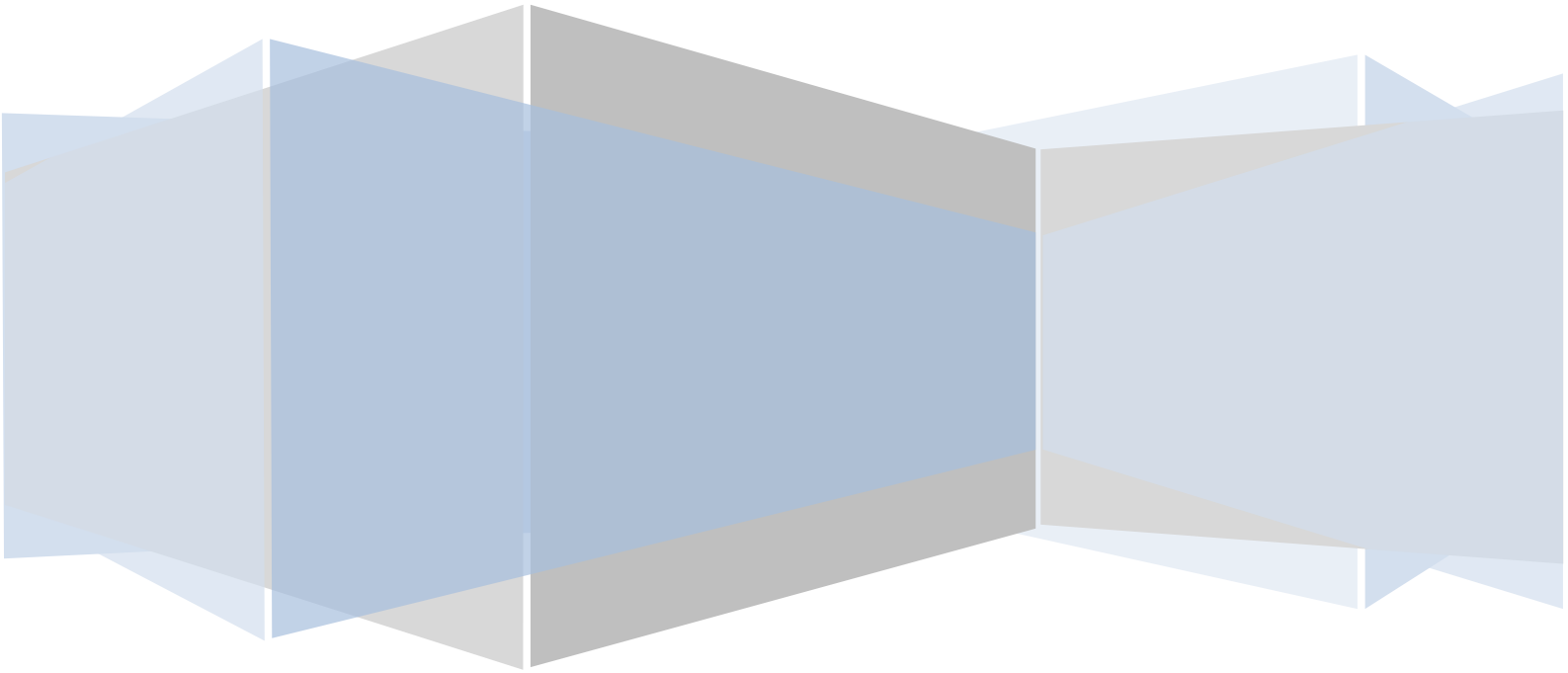
SSO Plugin

Integration for BMC Dashboards

J System Solutions

http://www.javasystemsolutions.com

Version 3.5



Introduction

This document covers installation and configuration of SSO Plugin for BMC Dashboards. Separate documents are available for other BMC components (ie AR System, Dashboards).

The JSS support website can be found here:

http://www.javasystemsolutions.com/jss/support

There's a video available to assist with installing the SSO Plugin and it can be found at http://www.javasystemsolutions.com/jss/video

Dashboards user administration

Dashboards maintains its own user database and role mapping. BMC provide no tool to integrate this with AR System. This means that you are required to maintain two user databases, each with their own role/group mappings.

