Introduction

This document covers:

- Compatibility matrix and other introductory material for SSO Plugin.
- Installation and configuration of SSO Plugin for BMC AR System.
- Installation and configuration of SSO for the Windows User Tool.
- Upgrading from previous versions.

Separate documents are available for other BMC components (ie Mid Tier, Dashboards, Analytics).

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

Compatibility

We strive to support the widest range of products and operating systems. If you require clarification or feel we've missed anything, get in touch with JSS support

Operating systems

Windows 2000, 2003, 2008, 2012

Sun Solaris 5.x

HP-UX 11.x

Linux 2.4.x+

AIX 5.3+.

BMC Action Request System / ITSM

We support all versions of the BMC AR System since version 6.3 even after BMC stopped supporting them.

If you require support for Mid Tier 6.3 or 7.0 then please contact us. For 7.1 to 7.5, use the latest version of SSO Plugin v3.x

For 7.6.04+ please use the latest version of SSO Plugin v4.x

For ITSM integrations we support version 7.03 to 8.x including BMC OnDemand.

Java web servers

We support Tomcat 7+, Weblogic 12c+ and Websphere 8.5+ for the Mid Tier, running under a Java or 7u79 or later Virtual Machine. Please use the latest version of the JVM as the earlier versions contain out-dated SSO related libraries.

If you use another Java servlet engine, please contact us to confirm supportability.

Single-sign on integrations and mechanisms

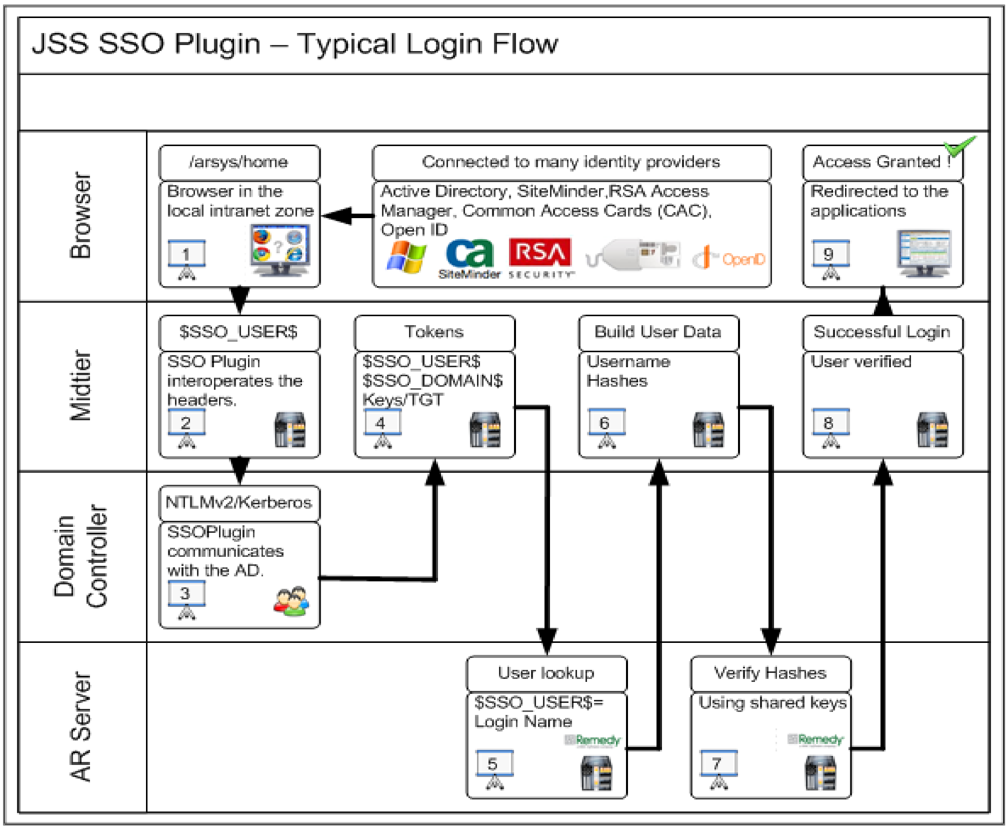
Please consult the Configuring Mid Tier document for a full list of supported integrations/mechanisms.

Mixing versions of SSO Plugin

It is not recommended to mix versions of SSO Plugin within your infrastructure.

Overview of the SSO Plugin

The SSO Plugin is invoked by the Mid Tier when a user goes to /arsys/home, /arsys/forms or /arsys/apps (these paths are configurable).



If the relevant details were available on the incoming request for the SSO Plugin to operate correctly, then these details are passed back to the Mid Tier, which in turn calls the AR System.

Assuming the JSS AREA plugin does not reject the connection – Mid Tier will login successfully.

