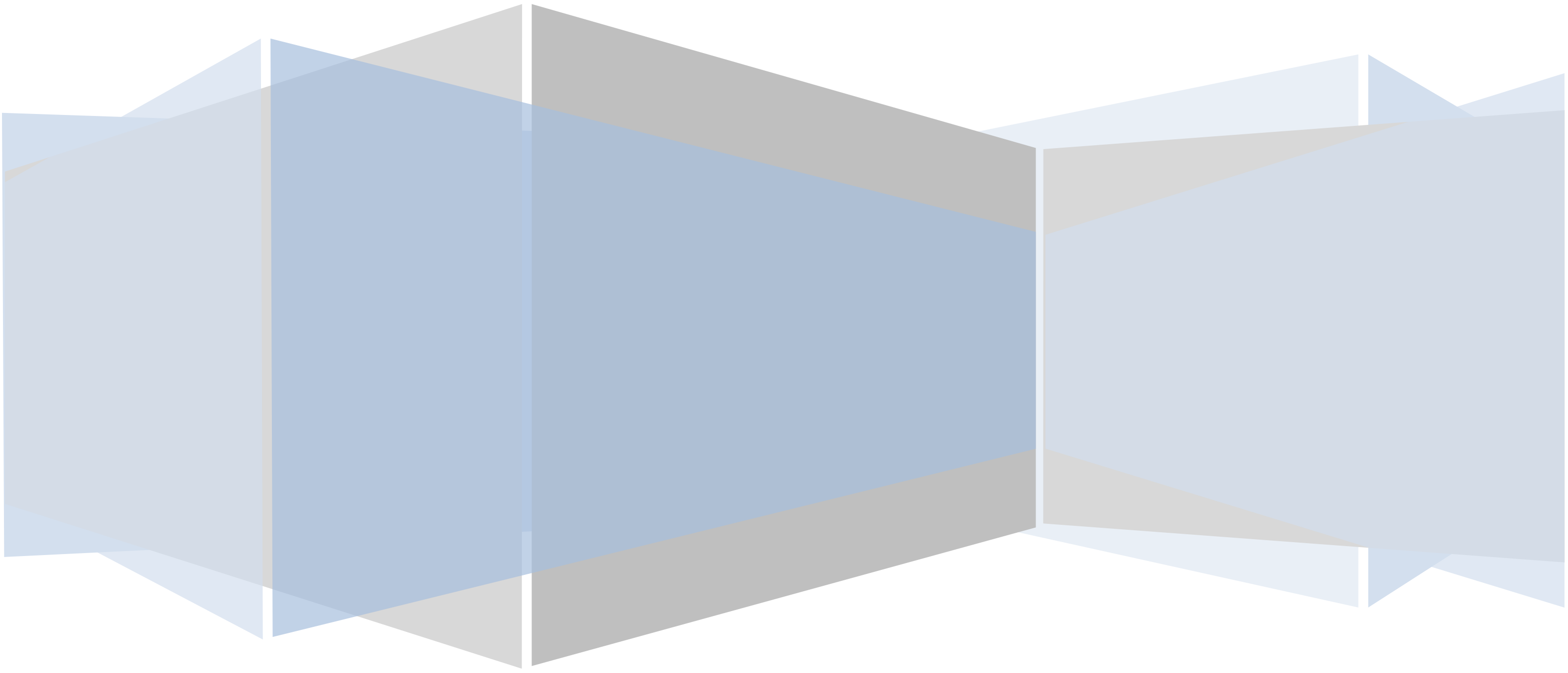
SSO Plugin

Integrating with BMC Atrium Orchestrator

J System Solutions

http://www.javasystemsolutions.com

Version 3.6



Introduction

This document covers the integration of SSO Plugin with BMC Atrium Orchestrator.

The JSS support website contains all the SSO Plugin documentation and videos covering installation and configuration.

Pre-requisite deployment choice

The integration makes use of the SSO Plugin Identity Federation Service, which allows a single SSO Plugin instance to be configured for user authentication, and for third party applications to authenticate against it.

If an existing SSO Plugin instance is deployed within your environment, ie SSO Plugin for BMC ITSM, this can be re-used.

If there is no existing SSO Plugin instance, download the SSO Plugin Authentication Service from the JSS website. To install it, follow these steps:

1. Unpack the zip file downloaded from the JSS website.
2. Locate the authentication-service.war file.
3. Copy the authentication-service.war file into the BMC AO Repository Tomcat instance webapps directory, typically located at C:\Program Files\BMC Software\BAO\REPO\tomcat\webaps\baorepo.
4. Restart the BMC AO Repository Tomcat.
5. Navigate to the SSO Plugin instance by taking the existing BMC AO Repository URL, removing barepo and replacing it with authentication-service, ie. https://host:28080/authentication-service.
6. Login with jss on the left hand side navigation and configure it to integrate with your SSO system. The configuration document contains detailed instructions on the various SSO integration options.

