

## APAR: IV61142

### Symptom:

The IBM Security Identity Manager, Version 6.0 infocenter steps to configure Single Sign-On with IBM Security Access Manager WebSEAL work for IBM WebSphere Application Server Version 7. However, the IBM WebSphere Application Server Version 8 requires some changes in the documented steps.

### Documentation Changes:

Following documentation changes to be incorporated to IBM Security Identity Manager, Version 6.0 infocenter under the following two sections:

**Section I :** IBM Security Identity Manager 6.0.0>IBM Security Identity Manager>Security>Configuring single sign-on>Configuring IBM Security Identity Manager for single sign-on with WebSphere Trust Association Interceptor and IBM Security Access Manager WebSEAL>Configuring WebSphere Application Server to point to IBM Security Access Manager

### LOCATION\_URL:

[http://www-01.ibm.com/support/knowledgecenter/api/content/SSRMWJ\\_6.0.0/com.ibm.isim.doc\\_6.0/securing/tsk/tsk\\_ic\\_security\\_sing\\_tai\\_ws2tam.htm?locale=en](http://www-01.ibm.com/support/knowledgecenter/api/content/SSRMWJ_6.0.0/com.ibm.isim.doc_6.0/securing/tsk/tsk_ic_security_sing_tai_ws2tam.htm?locale=en)

### <Infocenter update in blue pen>

3. Add PD.jar to the class path. Type one of the following commands on one line.

Note: If IBM WebSphere Application Server Version is 8 (WebSphere that hosts IBM Security Identity Manager) then copy the PD.jar from %WAS\_HOME%/tivoli/tam to %WAS\_HOME%/java/jre/lib/ext directory.

- Microsoft Windows operating systems:  
set CLASSPATH=%WAS\_HOME%/java/jre/lib/ext/PD.jar;%WAS\_CLASSPATH%
- UNIX and Linux operating systems:  
CLASSPATH=\${WAS\_HOME}/java/jre/lib/ext/PD.jar:\${WAS\_CLASSPATH}

4. Run the com.tivoli.pd.jcfg.PDJrteCfg utility to configure the Java™ Runtime Environment component. Type one of the following commands on one line.

### For IBM WebSphere Application Server, Version 7:

- Microsoft Windows operating systems:  
  
java -cp "%CLASSPATH%" -Djava.ext.dirs  
-Dpd.home="%WAS\_HOME%\java\jre\PolicyDirector"  
com.tivoli.pd.jcfg.PDJrteCfg -action config -was

```
-java_home "%JAVA_HOME%/jre"  
-cfgfiles_path "%JAVA_HOME%/jre"  
-host "tam policy server host name"
```

- UNIX and Linux operating systems:

```
java -cp ${CLASSPATH} -Djava.ext.dirs  
-Dpd.home=${WAS_HOME}/java/jre/PolicyDirector  
com.tivoli.pd.jcfg.PDJrteCfg -action config -was  
-java_home ${JAVA_HOME}/jre  
-cfgfiles_path ${JAVA_HOME}/jre  
-host "tam policy server host name"
```

For IBM WebSphere Application Server, Version 8:

The WebSphere Application Server, version 8 does not permit modification of any files under the WebSphere Application Server JRE directory. So it hosts the IBM Security Access Manager specific files under <WAS\_HOME>/tivoli/tam directory. In previous versions, these files were hosted under the <WAS\_HOME>/java/jre hierarchy.

- Microsoft Windows operating systems:

```
java -cp "%CLASSPATH%" -Djava.ext.dirs  
-Dpd.home="%WAS_HOME%\tivoli\tam\PolicyDirector"  
com.tivoli.pd.jcfg.PDJrteCfg -action config -was  
-java_home "%JAVA_HOME%/jre"  
-alt_config -cfgfiles_path "%WAS_HOME%/tivoli/tam"  
-host "tam policy server host name"
```

- UNIX and Linux operating systems:

```
java -cp ${CLASSPATH} -Djava.ext.dirs  
-Dpd.home=${WAS_HOME}/tivoli/tam/PolicyDirector  
com.tivoli.pd.jcfg.PDJrteCfg -action config -was  
-java_home ${JAVA_HOME}/jre  
-alt_config -cfgfiles_path ${WAS_HOME}/tivoli/tam  
-host "tam policy server host name"
```

The software generates the following message:

Configuration of Access Manager Runtime for Java completed successfully.