Please ensure you have read the ARS documentation concerning AREA plugins if you were not aware that blank passwords were required for SSO users in the User form. One of the most common support issues is due to a user not having a blank password in the User form, resulting in the AR System rejecting the request for authentication!

Please note, there are features in SSO Plugin to automate the removal of a user's password so their account is given SSO access. This is an option in the Mid Tier SSO Plugin configuration interface, and is described in the configuring Mid Tier document.

Extensions to AR System authentication

The AR System User form contains a status field that can be set to current and disabled. AR System ignores this setting but the SSO Plugin Mid Tier component does not, so you can disable AR System accounts by using this setting for all authentications passing through an SSO enabled Mid Tier.

AR System installation

The installation zip file contains two directories, installer and midtier. The midtier directory contains the files required by the Mid Tier, and the installer directory contains the files required by the AR System. Not all the files may be used for one particular installation method - please follow the instructions carefully.

The installation has two parts: Configuring the AR System and configuring the Mid Tier. The AR System is configured (and tested) before the Mid Tier is configured.

Please be aware that some of the directory paths may be different on your installation. If in doubt, consult JSS support.

Configuring the AR System

The AR System server you are initially installing must have the Administrator thread. If you are installing to one AR System server then this is not an issue. If you are installing to an AR System server group, then please make sure the server name you connect to owns that thread at that time. This is needed because the installation imports a BMC Application called SSO Administration and for that the Administrator thread is needed.

The product needs to communicate back to the AR System server through the AREA Plugin. BMC do not provide this without login credentials. So the installation process will create a new user with administrator permissions called ssoadmin. The password is not a readable word from any language and includes capital letters, numbers and special characters. Therefore, a fixed license is needed and will need to be free before installing.

The setup program makes use of the BMC ARDBC CONF plugin, which is installed by default on the AR System. If you do not have it installed, the setup program will tell you and to resolve the issue, add the following to your ar.cfg file:

Windows

```
Plugin: “c:\program files\AR System\serverName\ardbcconf.dll”
```

Solaris/Linux

```
Plugin: “/opt/bmc/AR System/bin/ardbcconf.so”
```

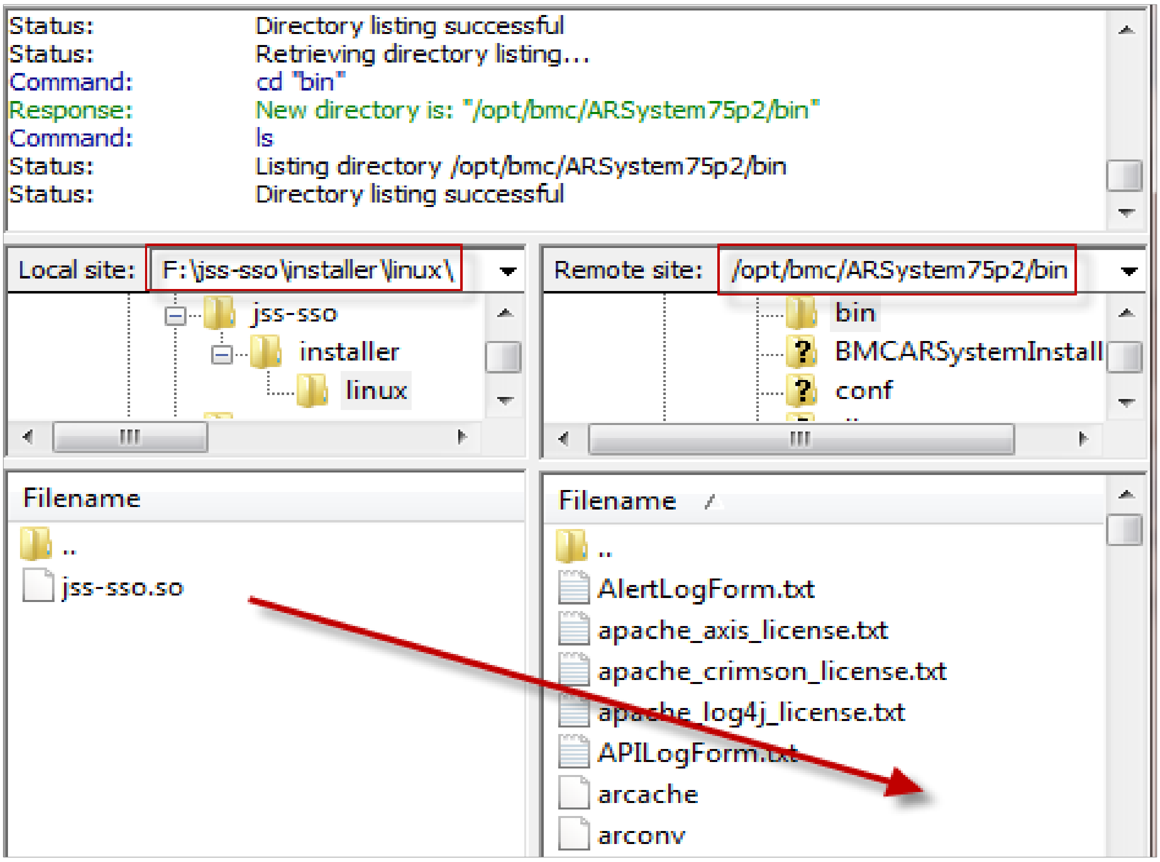
One final prerequisite is that you will need to copy file(s) to the AR System servers. So you will need operating system access.