Enabling the Identity Federation Service

You must enable the Identity Federation Service within the SSO Plugin instance identified above, ie either an existing one within BMC ITSM or the Authentication Service. To do so, follow these instructions:

1. Navigate to the SSO Plugin status page, with the configuration link on the left, and login.
2. Click configuration.
3. Tick 'Enable Identity Federation Service'.
4. Enter a unique key or press the button to create one. Take a note of the key.
5. Press 'Set configuration' and ensure the SSO Plugin still functions using the 'Test SSO' link.

Overview of installation process

BMC Atrium Orchestrator comprises of three applications, AO Repository, AO CDP and AO OCP. Each require patching for a fully working system as they talk to each other, and the installation process must be carried out in the order specified below.

When testing SSO on each application, success should be measured by logging into the application, not using it before all three have been patched.

This installation document looks like it involves a lot of effort, but patching each application involves similar steps, so after completing AO Repository, CDP and OCP should feel easier and similar to the work already carried out.

The installation refers to the jss-asso.jar in the asso directory within the installation files.

Hostnames

SSO Plugin uses cookies to send data between the different applications, so all three must be running within a common hostname.

Patching the BMC agent jar file

When configuring each application, you must patch the agent file typically called agent-version.jar (ie agent-7.7.00.00.jar) that is located in the application's WEB-INF/lib directory.

When installing the patched jar file, move the existing jar out of the WEB-INF/lib directory and into a directory outside of the Tomcat directory (ie a backup directory). If the original jar file remains in the WEB-INF/lib directory, Tomcat may ignore the patched jar file.

To obtain a patched jar file, use the agent patching tool on the JSS support website.

The agent jar files within the different applications are typically the same file so you should only need to patch one file and re-use it.

Enabling SSO for AO Repository

To enable SSO Plugin for AO Repository, follow these instructions:

1. Stop the Tomcat instance running the AO Repository.
2. Locate the AO Repository web application, typically located at C:\Program Files\BMC Software\BAO\REPO\tomcat\webapps\baorepo.
3. Patch the agent jar file in the WEB-INF/lib directory as previously discussed.
4. The web.xml file (in the WEB-INF directory) requires patching. We provide a web.xml patching tool on the JSS support website and recommend you use it. Alternatively, you can do this manually by following these steps:
    a. Create a backup of the web.xml file.

    b. Open the web.xml, locate the AtriumSSO filter and delete it:

```
<filter>
  <filter-name>Agent</filter-name>
  <filter-class>com.bmc.atrium.sso.agents.web.jee.JEEFilter</filter-class>
  ...
</filter>
<filter-mapping>
  <filter-name>Agent</filter-name>
  ...
  <dispatcher>ERROR</dispatcher>
</filter-mapping>
```

    c. Paste the following in the location of the now deleted AtriumSSO filter:

```
<filter>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <filter-
class>com.javasystemsolutions.sso.identityfederation.IdentityFederationAcce
ptor</filter-class>
  <init-param>
    <param-name>identityFederationServiceURL</param-name>
    <param-value>HOSTNAME/jss-sso/identityfederationservice</param-value>
  </init-param>
  <init-param>
    <param-name>key</param-name>
    <param-value>KEY</param-value>
  </init-param>
  <init-param>
    <param-name>loglevel</param-name>
    <!-- Set to TRACE for debugging when submitting logs to JSS -->
    <param-value>INFO</param-value>
  </init-param>
  <init-param>
      <param-name>principalSessionKey</param-name><param-
value>com.bmc.ao.sso.principal</param-value>
  </init-param>
  <init-param>
      <param-name>usernameSessionKey</param-name><param-
value>com.bmc.ao.sso.userid</param-value>
    </init-param>
</filter>
<filter-mapping>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <url-pattern>/messagebroker/*</url-pattern>
  <url-pattern>/repo-ui/*</url-pattern>
</filter-mapping>
```

d. Referring to the text above, pasted into the web.xml file, set the following variables:

i. **HOST:** This points to the identity federation service running on the SSO Plugin installation.

The word HOST must be replaced with the URL to the SSO Plugin instance, ie http://midtier/arsys if it is running on BMC ITSM, or https://host:28080/baorepo if you have installed the SSO Plugin authentication service within the AO Repository Tomcat.

