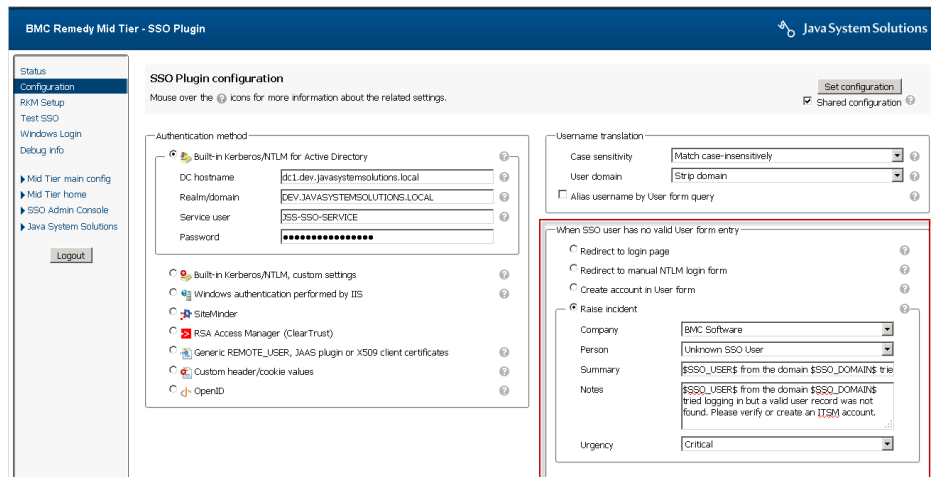


User Onboarding Just Got Easier

SSO Plugin now integrates with BMC Remedy Incident Management.

Best Practice Guide

BusinessDictionary.com states the meaning of Best Practice as “A method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark.” Over the past six years, JSS has provided Single Sign On to some of BMC’s largest enterprise customers. So it’s fair to say we have the expertise and the experience to create a best practice guide to SSO integrations.

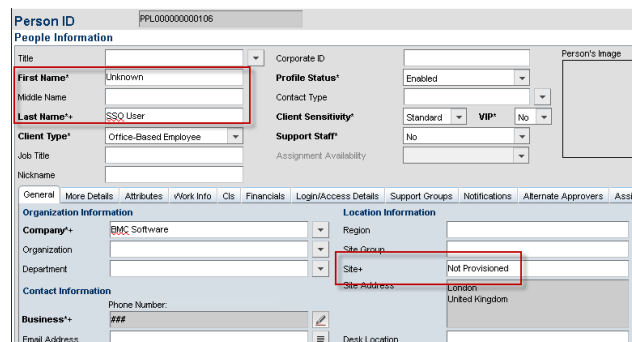


Where did it all start and where did this best practice come from?

Anyone that has performed any form of AR System login name to domain name synchronisation knows it’s no small task. JSS first came across this six years ago and thus created a feature called “User Aliasing”. This was born from one of our outsourcing customers having a system that had many tens of thousands of users, all of whom did not match their login names with domain names. “User Aliasing” allowed our customers to add a field to the User form so each user could have their domain username in the same record as their AR System login name. Therefore, when SSO looked for a user, it authenticated with the domain name but then allowed the AR System to continue using the login name. That handled the accounts that existed in the domain and the AR System. What about the people who had a domain account but not an ITSM account? In any implementation, user gathering is time consuming, active directories become the source of truth and that still leaves room for error for any joiners/leavers process. After consulting our customers, collectively, the answer was “Raise a ticket”.

Step 1: Configuring BMC Remedy ITSM — Dummy People Record

To raise an incident, there must always be a “Customer”. This is a representation of who raised the incident. In this special case, the system doesn’t know those details yet. So a dummy people account is needed with a dummy site name. In our experience, we created a site called “Not Provisioned” that is associated to our customer company. Then an account that has no permissions, just a first name of “Unknown” and surname of “SSO User” was created and the site “Not Provisioned” was associated. Make note of the **Person ID** for Step 2.



Step 2: Configuring BMC Remedy ITSM — Assignment

Best practice dictates that incoming incidents are measured based on resolution time, so a critical path to shorter times starts with automatic assignment. Luckily this is very easy with the BMC Remedy Incident Management application. Login to the system, Click on the Application Configuration Console > Custom Configuration > Foundation > Configure Assignment > Configure Application Assignment.

Here we fill out the **Event*** drop down to **-General-**. On the right you select your service desk group from your operating company (Assignment). Then below (Routing Order) you select your customer company with the Site location of "Not Provisioned". Finally, make sure you select the **User Service Request** check box on the right (Available Systems) and save.

Step 3: Configuring SSO Plugin

The final configuration is completed at the Midtier SSO plugin page found at the following URL <http://YourMidtier/arsys/jss-ssso/setup.jsp>

Login using the same password used to login to the BMC Midtier configuration (standard password is arsystem). Once you are logged in, select **Raise Incident** in the **When SSO user has no valid User form entry**. Place the **Person ID** created in Step 1 into the Person ID field and click Verify Person. Set an urgency and enter the notes and description. You have two variables to use. **\$\$SSO_USER\$** which will replace with the domain username and **\$\$SSO_DOMAIN\$** which will be replaced with the users domain. When you are happy with the text, click **Set Configuration**.

Testing...

In our development lab here at JSS, we created a domain account for **David Easter** with the domain name **deaster**. We made sure that **deaster** did not exist in our User form with that login name. We logged into a Windows desktop as **deaster** and browsed to <http://yourMidtier/arsys/home>. This is the screen **deaster** was presented with:

SSO Plugin

You do not have Single Sign On access to the AR System.

An incident has been raised with ID INC000000000503. Please contact your service desk to monitor the progress of this incident.

Your Single Sign On username is deaster@DEV.JAVASYSTEMSOLUTIONS.LOCAL. You may need to report this to the service desk.

You may be able to login manually by clicking [here](#).

Final words from us...

This feature further demonstrates that SSO Plugin is forever improving and aiding the deployment of SSO. No project is without risk but we believe SSO shouldn't be one of them. We are proud to be globally recognised as the market experts in SSO with the BMC AR System and ITSM. We have the client base and experience to prove it. Our confidence in our product allows us to offer free professional services during the evaluation, with no commitment to buy. We continue to offer 24/7 worldwide support to many of BMC's global customers. Our license model is based on site and not end user count for any number of systems. Please contact our support team at support@javasystemsolutions.com for further information on the JSS SSO Plugin.