Copy files to your AR System

If your AR System server runs on a Windows platform, the installer will copy the files to the AR System server directory. If you're using Unix and performing a remote installation, ie running the setup program on a Windows machine and connecting to a remote AR System server, you need to copy the JSS AREA plugin to the AR System server (described below).

Unix

On Unix based operating systems, you have only one file to copy. The relevant found is in the installer/sso-libs/platform directory and is called jss-sso.so. This file can be copied in a number of ways. We recommend FileZilla. The relevant operating system file (Linux, Solaris, HP) needs to be copied to the AR System servers bin directory as seen in the following screenshot:



```
Status:      Directory listing successful
Status:      Retrieving directory listing...
Command:     cd "bin"
Response:    New directory is: "/opt/bmc/ARSystem75p2/bin"
Command:     ls
Status:      Listing directory /opt/bmc/ARSystem75p2/bin
Status:      Directory listing successful
```

Local site: F:\jss-sso\installer\linux\

Remote site: /opt/bmc/ARSystem75p2/bin

Manually copying the Windows files (server groups)

The setup program performs this when running against a Windows based AR System server. However, when configuring server groups, you must manually copy the files to the non-admin thread members of the server group. Browse to the installer/sso-libs/windows directory and unzip the win32.zip file to the same location as deployed on the admin AR System server.

Typically, this is: c:\Program files\BMC Software\AR System\arserver\SSOvXX (where XX is the SSO Plugin release).

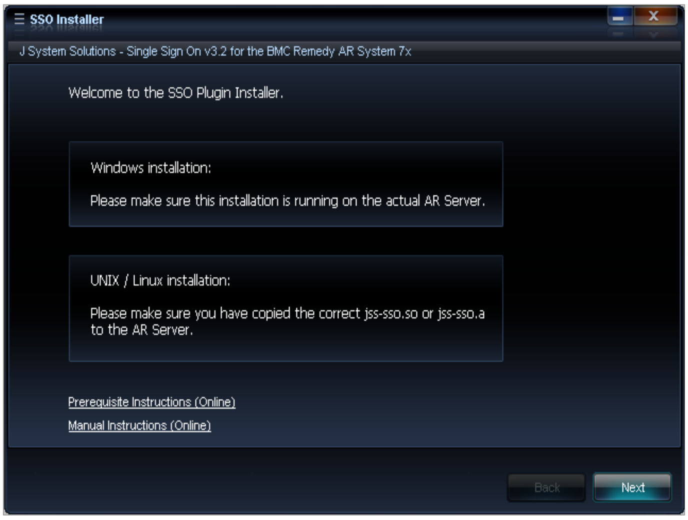
This is required to be set as the Plugin-Path in the ar.cfg file and is described later.

Using the SSO AREA plugin installer

The SSO AREA plugin installer will configure the AR System remotely. This means that as long as you have followed Copy files to your AR System, this application will complete the rest of the AR System server configuration.

Set the AR System cache mode to development (in the AR System Administration Console) and run setup.exe.

Below is a screenshot of the welcome page reminding you that if this is a Windows install to make sure this is running on the actual machine running AR System server or on UNIX or Linux, it's reminding you to place the correct file(s) on the AR System server.



J System Solutions - Single Sign On v3.2 for the BMC Remedy AR System 7x

Welcome to the SSO Plugin Installer.

Windows installation:

Please make sure this installation is running on the actual AR Server.

UNIX / Linux installation:

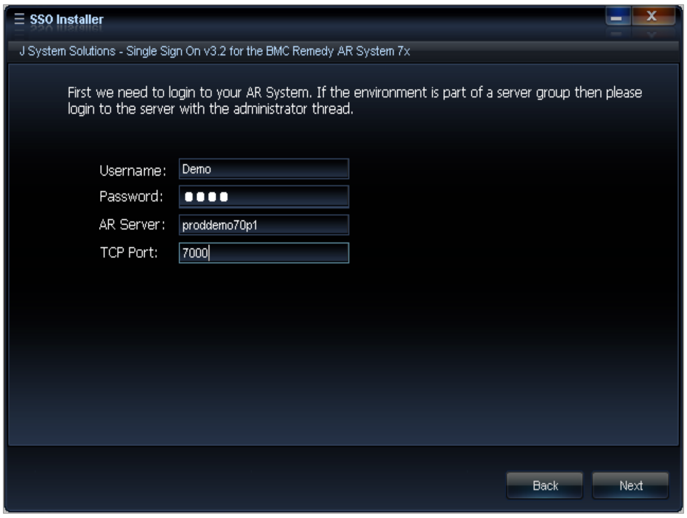
Please make sure you have copied the correct jss-sso.so or jss-sso.a to the AR Server.

