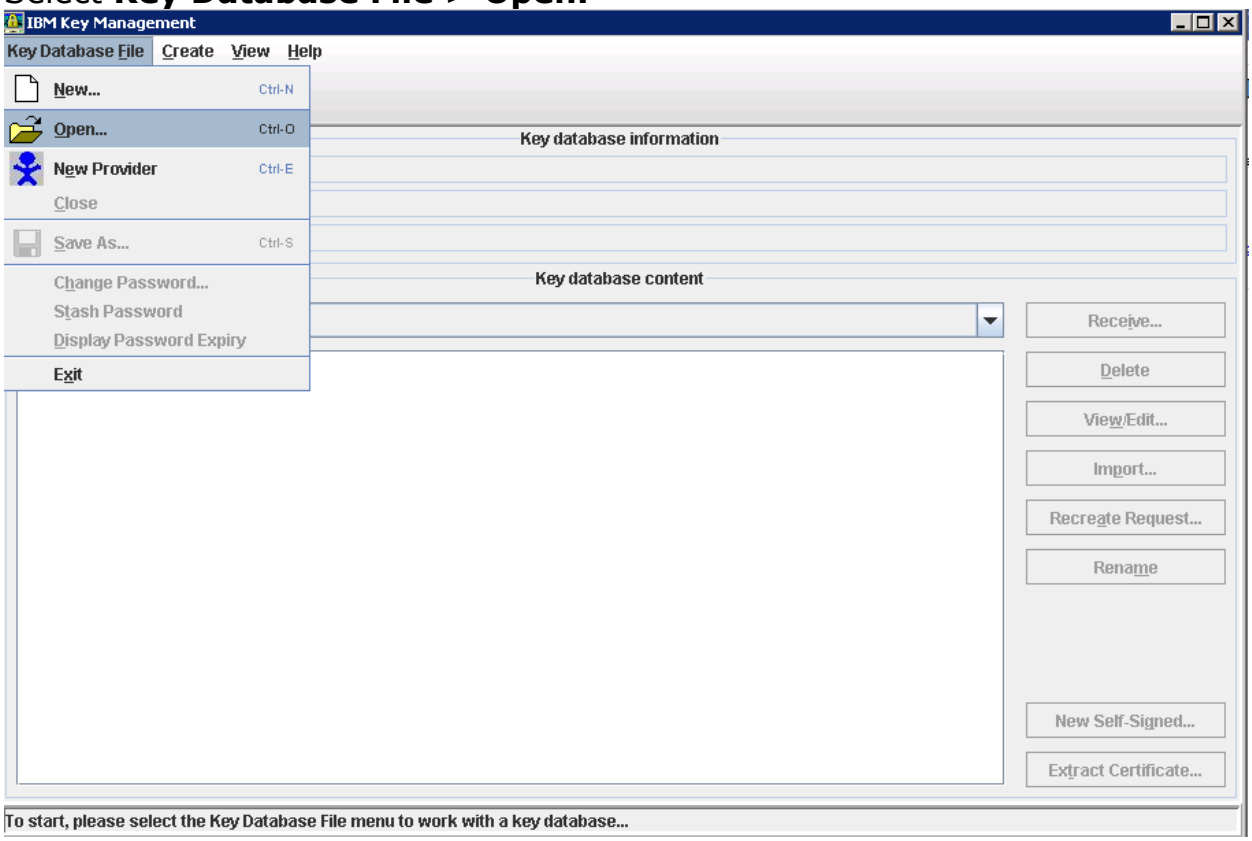
Important: If the Process Center and clustered runtime servers were started before you begin to configure SSL, and the LSW_SERVER table on the Process Center database contains the non-secure port of the Process Server, you must delete the Process Server from the Process Center repository:

1. Stop Process Server.
2. From the Servers tab on the Process Center Console, delete Process Server from the Process Center repository.
3. Delete the record with the non-secure port from the LSW_SERVER table on the Process Center database.
4. Start Process Server.

1. Install the Process Server signer certificate in to the Process Center trust store.
   a) Invoke Process Center: `WAS_HOME/java/jre/bin/ikeyman`.



