SSO Plugin

Integration for BMC MyIT and SmartIT

J System Solutions
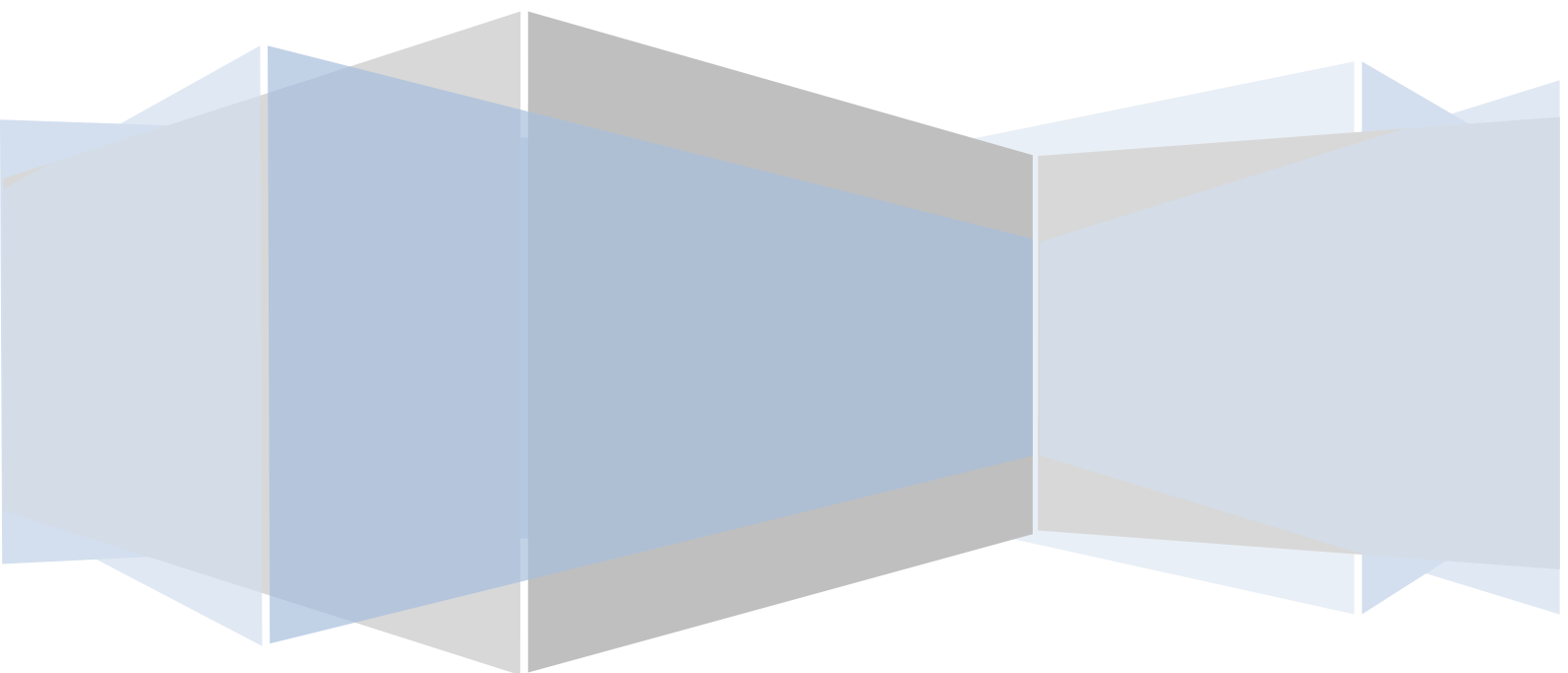
http://www.javasystemsolutions.com

Version 4.0

Introduction

This document covers installation and configuration of SSO Plugin for BMC MyIT 2+. Separate documents are available for other BMC components (ie AR System, Dashboards).

We do not support versions of MyIT prior to version 2.1 because BMC have vastly improved the product since the original release and this has simplified the SSO integration.