Prerequisite Instructions (Online)

Manual Instructions (Online)

Once you have verified the above, tick the box and click Next

Fill in your AR System server details, remembering to use a user with administrative permissions. If you are using a server group then make sure you use the AR System server details of which is running the administrator thread.

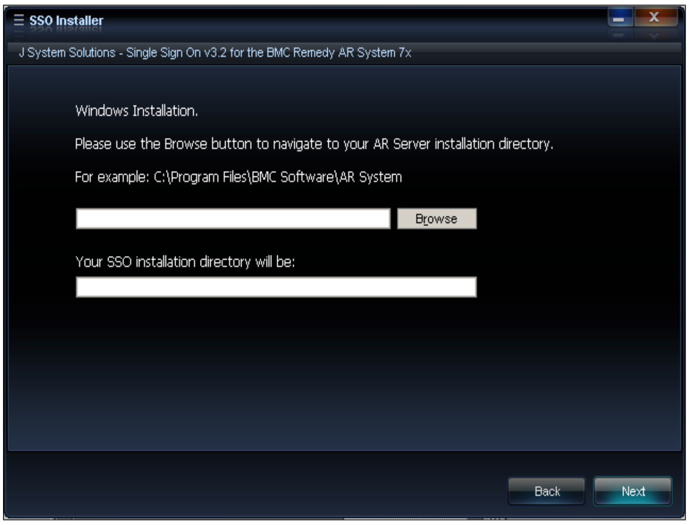


SSO Installer
J System Solutions - Single Sign On v3.2 for the BMC Remedy AR System 7x

First we need to login to your AR System. If the environment is part of a server group then please login to the server with the administrator thread.

Username: Demo
Password: ●●●●
AR Server: proddemo70p1
TCP Port: 7000

If the installation operating system is Windows then you will see the following tab. Use the Browse button to select your AR System installation directory. Select the directory where the arplugin.exe is located.



SSO Installer
J System Solutions - Single Sign On v3.2 for the BMC Remedy AR System 7x

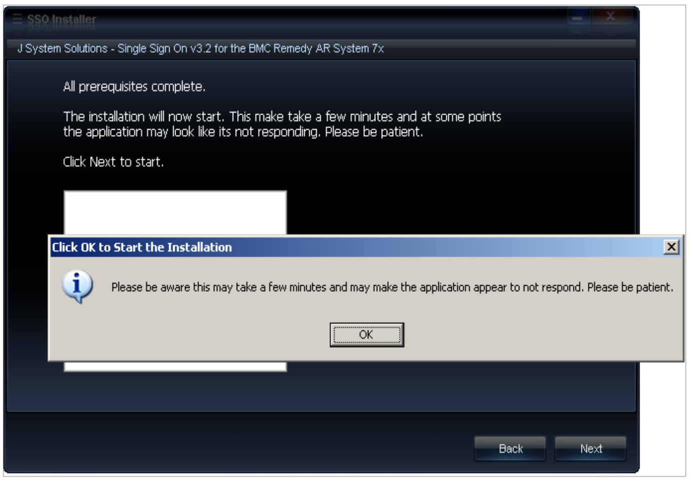
Windows Installation.

Please use the Browse button to navigate to your AR Server installation directory.

For example: C:\Program Files\BMC Software\AR System

Your SSO installation directory will be:

A warning is presented to remind the administrator that this may take some time depending on the AR System server performance. At times the installation may look unresponsive but please be patient. Updates will appear within the white box.



J System Solutions - Single Sign On v3.2 for the BMC Remedy AR System 7x

All prerequisites complete.

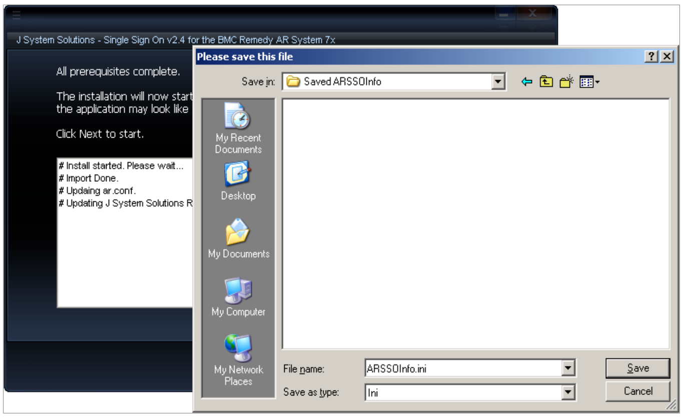
The installation will now start. This make take a few minutes and at some points the application may look like its not responding. Please be patient.