After entering the URL, check it works by pasting it into a web browser. You should see an SSO Plugin web page mentioning the Identity Federation Service.

ii. **KEY:** This must be set to the federated identity key noted when enabling the Identity Federation Service.

e. Save the file.

5. Locate the applicationContext.xml file located in the WEB-INF/classes/META-INF, which requires patching:

a. Create a backup of the applicationContext.xml file.

b. Open the applicationContext.xml and locate and delete the following:

```
<security:filter-chain pattern="/**"
  filters="httpSessionContextIntegrationFilter,
    atssoStaleTokenFilter,
    preAuthenticatedHttpSessionFilter,
    logoutFilter,
    atssoPreAuthFilter,
    wsseProcessingFilter,
    basicProcessingFilter,
    securityContextHolderAwareRequestFilter,
    enforcedAuthenticationFilter,
    exceptionTranslationFilter"/>
```

c. Place the following in the location of the text removed above:

```
<security:filter-chain pattern="/*" filters="none" />
<security:filter-chain pattern="/**"
  filters="httpSessionContextIntegrationFilter,
    preAuthenticatedHttpSessionFilter,
    logoutFilter,
    jss.j2eefilter,
    wsseProcessingFilter,
    basicProcessingFilter,
    securityContextHolderAwareRequestFilter,
    enforcedAuthenticationFilter,
    exceptionTranslationFilter"/>
```

d. Locate the following immediately after the text pasted above:

```
  </security:filter-chain-map>
</bean>
```

e. Paste the following immediately below </bean>:

```
<bean id="jss.j2eefilter"
class="com.javasystemsolutions.integrations.spring.security.ASSOPreAuthFilt
er" />
```

f. Enter the Identity Federation Service key in place of the word KEY.

g. Save the file.

6. Copy the jss-sso-asso.jar file, from the asso directory within the SSO Plugin for BMC AR System download, into the WEB-INF/lib directory, ie typically C:\Program Files\BMC Software\BAO\REPO\tomcat\webapps\baorepo\WEB-INF\lib.

7. Start the AO Repository Tomcat instance, navigate to it and ensure SSO works. If there are any problems that you can not resolve, follow these steps:

   a. Set the log level to TRACE in the filter you pasted into the web.xml file.

   b. Restart the AO Repository Tomcat.

   c. Attempt to AO Repository via a web browser.

   d. Stop the AO Repository Tomcat.

   e. Send the AO Repository Tomcat logs directory, the web.xml and applicationContext.xml files edited, to the JSS support team.

Enabling SSO for AO CDP

To enable SSO Plugin for AO CDP, follow these instructions:

1. Stop the Tomcat instance running the AO CDP (and OCP).
2. Locate the AO CDP web application, typically located at C:\Program Files\BMC Software\BAO\CDP\tomcat\webapps\baocdp.
3. Patch the agent jar file in the WEB-INF/lib directory as previously discussed.
4. The web.xml file (in the WEB-INF directory) requires patching. We provide a web.xml patching tool on the JSS support website and recommend you use it. Alternatively, you can do this manually by following these steps:
    a. Create a backup of the web.xml file.
    b. Open the web.xml, locate the AtriumSSO filter and delete it:

```
<filter>
  <filter-name>Agent</filter-name>
  <filter-class>com.bmc.atrium.sso.agents.web.jee.JEEFilter</filter-class>
  ...
</filter>
<filter-mapping>
  <filter-name>Agent</filter-name>
  ...
  <dispatcher>ERROR</dispatcher>
</filter-mapping>
```