JSS has worked closely with BMC MyIT releases, in particular, around the MyIT SSO interface. We therefore recommend you use version 2.2 of MyIT, or a suitably patched version of 2.1 (please contact JSS support for the most up to date advice).

As of MyIT version 2.1, the SmartIT product is encapsulated within MyIT so by following this document, SSO will be enabled for both MyIT and SmartIT.

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

Deployment approaches

This installation method in this document assumes an existing SSO Plugin enabled BMC Mid Tier is available, and re-uses its SSO integration. If the users of MyIT do not have access to Mid Tier (ie it is behind a firewall for external users) then you will need to integrate MyIT directly with the SSO implementation and these instructions can be found in the 'SSO Plugin Authentication Service' download.
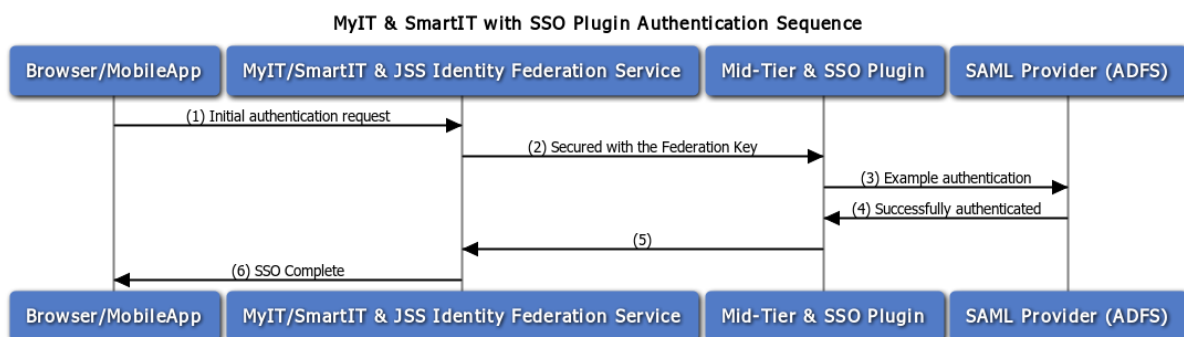
If in any doubt, discuss your implementation options with JSS support.

SSO Plugin integration

SSO Plugin runs on the Mid Tier providing SSO for the existing BMC applications, and also extends SSO to MyIT 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 flow of data is as follows:

1. When a request hits the SSO Plugin URL (http://myit.ssoplugin.local:9000/ux/myitapp/) on MyIT 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 MyIT with the AR System User form detail (such as their groups).

3. The SSO Plugin passes the username into MyIT which progresses through the existing MyIT login process.

MyIT & SmartIT with SSO Plugin Authentication Sequence

Browser/MobileApp	MyIT/SmartIT & JSS Identity Federation Service	Mid-Tier & SSO Plugin	SAML Provider (ADFS)
	(1) Initial authentication request →		
		(2) Secured with the Federation Key →	
			(3) Example authentication →
			(4) Successfully authenticated ←
	(5) ←		
(6) SSO Complete ←			

Configuring SSO Plugin

You must first set up SSO Plugin to enable the Identity Federation Service, typically running on BMC Mid Tier:

1. Login to the Mid Tier SSO Plugin configuration page, ie. http://yourmidtier/arsys/jss-sso/index.jsp.

2. Click Configuration.

3. Tick 'Enable Identity Federation Service'.

4. Enter a unique key or press the Random button to create one. Take a note of the key for the next section.

5. Click 'Set configuration' and ensure the SSO Plugin still functions using the 'Test SSO' link.

Patch the MyIT web.xml

The MyIT ux web.xml file (default location is C:\Program Files\BMC Software\Smart_IT_MyIT\Smart_IT_MyIT\ux\WEB-INF) requires patching. We provide a tool on the JSS support website to do this for you and recommend you use it, or you can do this manually.

1. Browse to the following page http://www.javasystemsolutions.com/jss/service

2. Select BMC MyIT from the Product menu

3. Enter your full URL of the Mid Tier default web path as it is configured in the AR System Administration Console. Example http://midtier.yournetwork.com/arsys

4. Enter the Federation Key copied in the previous task, to the Federation Key box

5. Click the Choose File button and browse to the MyIT ux web.xml on your installation. Note that your existing web.xml file will not be modified.