Click Next to start.

Click OK to Start the Installation

Please be aware this may take a few minutes and may make the application appear to not respond. Please be patient.

You will be prompted to save a file called ARSSOInfo.ini. This has to be the name and can not be changed. At this point, the ini file has been configured with specific information belonging to that instance of the AR System or server group. This file also contains encrypted information. Please save this file and keep safe. This file will be one of two files deployed to the clients desktops who wish to use JSS SSO for the BMC Remedy Window User Tool.



J System Solutions - Single Sign On v2.4 for the BMC Remedy AR System 7x

All prerequisites complete.

The installation will now start
the application may look like

Click Next to start.

```
# Install started. Please wait...
# Import Done.
# Updaing ar.conf.
# Updating J System Solutions R
```

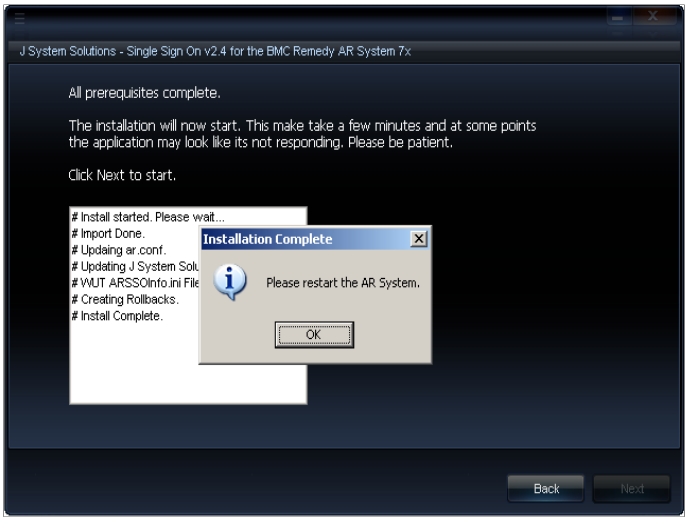
Please save this file

Save in: Saved ARSSOInfo

File name: ARSSOInfo.ini

Save as type: Ini

Finally upon seeing this screen, you must now **restart your AR System**.



J System Solutions - Single Sign On v2.4 for the BMC Remedy AR System 7x

All prerequisites complete.

The installation will now start. This make take a few minutes and at some points the application may look like its not responding. Please be patient.

Click Next to start.

```
# Install started. Please wait...
# Import Done.
# Updaing ar.conf.
# Updating J System Solu
# WUT ARSSOInfo.ini File
# Creating Rollbacks.
# Install Complete.
```

Installation Complete

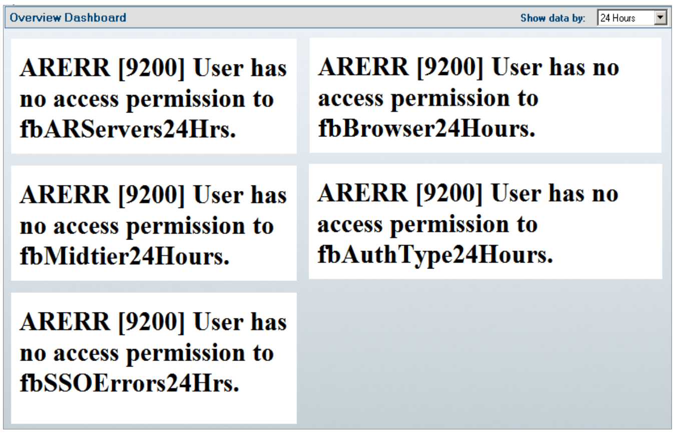
Please restart the AR System.

Installation of the AREA plugin is complete. You can now progress to install the Mid Tier plugin.

Flashboards

When opening the SSO Administration Console, and clicking on the Dashboard > Overview Dashboard, flashboards should render showing valuable information about authentication requests.

If the following error appears, then this means the flashboards will have to be imported manually. This is due to the AR API sometimes preventing the importing of the Flashboards.



ARERR [9200] User has no access permission to fbARServers24Hrs.