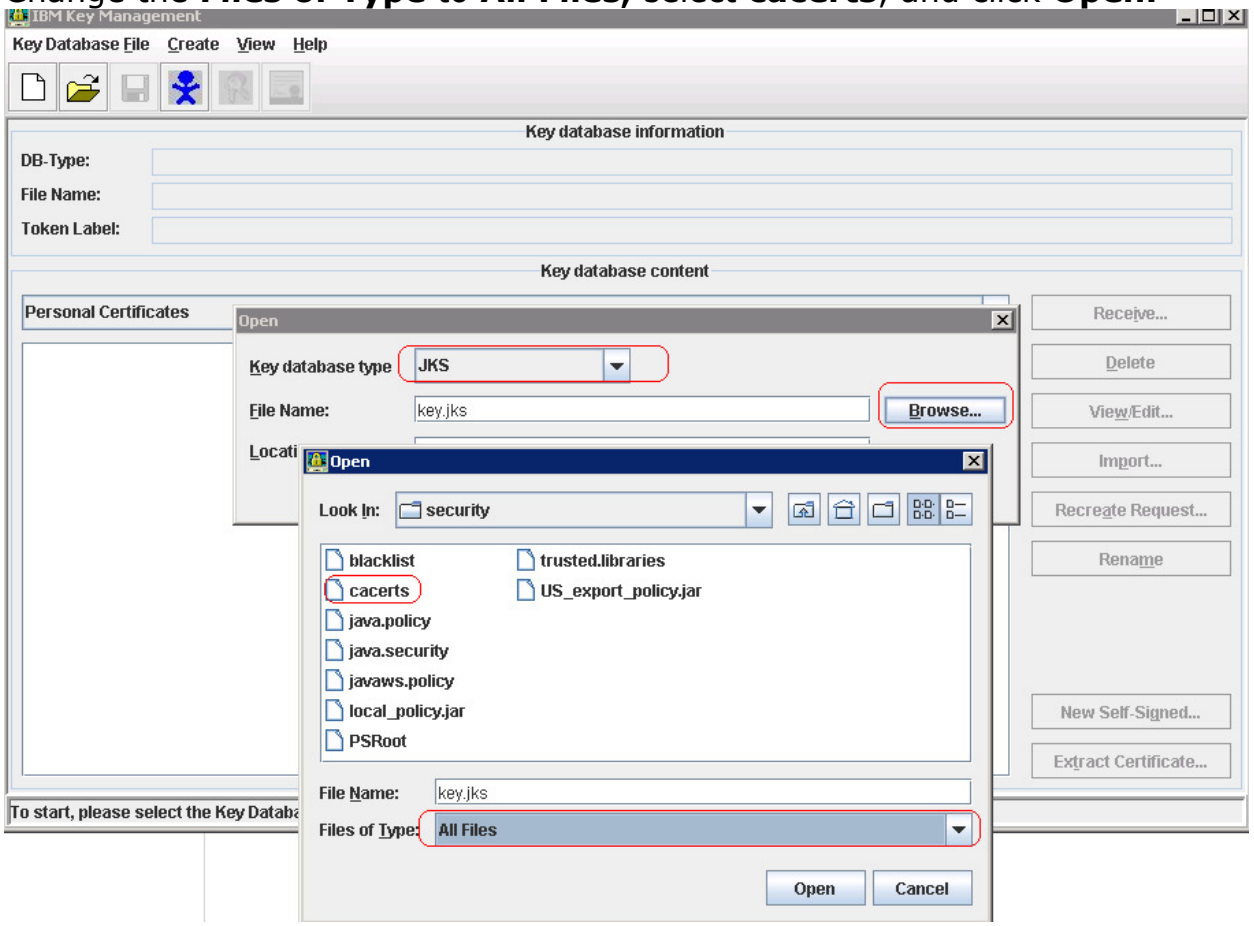
b) Select **Key Database File > Open.**



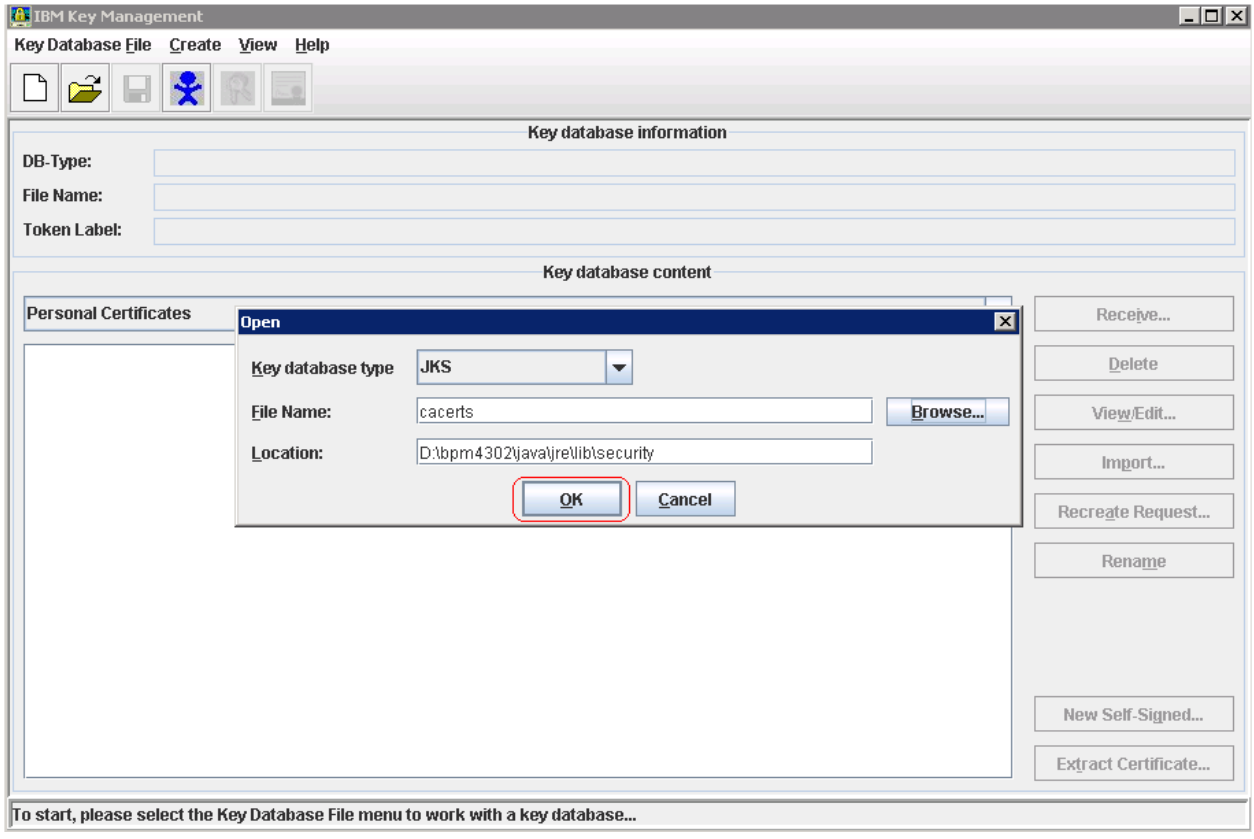
c) Set the Key database type to JKS.