6. Click Get patched file and save the new patched-web.xml to the same directory for use in the next section.
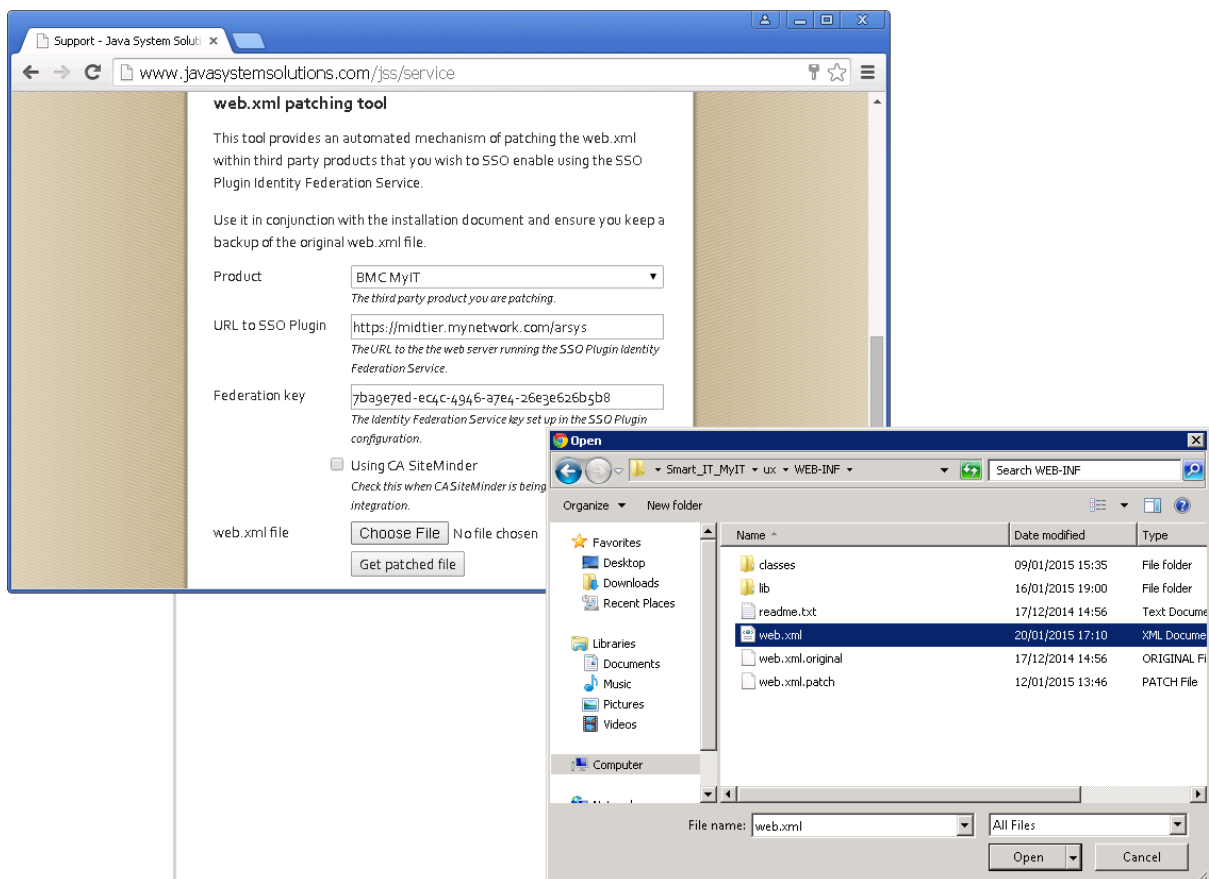
Installing SSO Plugin for BMC MyIT 2.2

To enable SSO Plugin for BMC MyIT, the following steps must be followed:

1. Stop the instance of Tomcat running MyIT. The display name is **Smart IT/MyIT Application**

2. Backup the original web.xml file and rename the patched-web.xml that was configured via the JSS website and saved in the previous section to web.xml. The default directory is C:\Program Files\BMC Software\Smart_IT_MyIT\Smart_IT_MyIT\ux\WEB-INF

3. Copy the WEB-INF directory and contents from the SSO Plugin download MyIT folder and paste into the MyIT installation ux directory. Example screenshot:
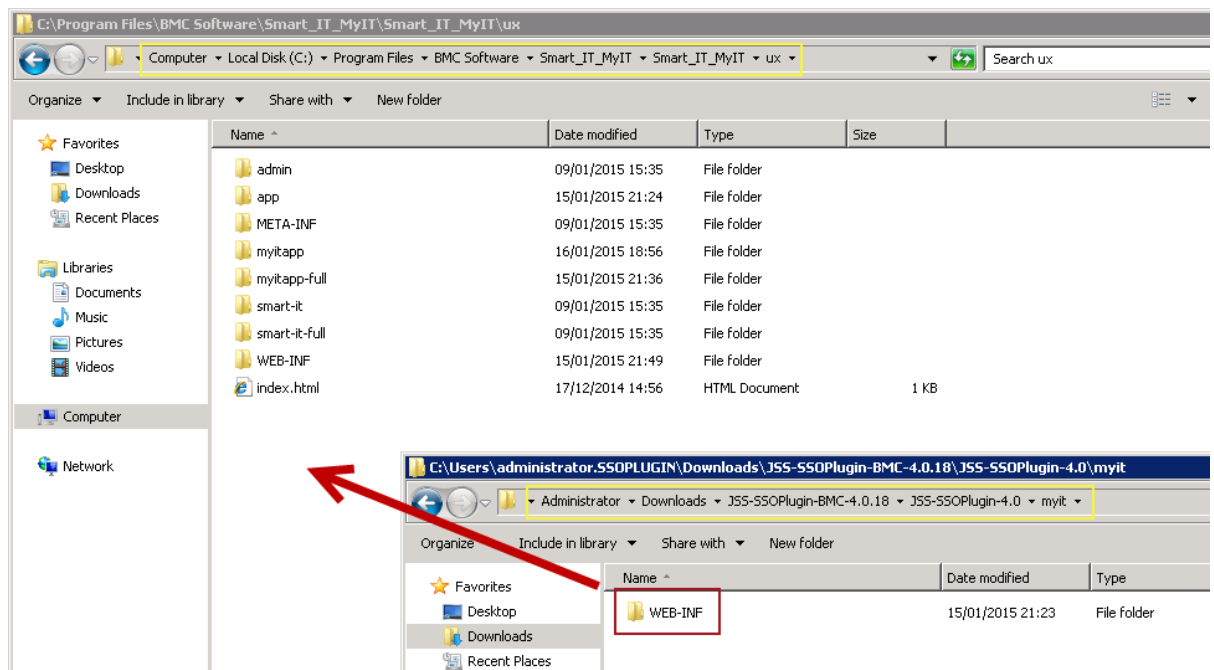

4. Locate the index.html file under the ux web application directory.

5. Rename the index.html file to index.jsp.

6. Open the index.jsp file in your favourite text editor and add the following to the top of the file:

```
<% response.setHeader("Cache-Control", "no-cache"); %>
```

7. A setting in the MyIT database switches on SSO. Locate the TENANT table and set SAML_AUTHENTICATION=1 where PK=1. Example SQL:

```
update [SmartIT]. [SmartIT_System].TENANT set SAML_AUTHENTICATION = 1 where PK = 1
```