Dashboards has a basic LDAP authentication interface that is similar to the BMC AREA LDAP plugin, however this still requires you to maintain two lists of roles and is redundant when using SSO Plugin.

SSO Plugin provides this functionality to you through the integration with BMC AR System.

SSO Plugin integration

SSO Plugin runs on the Mid Tier providing corporate SSO, and also extends SSO to Dashboards through the JSS *Identity Federation Service*. This allows third party products, BMC or non-BMC, to be SSO enabled with the Mid Tier (and hence, AR System User form) as a single repository of data.

The integration leaves Dashboards configured to use SSO Plugin or the Dashboards local database, allowing the administrator to maintain additional accounts in Dashboards that are not present in AR System if necessary.

The flow of data is as follows:

1. When a request hits Dashboards and no session exists, it is redirected to the Mid Tier running SSO Plugin.
2. The user passes through the configured SSO implementation and when complete, the request is sent back to Dashboards with the AR System User form detail (such as their groups).
3. The SSO Plugin for Dashboards checks the Dashboards database for an account. One of the following actions is followed:
    1. If an account doesn't exist **and** the AR System user is in a valid group (see *group/role synchronisation* below), an account is created and placed in the matching roles.

2. If an account does exist then it the roles are synchronised with the AR System groups.
3. If the Dashboards user has a valid role then login can proceed.
4. If the Dashboards user no longer has a valid role, the request is sent to the Dashboards login page where a user/administrator can login manually.

Group/role synchronisation

This feature brings the AR System User form and Dashboards user repository together and is extremely powerful for AR System administrators.

Groups are defined in AR System that match Dashboard roles and every time a user logs into Dashboards via SSO Plugin, the Dashboards roles are synchronised with the AR System user groups.

For example, if user Bob in AR System has no Dashboard groups, he has no SSO access to Dashboards.

If he is then placed in ITSM group Release Manager, when he access Dashboards via SSO, his Dashboards account is created (if it doesn't already exist) and he gains access to functionality within that Dashboards role (by default, Change configuration release manager).

If the AR System administrator removes Bob from this group, the next time he accesses Dashboards, SSO Plugin will remove him from that Dashboards role and he will no longer have access.

A user may be added to or removed from multiple Dashboards groups in AR System and they will all be synchronised on the next Dashboards SSO login.

Default ITSM to Dashboards group/role mapping

The product is shipped with a default mapping for BMC ITSM groups to BMC Dashboard roles. The mappings are many to one, allowing you to map many AR System groups to a Dashboards role.

The default mappings are shown below: on the left is a list of groups and on the right is the Dashboards role to which the groups are mapped. The user can be in any BMC ITSM group in order to be mapped to the Dashboards role.

Please note:

1. The user can be in **any** BMC ITSM group in order to be mapped to the Dashboards role.
2. Any AR System administrator user is mapped to the Dashboards Administrator role.
3. The Dashboards value in brackets is used when defining your own mapping.

BMC ITSM	BMC Dashboards
Incident Config Asset Config Change Config Problem Config Release Config SLM Config SRM Administrator	Administrator (BSD_ADMIN_ROLE_NAME)
Release Manager	Change configuration release manager (BSD_CHANGE_CONFIG_RELEASE_MANAGER_NAME)
Business Manager Incident Master Problem Master Asset Master Change Master Release Master	IT Supervisor (BSD_IT_SUPERVISOR_NAME)
Problem Manager	Problem manager (BSD_PROBLEM_MANAGER_NAME)

Incident Master Asset Master Change Master Problem Master Release Master	Service delivery manager (BSD_SERVICE_DELIVERY_MANAGER_NAME)
Incident Master Problem Master	Service desk manager (BSD_SERVICE_DESK_MANAGER_NAME)
SLM Master	Service level manager (BSD_SERVICE_LEVEL_MANAGER_NAME)
Business Manager Work Order Master SRM Administrator	Service request manager (BSD_SERVICE_REQUEST_MANAGER_NAME)
Business Manage Incident Master Problem Master Asset Master Change Master Release Master	Service support manager (BSD_SERVICE_SUPPORT_MANAGER_NAME)

Accessing the admin console

Any AR System administrator and any user mapped to one of the ITSM config groups detailed above can access the Dashboards Admin console.