d) Click **Browse** and set the file location to *WAS_HOME*`/java/jre/lib/security`.

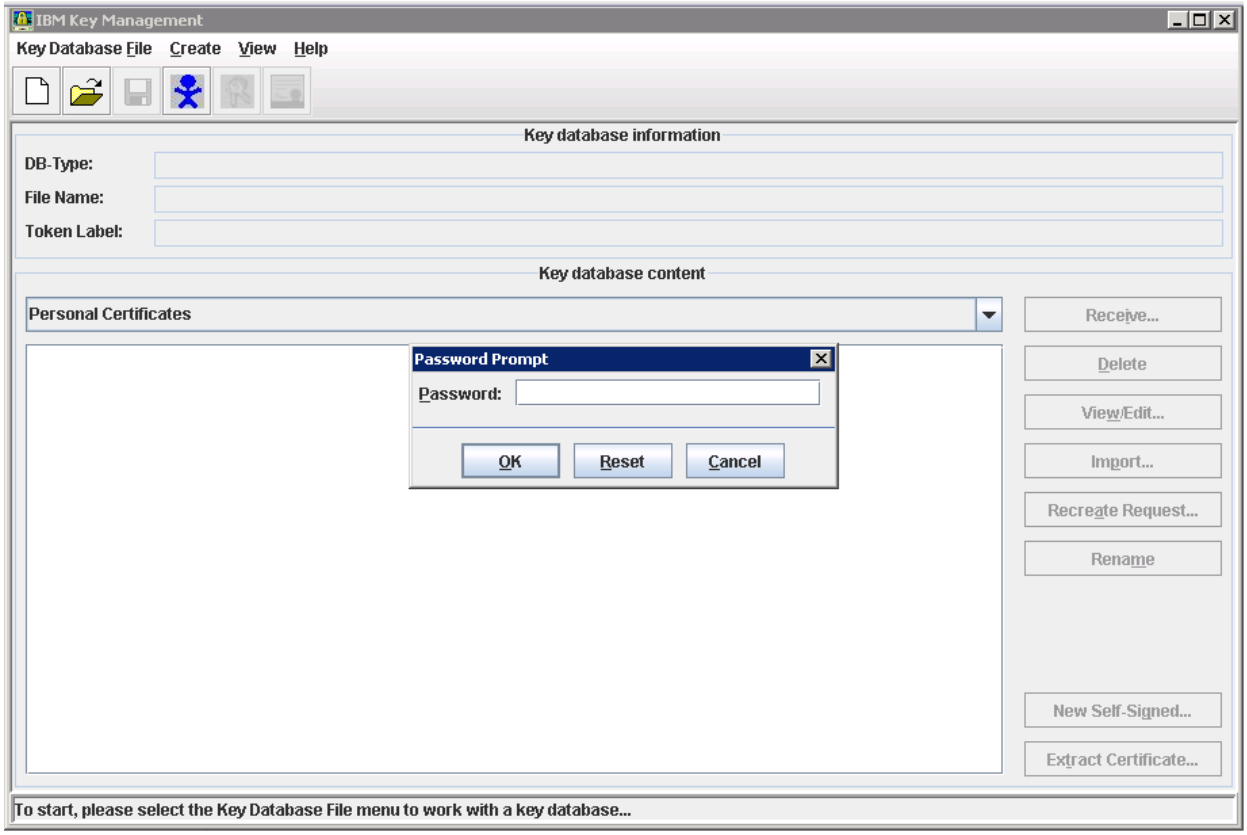
e) Change the **Files of Type** to **All Files,** select **cacerts**, and click **Open.**