8. Example screenshot:
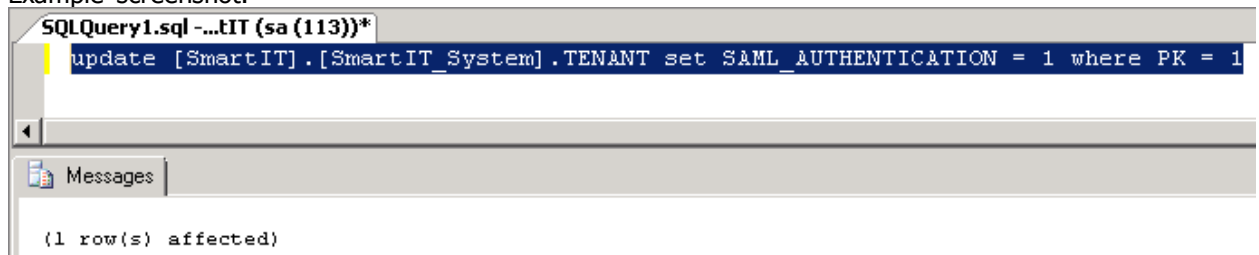
9. Start the instance of Tomcat running MyIT. The display name is **Smart IT/MyIT Application**

10. Verify the installation by browsing to http://myit.yourdomain.com:9000/ux/

Installing SSO Plugin for BMC MyIT 2.0 & 2.1

To enable SSO Plugin for BMC MyIT, the following steps must be followed:

1. Stop the Tomcat instance running MyIT.

2. The MyIT application is deployed as a war file and requires unpacking so it can be configured for use with SSO Plugin. Prior to MyIT2.1 it is called myit.war, and since MyIT2.1 it is called ux.war. The following instructions assume it is called myit.war but if using MyIT2.1, the same steps are followed but use ux.war where you read myit.war.

    a. Locate the war file in the MyIT installation directory, ie c:\Program Files\BMC Software\MyIT\MyIT\myit.war or **ux.war.**

    b. Take a backup of the war file so it can be re-introduced if the SSO integration fails.

    c. Rename the war file to myit.war.zip.

    d. Extract myit.war.zip to a directory called myit.war.

    e. Delete the myit.war.zip file.

Screenshot Example
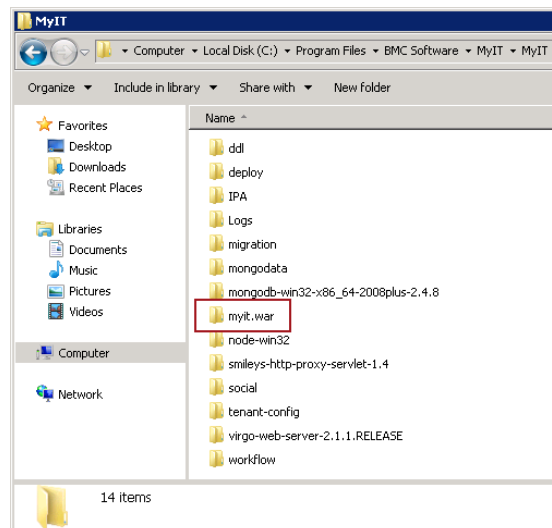
3. Locate the SSO Plugin MyIT installation files and copy them into the MyIT web application directory unpacked in the previous step. Copying will ask you to confirm the folder replace because WEB-INF already exists. Please select **Yes**.