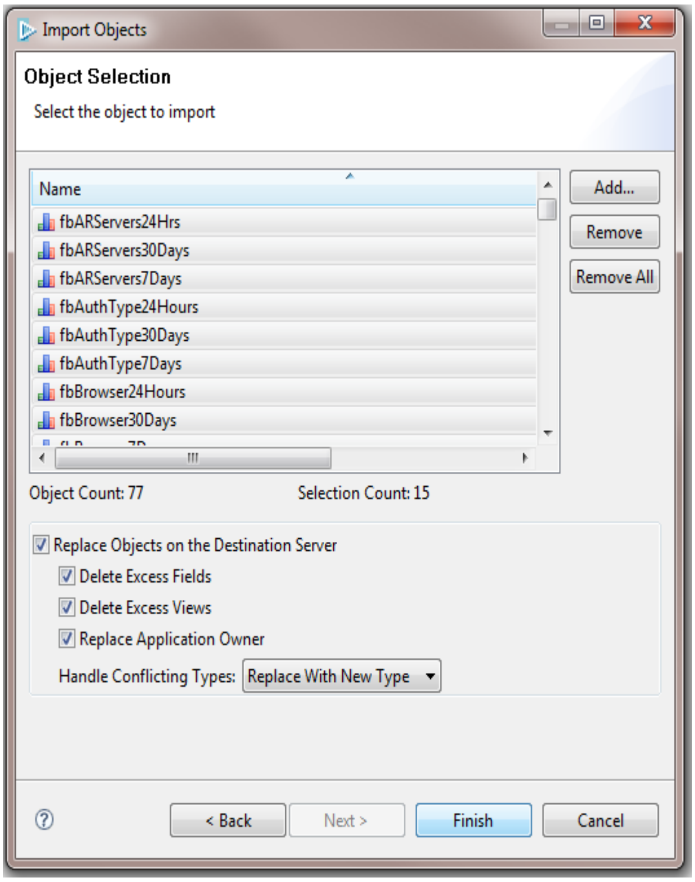
ARERR [9200] User has no access permission to fbBrowser24Hours.

ARERR [9200] User has no access permission to fbMidtier24Hours.

ARERR [9200] User has no access permission to fbAuthType24Hours.

ARERR [9200] User has no access permission to fbSSOErrors24Hrs.

Using the BMC Developer Studio, import the Flashboards manually:



Object Selection

Select the object to import

Name
fbARServers24Hrs
fbARServers30Days
fbARServers7Days
fbAuthType24Hours
fbAuthType30Days
fbAuthType7Days
fbBrowser24Hours
fbBrowser30Days

Object Count: 77   Selection Count: 15

☑ Replace Objects on the Destination Server

☑ Delete Excess Fields

☑ Delete Excess Views

☑ Replace Application Owner

Handle Conflicting Types: Replace With New Type

Server groups

The SSO Plugin holds the configuration in a form (JSS:SSO:ARSConfig) within AR System. Therefore, when using AR System server groups, the installation steps are as follows:

1. Login to AR System as an admin user, query AR System Server Group Operation Ranking form and this will tell you the name of the AR System server running the administrator thread.
2. Run the installer against the AR System server with the administrator thread. This will import an AR System definition file to store the configuration information, and thus the admin thread needs to be present.
3. Make sure you follow the same steps as Copy files to your AR System on the remaining AR System servers in the server group
4. The installer wrote an entry to the AR System ar.cfg/conf file called jss-sso-salt, which is used to generate the password to the ssoadmin account (created by the installer). Open the ar.cfg/conf file on the AR System server with the **administrator** thread and copy the jss-sso-salt entry.
5. For each of the additional AR System servers in the group, add the following lines to your ar.cfg or ar.conf file:

```
Plugin-Path: C:\Program Files (x86)\BMC Software\ARSystem\SSOvXX (where XX is version)
Plugin: “C:\Program Files (x86)\BMC Software\ARSystem\SSOvXX\jss-sso.dll”
Crossref-Blank-Password: T
External-Authentication-RPC-Socket: 390695
External-Authentication-Return-Data-Capabilities: 31
Authentication-Chaining-Mode: 0
Allow-Guest-Users: F
jss-sso-salt: valueNotedInStep4
```