**Note:** If this command fails with `NullPointerException` or `InvocationTargetException`, then use the `java` command that is not included in the WebSphere Application Server. For example, if you installed Java on your Tivoli® Directory Integrator directory, then use the `/opt/IBM/TDI/V7.1/jvm/jre/bin/java` command

instead of the java command as follows:

For IBM WebSphere Application Server, Version 7:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java -cp ${CLASSPATH} -Djava.ext.dirs
-Dpd.home=${WAS_HOME}/java/jre/PolicyDirector
com.tivoli.pd.jcfg.PDJrteCfg -action config -was
-java_home ${JAVA_HOME}/jre
-cfgfiles_path ${JAVA_HOME}/jre
-host "tam policy server host name"
```

For IBM WebSphere Application Server, Version 8:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java -cp ${CLASSPATH} -Djava.ext.dirs
-Dpd.home=${WAS_HOME}/tivoli/tam/PolicyDirector
com.tivoli.pd.jcfg.PDJrteCfg -action config -was
-java_home ${JAVA_HOME}/jre
-alt_config -cfgfiles_path ${WAS_HOME}/tivoli/tam
-host "tam policy server host name"
```

5. Run the SSL configuration. Type one of the following commands on one line.

For IBM WebSphere Application Server, Version 7:

- Microsoft Windows operating systems:  
java -cp "%CLASSPATH%"  
-Dpd.cfg.home="%WAS\_HOME%\java\jre"  
-Xnoargsconversion com.tivoli.pd.jcfg.SvrSslCfg -action config  
-admin\_id sec\_master -admin\_pwd \*\*\*\*\* -appsvr\_id sso  
-polycysvr tam:7135:1 -port 7135 -authzsvr tam:7136:1 -mode remote  
-cfg\_file "%WAS\_HOME%\java\jre\PdPerm.properties"  
-key\_file "%WAS\_HOME%\java\jre\lib\security\PdPerm.ks"  
-cfg\_action replace
- UNIX and Linux operating systems:  
java -cp \${CLASSPATH}  
-Dpd.cfg.home=\${WAS\_HOME}/java/jre  
-Xnoargsconversion com.tivoli.pd.jcfg.SvrSslCfg -action config  
-admin\_id sec\_master -admin\_pwd \*\*\*\*\* -appsvr\_id sso  
-polycysvr tam:7135:1 -port 7135 -authzsvr tam:7136:1 -mode remote  
-cfg\_file \${WAS\_HOME}/java/jre/PdPerm.properties  
-key\_file \${WAS\_HOME}/java/jre/lib/security/PdPerm.ks  
-cfg\_action replace

For IBM WebSphere Application Server, Version 8:

- Microsoft Windows operating systems:  
java -cp "%CLASSPATH%"

```
-Dpd.cfg.home="%WAS_HOME%\tivoli\tam"
-Xnoargsconversion com.tivoli.pd.jcfg.SvrSslCfg -action config
-admin_id sec_master -admin_pwd ***** -appsvr_id sso
-policysvr tam:7135:1 -port 7135 -authzsvr tam:7136:1 -mode remote
-cfg_file "%WAS_HOME%\tivoli\tam\PdPerm.properties"
-key_file "%WAS_HOME%\tivoli\tam\PdPerm.ks"
-cfg_action replace
```

- UNIX and Linux operating systems:  

```
java -cp ${CLASSPATH}
-Dpd.cfg.home=$WAS_HOME/tivoli/tam
-Xnoargsconversion com.tivoli.pd.jcfg.SvrSslCfg -action config
-admin_id sec_master -admin_pwd ***** -appsvr_id sso
-policysvr tam:7135:1 -port 7135 -authzsvr tam:7136:1 -mode remote
-cfg_file $WAS_HOME/tivoli/tam/PdPerm.properties
-key_file $WAS_HOME/tivoli/tam/PdPerm.ks
-cfg_action replace
```

</Infocenter update in blue pen>

**Section II:** IBM Security Identity Manager 6.0.0>IBM Security Identity Manager>Security>Configuring single sign-on>Configuring IBM Security Identity Manager for single sign-on with WebSphere Trust Association Interceptor and IBM Security Access Manager WebSEAL>Configuring the Trust Association Interceptor

**LOCATION\_URL:**

[http://www-01.ibm.com/support/knowledgecenter/SSRMWJ\\_6.0.0/com.ibm.isim.doc\\_6.0/securing/tsk/tsk\\_ic\\_security\\_sing\\_tai\\_config.htm](http://www-01.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0/com.ibm.isim.doc_6.0/securing/tsk/tsk_ic_security_sing_tai_config.htm)

<Infocenter update in blue pen>

4. Click Interceptors.

- Click com.ibm.ws.securityweb.TAMTrustAssociationInterceptorPlus.
- Add the following custom properties and click New to add each property.
  - Name: com.ibm.websphere.security.webeal.id Value: iv-creds
  - Name: com.ibm.websphere.security.webseal.checkViaHeader Value: false
  - Name: com.ibm.websphere.security.webseal.loginId Value: sso  
 Note: sso is the IBM Security Access Manager user name that was created in the first task of this procedure
  - For IBM WebSphere Application Server, Version 8:  
 Name: com.ibm.websphere.security.webseal.configURL  
 Value:<WAS\_HOME>/tivoli/tam/PdPerm.properties  
 Where WAS\_HOME is the IBM WebSphere Application Server home directory.

</Infocenter update in blue pen>