   Copying the files
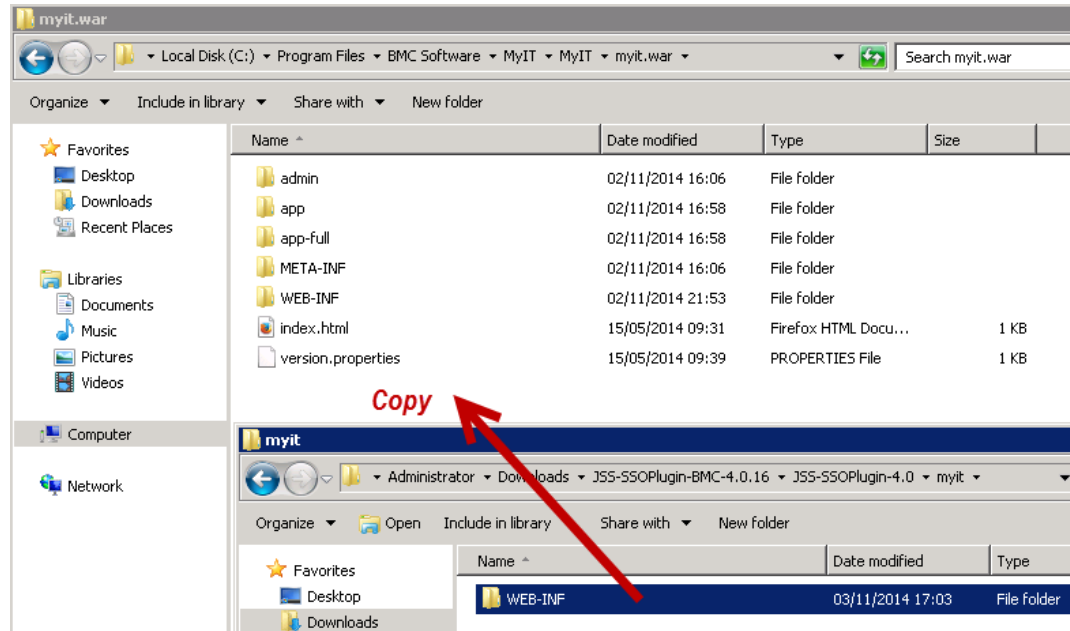
   a. Move the new jar to C:\Program Files\BMC Software\MyIT\MyIT\myit.war\WEB-INF\lib Overwriting the old file if it still exists.

4. Various index.html files require a small change in order to ensure the browser does not cache them:

   a. In MyIT 2.0.x, locate the index.html files under the app and app-full directories.

   b. In MyIT 2.1.x, locate the index.html files under the myit-app and smartit directories.

   Two changes must be made to each index.html file:

   a. Rename it to index.jsp.

   b. Open it in your favourite text editor and add the following to the top of the file:

```
<% response.setHeader("Cache-Control", "no-cache"); %>
```

5. A setting in the MyIT database switches on SSO. Locate the TENANT table and set SAML_AUTHENTICATION=1 where PK=1 as per the following screenshot:

```
SQLQuery1.sql ...ter (sa (105))*
    /****** Script for SelectTopNRows command from SSMS  ******/
  SELECT TOP 1000 [PK]
        ,[HOSTNAME]
        ,[ID]
        ,[NAME]
        ,[SAML_AUTHENTICATION]
    FROM [myit].[myitsystem].[TENANT]
    UPDATE [myit].[myitsystem].[TENANT] set SAML_AUTHENTICATION = 1 WHERE PK = 1
```

	PK	HOSTNAME	ID	NAME	SAML_AUTHENTICATION
1	1	localhost	6a50b5bc-e8ad-4af2-808c-3b8b5a9c3934	000000000000001	1

6. The MyIT web.xml file (in the C:\Program Files\BMC Software\MyIT\MyIT\myit.war\WEB-INFdirectory) 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:

    a. Open the web.xml.patch file from myit\WEB-INF, select all and copy to clipboard.

    b. Open the myit\WEB-INF\web.xml file.

    c. Locate the first filter-mapping element and paste the patch before it, ie.

```
<!-- paste patch here -->
<filter-mapping>
   ...
```

    d. Referring to the patch pasted above, perform the following changes:

        i. **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://bmcMidTier:8080/arsys
```

        then the **identityFederationServiceURL** is:

http://www.javasystemsolutions.com

`http://bmcMidTier:8080/arsys/jss-sso/identityfederationservice`

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

7. Start the MyIT Tomcat instance.

8. The URL entry points differ per MyIT version:

    a. Prior to version 2.1, navigate to: http://host/myit.

    b. From version 2.1 or above, navigate to:

        i. http://host/ux/myit-app (for MyIT).

        ii. http://host/ux/smartit (for SmartIT).

9. If there is an issue you can not resolve in the SSO implementation, follow these steps:

    a. Stop the MyIT Tomcat instance.

    b. Move the myit war file from the webapps directory into a location outside of Tomcat so it can be kept for debugging purposes.

    c. Place the myit.war file backed up in step 2(b) in the webapps directory.

    d. Start the MyIT Tomcat instance.