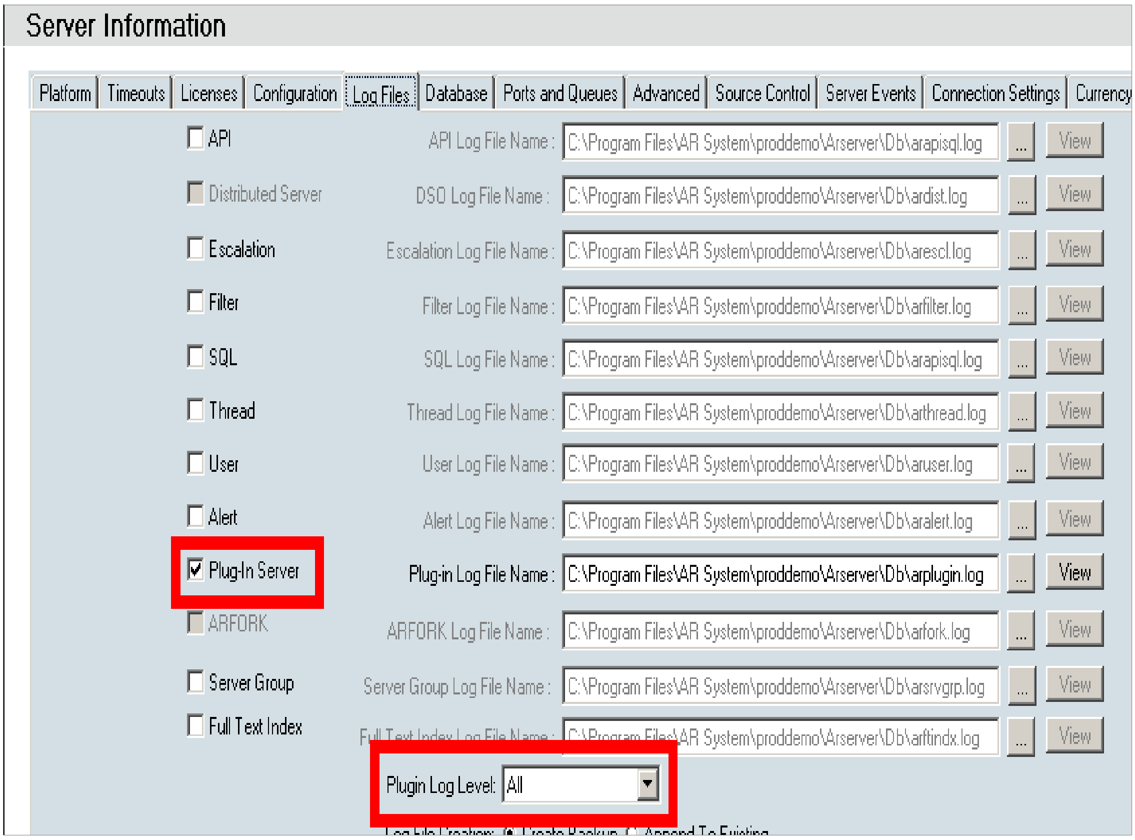
6. Restart the AR System servers.

Enable logging for verification

The JSS AREA plugin can be verified via the AR Systems plugin log file. It is recommended this be enabled now to save time and effort later.

Login to AR System using the BMC Windows User Tool with an administrative user. Open the AR System Administration Console and click on System and then General.

- Click on the Log Files tab.
- Check the Plug-in Server
- Check the Plug-in Log Level to ALL
- Click Apply and Save.



Server Information

□ API — API Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arapisql.log

□ Distributed Server — DSO Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\ardist.log

□ Escalation — Escalation Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arescl.log

□ Filter — Filter Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arfilter.log

□ SQL — SQL Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arapisql.log

□ Thread — Thread Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arthread.log

□ User — User Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\aruser.log

□ Alert — Alert Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\aralert.log

☑ Plug-In Server — Plug-in Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arplugin.log

□ ARFORK — ARFORK Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arfork.log

□ Server Group — Server Group Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arsrvgrp.log

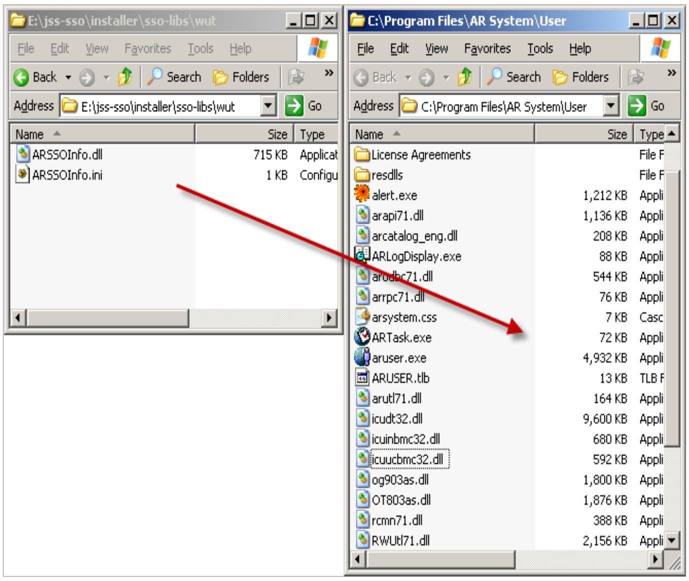
□ Full Text Index — Full Text Index Log File Name : C:\Program Files\AR System\proddemo\Arserver\Db\arftindx.log

Plugin Log Level: All

Log File Creation: ● Create Backup ○ Append To Existing

SSO for the Windows User Tool

If you used the installation setup.exe, you would have been prompted to save a file called ARSSOInfo.ini. This file coupled with a dynamic link library, ARSSOInfo.dll, must be copied to the client machine and placed in the same director as aruser.exe.


