

# Planning an SSO Implementation

## Not sure where to start with your SSO initiative?

### Best Practice Guide



Since 2006, JSS has offered free professional services to implement single sign on with the BMC AR system and ITSM. Over that time, we have learnt how to deploy quickly, securely and more importantly, how to identify the risks. This document is the first step in that process.

### 1.1 What "Authentication Method" will be used?

The first step involves looking at your current/to-be architecture and deciding how your users are going to be authenticated.



### Are you using Siteminder or RSA Access Manager (Cleartrust)?

These type of JAAS module technologies are company wide implementations where these products protect a number of other web applications such as intranets etc and are normally part of a corporate standard. A JAAS module is the plugin to Tomcat that authenticates the SM/CT cookie with the SM/CT server.



**Task:**  
**Verify the header technology is protecting your midtier installations.**

### OpenID Are you using OpenID?

Open ID is a free and easy way to use a single digital identity across the internet. This type of authentication method is only used for customers who could not connect the midtier instances to any Active Directory. This functionality is very powerful due to the fact there are multiple OpenID providers on the internet. You probably use one such as Google, Yahoo etc



- Task:**
- **This authentication method relies on every user within your user form, having an account with an OpenID provider.**
  - **Two new fields will need to be added to the User form. See the installation doc for exact steps: [www.javasystemsolutions.com/jss/downloads](http://www.javasystemsolutions.com/jss/downloads)**



## Are you using Microsoft IIS?

Internet Information Service is the Windows standard for HTTP services. If your midtier is installed on windows then you are likely to have this configured. When installing BMC midtier, it will install the Tomcat adaptor to process the javascript. IIS can authenticate Windows users but there are some configuration steps that may require you to organise before installation.



### Task:

- **Verify that midtier is using IIS.**
- **Verify the Tomcat adaptor is installed, configured and working**
- **When its time to install, you will need permission to select "Enable anonymous access". See the installation pdf [www.javasystemsolutions.com/jss/downloads](http://www.javasystemsolutions.com/jss/downloads)**



## Windows Server

Active Directory

## Integrating directly with Active Directory?

The SSO Plugin refers to this as the "Built-in Active Directory Method". This means that, as the customer, you don't have to have anything else other than an Active Directory domain. This is the most common setup our customers have. Microsoft's Integrated Windows Authentication protocol is built on two protocols, NTLM and Kerberos, and depending on the Windows clients on your network, will depend on what one you will need. Here is a best practice lesson learnt the hard way. Some Windows clients send NTLM and some send Kerberos. Therefore, we provide automation tools to assist in configuring both protocols.

This integration requires a computer account to be created within your Active Directory for every midtier. Details of why are here on the [MS Web](#) We have provided a script to do all this for you. The reason is that the standard MS tools let you create a computer account but do not let you assign a password to it. This is critical for security products and therefore why we created the script.



### Task:

- **A computer account needs to be created, in your Active Directory, for every midtier. A script provided can automate this but the manual steps are both documented in our installation.pdf This should be completed before installation time.**
- **If the above script is to be executed by another person or group, then it is important they provide you with the names and passwords used as this information will be required when configuring SSO on the midtier.**

## 1.2 Domain name and login name synchronisation

An important consideration when planning the SSO deployment is multiple accounts configured in different repositories, that do not always match.

For example, David Easters domain login name may be deaster and his AR System or ITSM login name should be the same. When the SSO technology verifies its deaster from the browser and Active Directory, it's that name it will send to the AR Server as the login name. Another challenge is that if your AR Servers operating system is UNIX or LINUX, then case sensitivity comes into play. Meaning if deasters domain login starts with a capital D but his AR system ITSM login name doesn't, then the two names don't match and will never work.

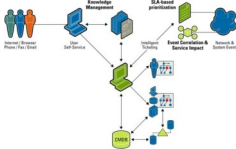
So if you were using any other SSO product, you would see the massive task of possibly modifying all your users to match their domain names. Not with JSS SSO Plugin. We provide automatic features to cover all of the above. This has been the single most important value add for all our customers. In fact we go a step further. If your domain name is deaster, but your AR System / ITSM login includes your domain, we have a feature to build the correct login name to identify you. This is called "Alias username by User for query".



### Task:

- **Investigate how usernames are structured in both the domain and the AR Systems user form.**
- **Decide whether you need to strip/add the domain to the user name.**
- **Decide whether your names are so different you need aliasing.**

## 1.3 What will happen if the user doesn't have an AR System / ITSM account?



Another best practice lesson that can only be learnt from experience. What happens when the domain user doesn't have an account in the AR system / ITSM and they browse to the Home Page? Some customers have tens of thousands of end users and creating accounts for all of those on day 1 is a tough demand. There will always be some that slip through the net. Again, JSS provides functionality that no other SSO solution can. JSS SSO Plugin offers functionality to configure what happens in such scenarios. Including the very popular, "Create an Incident". This automatically gathers information from the Microsoft security model to identify the domain name, the fully qualified domain name and finally the short domain name. And lets you structure a template to create an incident, with the correct data, to allow the service desk to respond effectively and efficiently without the cost of the end user contacting them.

This powerful functionality allows you to build a custom query to identify the domain user within the user form.



### Task:

- **Decide what you want the system to behave when users try to login without an account.**
  - **Redirect to login page**
  - **Redirect to a page allowing them to use their domain name and domain password**
  - **Create an entry in the user form**
  - **Create an incident within the BMC Remedy Incident Management Application.**

## 1.4 Organise the distribution of the User Tool SSO components.

If your company wish to include the BMC Windows User Tool and the BMC Alert Tool in your SSO deployment, then JSS SSO Plugin has that capability. However, this does involve the distribution of two files onto the end users machines. The two files in question are a dynamic link library called ARSSOInfo.dll and a configuration file called ARSSOInfo.ini These files need to be copied into the same directory as the aruser.exe The ARSSOInfo.dll can be found within the product download and the ARSSOInfo.ini will be produced by the installation of SSO Plugin  
Depending on your organisation, this could mean engaging with your desktop distribution team or simply have someone go round the office with a USB stick.



### Task:

- **Investigate how files can be distributed within your organisation.**

## 1.5 Final Checklist



The following list is a guide to help summarise the actions within this document.

- Decide what Authentication Method and action any prerequisites.**
- Investigate username gaps and decide what SSO feature is needed.**
- Decide what your business would like to happen when the user doesn't exist in the AR System / ITSM. If you utilise the incident creation then plan to structure a template.**
- If you are using SSO for the user / alert tool, then investigate file distribution.**

## 1.6 Addendum

- **SSO Plugin 3.3 Installation**
  - [Installation.pdf](#)
  - [Installation Video Walk Through—AR System and User Tool](#)
  - [Installation Video Walk Through—Midtier Active Directory](#)
- [Configuring SSO Plugin with IIS](#)
- [Configuring SSO Plugin with OpenID](#)