Automated integration with BMC ITSM

The user accounts in ITSM contain the user's first and last name plus an email address. When a user is created in Dashboards, their ITSM People data is used to populate these fields.

Configuring SSO Plugin

You must first set up SSO Plugin to enable the Identity Federation Service:

1. Login to the Mid Tier SSO Plugin setup page.
2. Tick 'Enable Identity Federation Service'.

3. Enter a unique key or press the button to create one. Take a note of the key.
4. Press 'Set configuration' and ensure the SSO Plugin still functions using the 'Test SSO' link.

Installing SSO Plugin for Dashboards

To enable SSO Plugin for BMC Dashboards, the following steps must be followed to copy the plugin to Dashboards:

1. Login to Dashboards and ensure you know the password for the Administrator account. This will allow you to login manually should you need to troubleshoot the SSO integration once complete.
2. Locate the BMC Dashboards program directory, typically found in C:\BMC Software\BSM Dashboards\tomcat\webapps\bsmdashboards. Go to the WEB-INF\lib directory and remove the log4j-1.2.11.jar file. An updated one is provided by SSO Plugin and copied in the next step.
3. Locate the bsmdashboards directory in the SSO Plugin installation files. Copy the **contents** of this directory into the BMC Dashboards program directory, typically found in C:\BMC Software\BSM Dashboards\tomcat\webapps\bsmdashboards.
4. The Dashboards web.xml file (in the WEB-INF directory) requires patching. We provide a tool on the JSS support website to do this for you (http://www.javasystemsolutions.com/jss/service) and recommend you use it, or you can do this manually by following these steps:
   4.1. Open the web.xml.patch file from bsmdashboards\WEB-INF, select all and copy to clipboard.
   4.2. Open the web.xml file from bsmdashboards\WEB-INF\web.xml.
   4.3. Paste the block of text copied to clipboard below the <description> tag, ie:

```
<description>..</description>
<filter>
…
```

   4.4. Referring to the patch pasted above, perform the following changes:
      a) **identityFederationServiceURL:** This points to the identity federation service running on the SSO Plugin installation. The identity federation service URL is /jss-sso/identityfederationservice, relative to the Mid Tier installation. Therefore, if the Mid Tier is installed at:

```
http://bmcMid Tier:8080/arsys
```

then the **identityFederationServiceURL** is:

```
http://bmcMid Tier:8080/arsys/jss-sso/identityfederationservice
```

b) **key:** This must be set to the federated identity key set in the Mid Tier SSO Plugin interface.

4.5. Locate the following:

```
<welcome-file>ExecutiveDashboards.html</welcome-file>
```

and replace with:

```
<welcome-file>/index.jsp</welcome-file>
```

4.6. Locate the following:

```
<servlet-
class>com.bmc.bsm.dashboards.util.servlet.AdminConsoleServlet</servl
et-class>
```

and replace with the following:

```
<jsp-file>/admin.jsp</jsp-file>
```

5. Open the bsmdashboards/WEB-INF/classes/dashboards.properties, locate the following line:

```
com.bmc.bsm.dashboards.authentication.type=ldap
```

and modify by setting to database (if it not database already):

```
com.bmc.bsm.dashboards.authentication.type=database
```

Do not put sso on this line as the text in the file suggests.

6. Ensure your BMC AR System user is an AR System administrator or in one of the BMC ITSM config groups detailed in the Default ITSM to Dashboards group/role mapping section.
7. Restart the BSM Dashboards Tomcat instance.
8. Open a browser and **delete the browser history**. This is because the previous Dashboards HTML pages are cached and will be used instead of the SSO enabled pages.
9. Navigate to: http://host/bsmdashboards/admin. You should now be logged in as the AR System user to which your SSO user is mapped.
10. Test http://host/bsmdashboards.

Bespoke group mapping

You can implement your own group mapping scheme if the out of the box implementation does not meet your requirements, although we would appreciate hearing about this if it is the case (with the view to learning why and discussing whether the out of the box defaults should change).

In the web.xml file, locate the roleMap parameter in the patch added by SSO Plugin and define a roleMap in the syntax:

DashboardsRole=ARSystemGroup1,ARSystemGroup2,..,ARSystemGroupN

For example:

BSD_SERVICE_DESK_MANAGER_NAME=ARSgroup1,ARSgroup2.