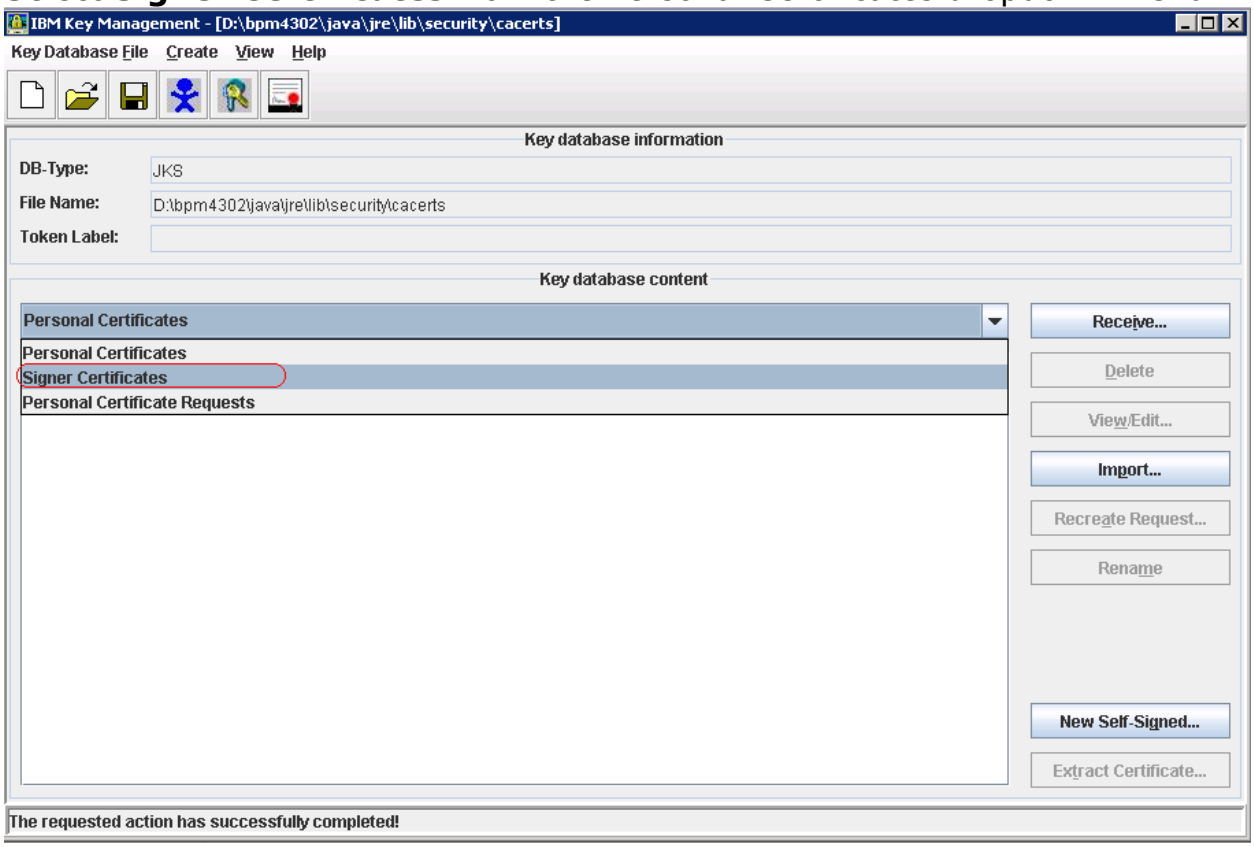
f) Click OK.



g) Provide the **Password**. Default is **changeit**.