    c. Paste the following in the location of the now deleted AtriumSSO filter:

```
<filter>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <filter-
class>com.javasystemsolutions.sso.identityfederation.IdentityFederationAcce
ptor</filter-class>
  <init-param>
    <param-name>identityFederationServiceURL</param-name>
    <param-value>HOSTNAME/jss-sso/identityfederationservice</param-value>
  </init-param>
  <init-param>
    <param-name>key</param-name>
    <param-value>KEY</param-value>
  </init-param>
  <init-param>
    <param-name>loglevel</param-name>
    <!-- Set to TRACE for debugging when submitting logs to JSS -->
    <param-value>INFO</param-value>
  </init-param>
<init-param>
    <param-name>principalSessionKey</param-name>
    <param-value>com.bmc.ao.sso.principal</param-value>
  </init-param>
  <init-param>
    <param-name>usernameSessionKey</param-name>
    <param-value>com.bmc.ao.sso.userid</param-value>
  </init-param>
  <init-param>
    <param-name>skipURIs</param-name>
    <param-value>/ws/</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

d. Referring to the text above, pasted into the web.xml file, set the following variables:

   i. **HOST:** This points to the identity federation service running on the SSO Plugin installation.

      The word HOST must be replaced with the URL to the SSO Plugin instance, ie http://midtier/arsys if it is running on BMC ITSM, or https://host:28080/baorepo if you have installed the SSO Plugin authentication service within the AO Repository Tomcat.

      After entering the URL, check it works by pasting it into a web browser. You should see an SSO Plugin web page mentioning the Identity Federation Service.

   ii. **KEY:** This must be set to the federated identity key noted when enabling the Identity Federation Service.

e. Save the file.

5. Copy the jss-sso-asso.jar file, from the asso directory within the SSO Plugin for BMC AR System download, into the WEB-INF/lib directory, ie typically C:\Program Files\BMC Software\BAO\CDP\tomcat\webapps\baocdp\WEB-INF\lib.

6. Start the AO CDP/OCP Tomcat instance, navigate to it and ensure SSO works. If there are any problems that you can not resolve, follow these steps:

   a. Set the log level to TRACE in the filter you pasted into the web.xml file.

   b. Restart the AO CDP/OCP Tomcat.

   c. Attempt to AO CDP via a web browser.

   d. Stop the AO CDP/OCP Tomcat.

   e. Send the AO CDP/OCP Tomcat logs directory and the web.xml edited to the JSS support team.

Enabling SSO for AO OCP

To enable SSO Plugin for AO OCP, follow these instructions:

7. Stop the Tomcat instance running the AO OCP (and CDP).
8. Locate the AO OCP web application, typically located at C:\Program Files\BMC Software\BAO\CDP\tomcat\webapps\baoocp.
9. Patch the agent jar file in the WEB-INF/lib directory as previously discussed.
10. The web.xml file (in the WEB-INF directory) requires patching. We provide a web.xml patching tool on the JSS support website and recommend you use it. Alternatively, you can do this manually by following these steps:
    a. Create a backup of the web.xml file.
    b. Open the web.xml, locate the AtriumSSO filter and delete it:

```
<filter>
  <filter-name>Agent</filter-name>
  <filter-class>com.bmc.atrium.sso.agents.web.jee.JEEFilter</filter-class>
  ...
</filter>
<filter-mapping>
  <filter-name>Agent</filter-name>
  ...
  <dispatcher>ERROR</dispatcher>
</filter-mapping>
```

    c. Paste the following in the location of the now deleted AtriumSSO filter:

```
<filter>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <filter-
class>com.javasystemsolutions.sso.identityfederation.IdentityFederationAcce
ptor</filter-class>
  <init-param>
    <param-name>identityFederationServiceURL</param-name>
    <param-value>HOSTNAME/jss-sso/identityfederationservice</param-value>
  </init-param>
  <init-param>
    <param-name>key</param-name>
    <param-value>KEY</param-value>
  </init-param>
  <init-param>
    <param-name>loglevel</param-name>
    <!-- Set to TRACE for debugging when submitting logs to JSS -->
    <param-value>INFO</param-value>
  </init-param>
<init-param>
    <param-name>principalSessionKey</param-name>
    <param-value>com.bmc.ao.sso.principal</param-value>
  </init-param>
  <init-param>
    <param-name>usernameSessionKey</param-name>
    <param-value>com.bmc.ao.sso.userid</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>ssoplugin-identity-federation-acceptor</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

d. Referring to the text above, pasted into the web.xml file, set the following variables:

i. **HOST:** This points to the identity federation service running on the SSO Plugin installation.

The word HOST must be replaced with the URL to the SSO Plugin instance, ie http://midtier/arsys if it is running on BMC ITSM, or https://host:28080/baorepo if you have installed the SSO Plugin authentication service within the AO Repository Tomcat.

After entering the URL, check it works by pasting it into a web browser. You should see an SSO Plugin web page mentioning the Identity Federation Service.

ii. **KEY:** This must be set to the federated identity key noted when enabling the Identity Federation Service.

e. Save the file.

11. Copy the jss-sso-asso.jar file, from the asso directory within the SSO Plugin for BMC AR System download, into the WEB-INF/lib directory, ie typically C:\Program Files\BMC Software\BAO\CDP\tomcat\webapps\baoocp\WEB-INF\lib.

12. Start the AO CDP/OCP Tomcat instance, navigate to it and ensure SSO works. If there are any problems that you can not resolve, follow these steps:

f. Set the log level to TRACE in the filter you pasted into the web.xml file.

g. Restart the AO CDP/OCP Tomcat.

h. Attempt to AO CDP via a web browser.

i. Stop the AO CDP/OCP Tomcat.

j. Send the AO CDP/OCP Tomcat logs directory and the web.xml edited to the JSS support team.