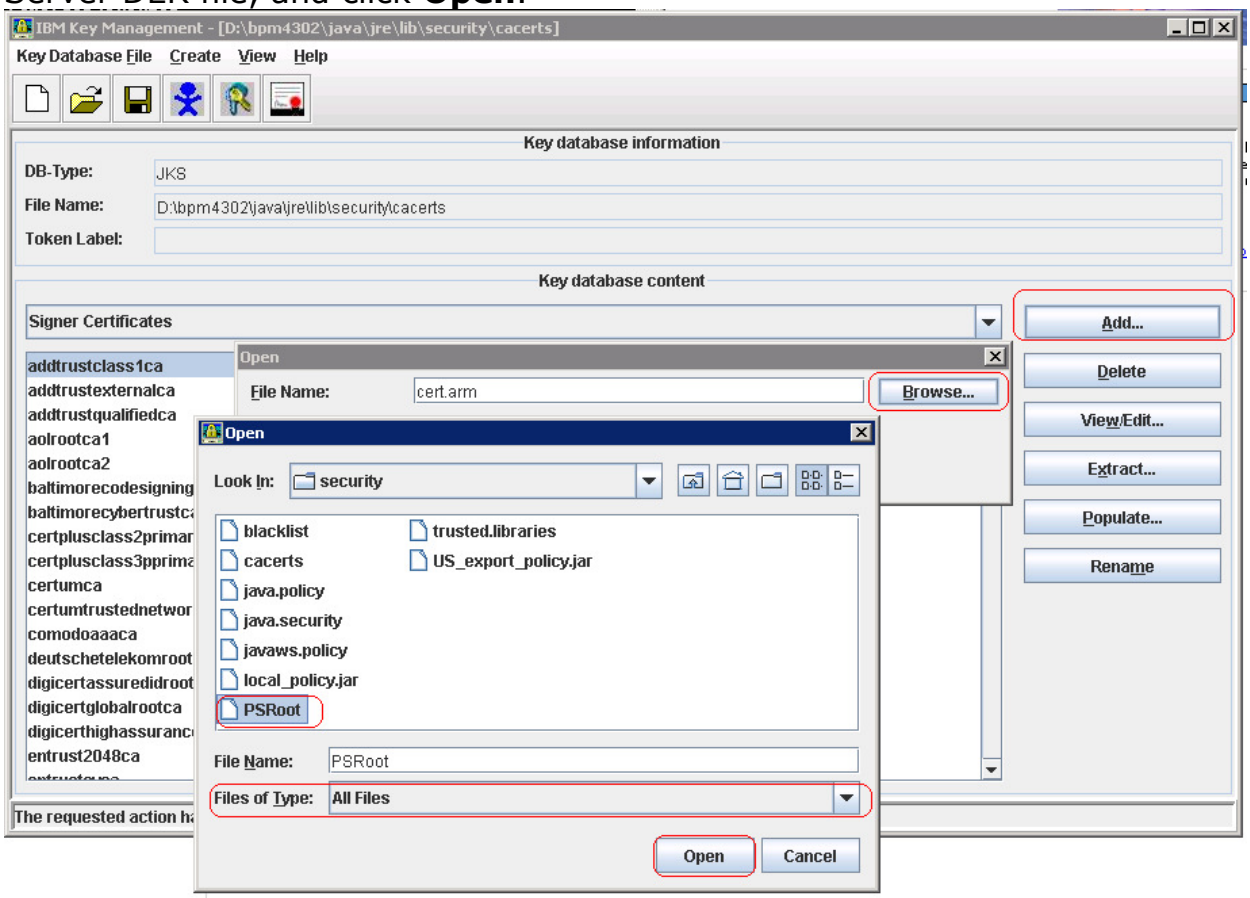


h) Select **Signer Certificates** from the Personal Certificates dropdown menu.

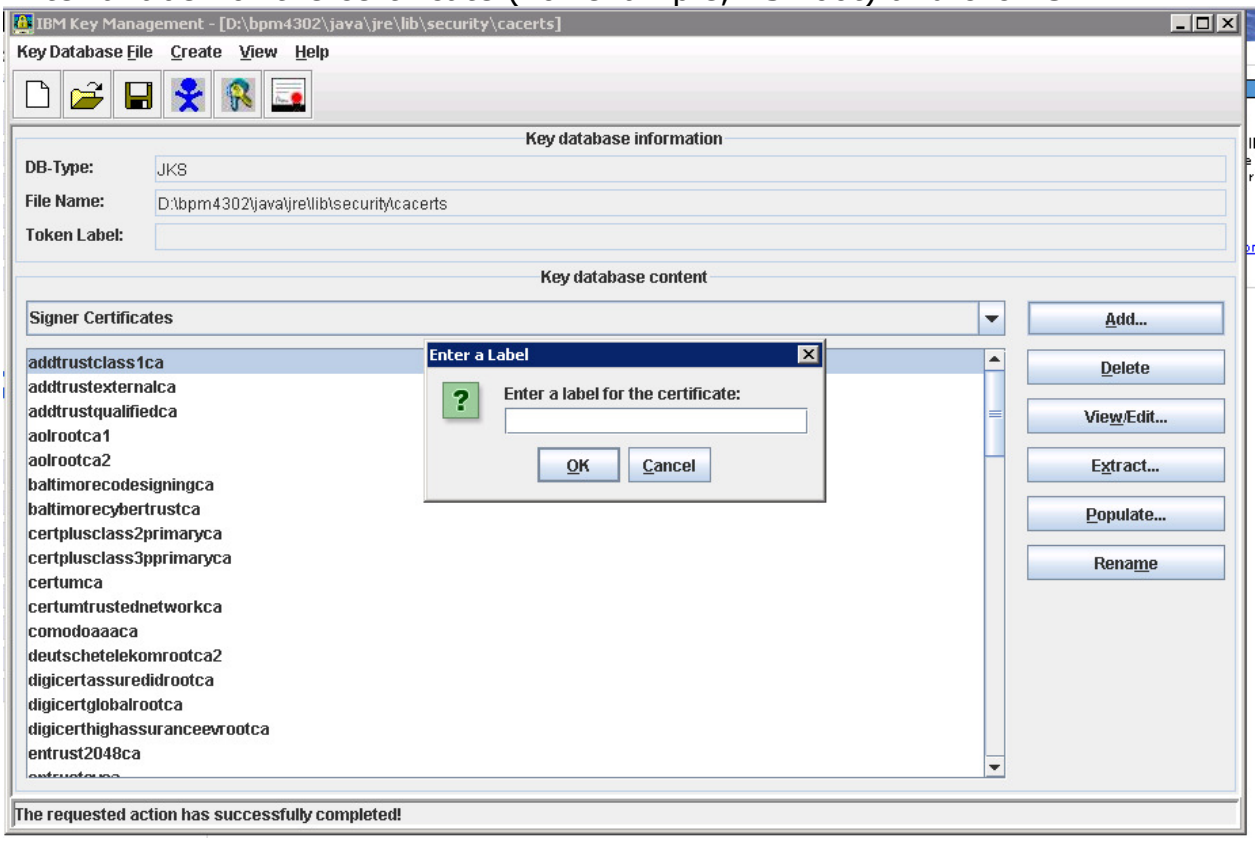


i) Click **Add**.

j) Change the **Files of Type** to **All Files**, select the location of the Process Server DER file, and click **Open**.



k) Enter a label for the certificate (For example, PS-root) and click **OK.**

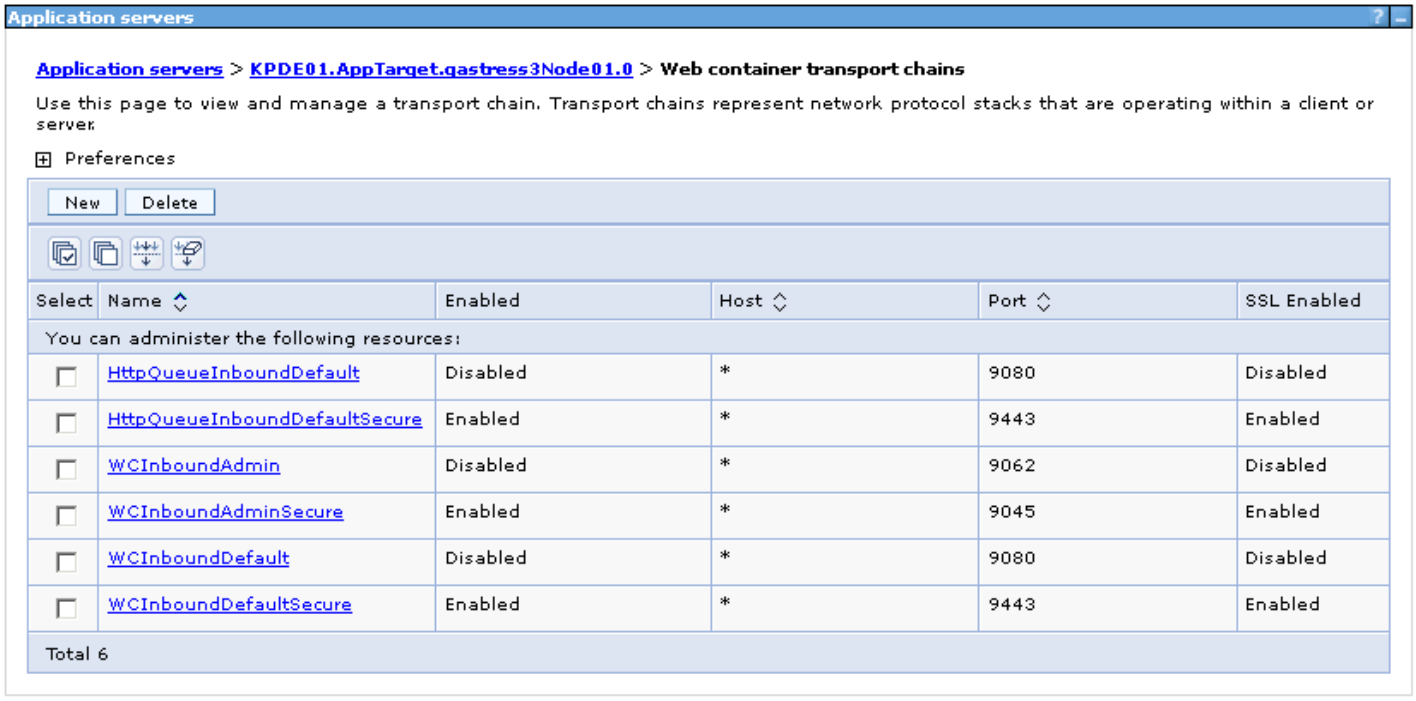


l) Close the ikeyman window.

2. Install the Process Center signer certificate in to the Process Server trust store.
   a) Invoke Process Server *WAS_HOME*/java/jre/bin/ikeyman.
   b) Set the Key database type to JKS.
   c) Click **Browse** and set the file location to *WAS_HOME*/java/jre/lib/security.
   d) Change the **Files of Type** to **All Files,** select **cacerts**, and click **Open**.
   e) Click **OK**.
   f) Provide the **Password**. Default is **changeit**.
   g) Select **Signer Certificates** from the Personal Certificates dropdown menu.
   h) Click **Add**.
   i) Change the **Files of Type** to **All Files**, select the location of the Process Center DER file, and click **Open**.
   j) Enter a label for the certificate (For example, Process Center-root) and click **OK**.
   k) Close the ikeyman window.

Disable all unsecured ports on all Process Center and Process Server servers.

1. Log in to the WebSphere administrative console and navigate to **Servers > Server Types > WebSphere Application Servers**.
2. For each server, click on the server link, then go to **Container Settings > Web Container Settings > Web container transport chains**.
3. Click on each link for the unsecured port, for example, **HttpQueueInboundDefault**, and deselect the **Enabled** checkbox.
4. Repeat these steps for all WebSphere Application Server cluster members on all nodes. For example, if the *xxx.AppTarget* cluster has members on Node1 and Node2, these steps must be performed on both nodes.



Verify the Process Server `100Custom.xml` file changes in the server

1. Open the `TeamWorksConfiguration.running.xml` file, which is located in the *`WAS_HOME`*`\profiles\`*`PS dmgr profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`app target server name`*`\process-server\` directory. Confirm the changes in the 100Custom.xml file. For example:
   `c:\BPM\profiles\PSDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PS1.AppTarget.PS1Node1.0\process-server\TeamWorksConfiguration.running.xml`

Verify the Process Center `100Custom.xml` file changes in the server

1. Open the `TeamWorksConfiguration.running.xml` file, which is located in the *`WAS_HOME`*`\profiles\`*`PC dmgr profile name`*`\config\cells\`*`cell name`*`\nodes\`*`node name`*`\servers\`*`app target server name`*`\process-center\` directory. Note: The TeamWorksConfiguration.running.xml file may not be available in every environment.
   Confirm the changes in the 100Custom.xml. For example:
   `c:\BPM\profiles\PCDmgr01\config\cells\gascogne01Cell\nodes\gascogneNode01\servers\PC1.AppTarget.PC1Node1.0\process-center\TeamWorksConfiguration.running.xml`

   *Note:
   Depending on your environment, you may need to repeat the following steps for the personal certificate:
   - Export the Process Center **root signer certificate**
   - Export the Process Server **root signer certificate**
   - Install Process Center signer certificate in Process Server trust store
   - Install Process Server signer certificate in Process Center trust store

Restart the Process Server and Process Center servers

6. Use admin console to stop the clusters.
7. Stop the node agent and deployment manager.
8. Re-start the node agent.
9. Re-start the deployment manager.
10. Use Admin console to start the clusters.

Verify your configuration

1. Log in to the Process Center console using an https connection.
2. From the Server tab, select **runtime server**, and click **configure server**. Confirm that it is opened in a secure browser with https.

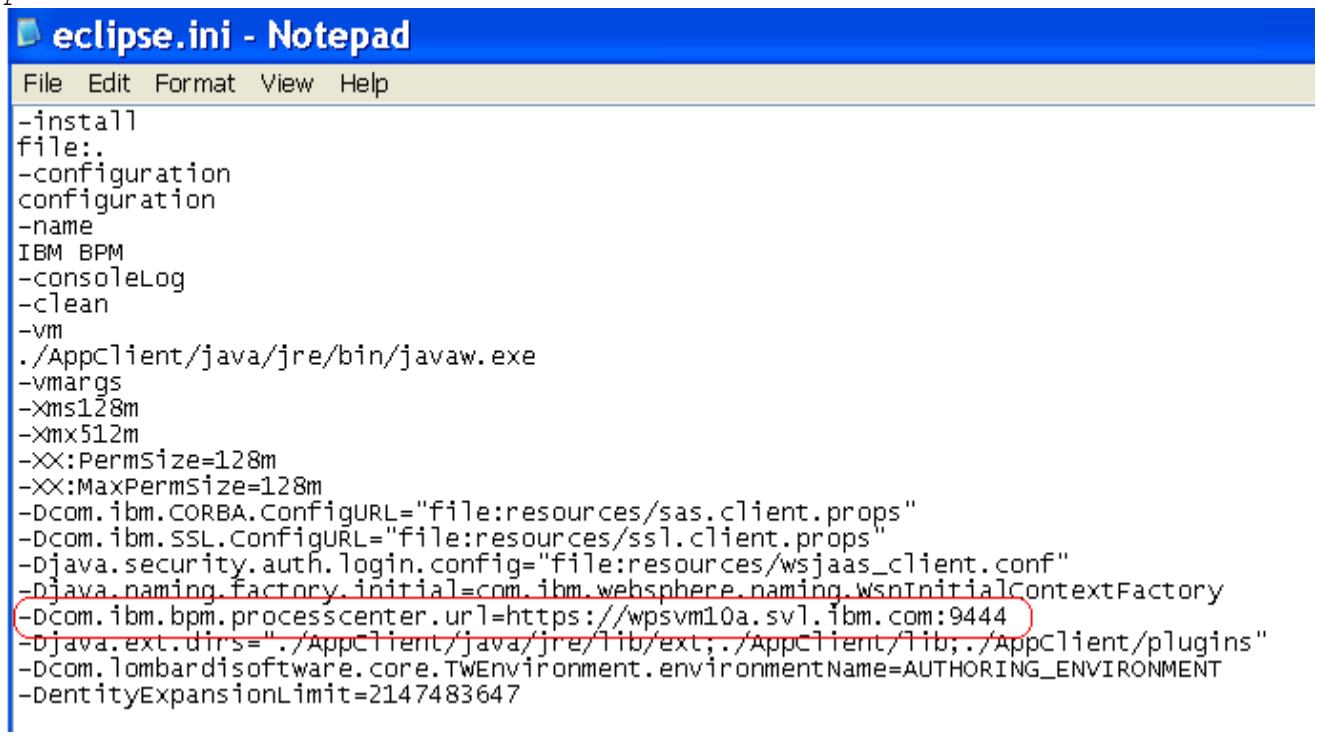
Importing an SSL security certificate into Integration Designer

In order to connect to an HTTPS enabled server, you need to import the SSL security certificate (X509Certificate) for the server. The steps described in this procedure are performed using Internet Explorer.

1. Launch your web browser and enter https://hostname:secure_port/ProcessCenter/login.jsp where hostname is the fully-qualified domain name of the process center server, and secure_port is the process center secure SSL port number.
2. On the Security Alert window, click View Certificate.
3. On the Certificate window, click the Details tab.
4. Click Copy to File to specify where to save the certificate file on your system.
5. In the wizard, click Next, accept the default values, and then click Next again.
6. Enter a file name for the security certificate, for example, pc_cert.cer, and click Next.
7. Click Finish. After you have created the SSL certificate, you can import it into the Java JRE that you will be using for Integration Designer.
8. Copy the certificate to IIDInstall\jdk\jre\bin where IIDInstall is the directory where you installed Integration Designer.
9. Switch to the same location in the command line and run the keytool command line as follows:
   a. keytool.exe -import -v -file <certificate file> -keystore ..\lib\security\cacerts
   If you previously imported SSL certificates into the Integration Designer, add the -alias <key name> parameter to specify a different key name to avoid name conflicts. The default value is mykey.
   b. Enter the keystore password: changeit (this is usually the default password).
   c. Enter y at the prompt to trust the certificate.

Configure Process Designer to access Process Center using SSL

1. Navigate to the Process Designer installation location. For example: `C:\W751\IBMProcessDesigner751`.
2. Edit the eclipse.ini file
3. Locate *`-Dcom.ibm.bpm.processcenter.url`* and change `http://PC_hostname:`*`non_secured_port`* to `https://`*`PC_hostname`*`:`*`secured-port`*.



4. Save and close the eclipse.ini file.
5. Launch the Process Designer and verify access to the Process Center using SSL.
6. Optional: If you have created and configured your own trust store, you must modify one of the following configuration files to point to the correct location for your trust store:
   - Standalone configuration: `NodeDefaultTrustStore`
   - Network deployment configuration: `CellDefaultTrustStore`

   Note: When the Process Designer is downloaded, by default a `trust.p12` file will be included with the zip file. The `trust.p12` file that is included reflects what is specified for the `NodeDefaultTrustStore` (stand-alone server) or `CellDefaultTrustStore` (network deployment environment) found in the Administrator console under **Global Security > SSL certificate and key management > Key stores and certificates**. The `trust.p12` file from that server location is copied and the password is set to `WebAS` before it is included in the zip file. If you have configured a custom trust store with a different password or have multiple trust stores, you must manually copy the `trust.p12` file from the server to your Process Designer install directory and update the `-Djavax.net.ssl.trustStoreType`, `-Djavax.net.ssl.trustStore`, and `-Djavax.net.ssl.trustStorePassword` properties in the `eclipse.ini` file.

7. Verify your configuration.
   a. Log in to the Process Designer.
   b. Right click the Process Apps tab and select Properties.
   c. Confirm that the Address: (URL) section contains the `https://PC hostname:secured port secure` address.