E:\jss-sso\installer\sso-libs\wut
File Edit View Favorites Tools Help
Back Search Folders
Address E:\jss-sso\installer\sso-libs\wut Go
C:\Program Files\AR System\User
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\AR System\User Go

Name	Size	Type
ARSSOInfo.dll	715 KB	Applicat
ARSSOInfo.ini	1 KB	Configu

Name	Size	Type
License Agreements		File F
resdlls		File F
alert.exe	1,212 KB	Appli
arapi71.dll	1,136 KB	Appli
arcatalog_eng.dll	208 KB	Appli
ARLogDisplay.exe	88 KB	Appli
arodbc71.dll	544 KB	Appli
arrpc71.dll	76 KB	Appli
arsystem.css	7 KB	Casc
ARTask.exe	72 KB	Appli
aruser.exe	4,932 KB	Appli
ARUSER.tlb	13 KB	TLB F
arutl71.dll	164 KB	Appli
icudt32.dll	9,600 KB	Appli
icuinbmc32.dll	680 KB	Appli
icuucbmc32.dll	592 KB	Appli
og903as.dll	1,800 KB	Appli
OT803as.dll	1,876 KB	Appli
rcmn71.dll	388 KB	Appli
RWUtl71.dll	2,156 KB	Appli

Explanation of the ARSSOInfo.ini file

The contents of the ini file dictate how the SSO interface works. Here is an explanation of those settings:

General Section

Enabled: Values are 1 means enabled, 0 means disabled. If the option is 0 then you are prompted with the login screen as normal.

Loginarserver: Values are arserver1, arserver2. This points to the section of AR System server connection information that should be used to login.

Userpreferenceserver: Values are arserver1, arserver2. This points to the section of AR System server connection information that should be used as the preference server.

Debuglogging: If asked by JSS to enable logging, this option should be set to 1.

Ssover: Values are 2 or 3. This version should match whatever SSO version you are running on your AR System server(s).

ARServer section

servername: this is the server-name reference in the ar.cfg file. If you are using server groups then this will be the front end load balancer DNS name.

servertcpport: This should be the TCP port of the arserver

serverrpcport: If you need your clients to connect to a certain RPC port then place that value here.

shared-key: This is the unique encrypted value that is used to ensure security.

newshared-key: If the jss-sso-salt (in the AR System SSO Plugin configuration) changes, enter the value and restart aruser.exe.

forcemode: Values 0,1,2,3,4,5. This changes the format of the username and/or the domain, before the values are submitted for authentication to the AR System server.

The modes are as follows:

0. Will send the username and domain as presented in the Active Directory.
1. Will modify both the username and domain to lowercase. eg dev\dkellett
2. Will modify both the username and domain to uppercase. eg DEV\DKELLETT
3. Will modify both the username first letter to capitals. eg dev\Dkellett
4. Will modify the username to uppercase and the domain to lowercase. eg dev\DKELLETT
5. Will modify the username to lowercase and the domain to uppercase. Eg DEV\dkellett

Please note: the forcemode parameter is also applied if user aliasing is enabled.

useralias: See Mapping Windows accounts to AR System login names below.

Mapping Windows accounts to AR System login names

If your AR System login names are constructed with the domain name, you can use the ini file parameter *useralias* to construct a bespoke login name with the following variables:

- SSO_USER: the domain username and is mandatory. If this is missing the whole line/feature will be ignored.
- SSO_DOMAIN: the NETBIOS (short name) of your domain, ie javasystemsolutions.
- SSO_DOMAIN_LONG: the Windows DNS Domain name, ie javasystemsolutions.com.

For example, consider user dkellett logged into the JAVASYSTEMSOLUTIONS (dns: javasystemsolutions.com) domain:

- useralias=SSO_DOMAIN\SSO_USER creates a login name JAVASYSTEMSOLUTIONS\dkellett
- useralias=$SSO_DOMAIN_ LONG$\SSO_USER creates a login name javasystemsolutios.com\dkellett

This feature can be used in conjunction with the forcemode feature. For example, if forcemode=1 then the generated login will all be lowercased.

Recreating a lost ARSSOInfo.ini

The ARSSOInfo.ini file contains encrypted information and is unique to every AR System server SSO enabled instance. The installation program can recreate those same encrypted keys by logging into an SSO enabled AR System. Use the same installation program, login when asked and you should be shown a different screen following a discovered SSO instance. Select Create ARSSOInfo.ini and Exit, click Next and you should be prompted to save the new file.

Mid Tier installation

A separate highly detailed document exists that explains how to configure SSO Plugin for Mid Tier. This section only covers the installation process.

To install the SSO Plugin on the Mid Tier, please follow these steps:

1. Copy the contents of the midtier directory into the root Mid Tier directory. ie. the contents of midtier into the Mid Tier directory that contains the WEB-INF directory.
2. If the BMC Mid Tier version is 8.1.01 SP1 or higher, please delete the Xerces jar file that BMC install in the midtier/web-inf/lib directory
3. Restart Mid Tier.
4. If you are using IBM Websphere 7, use WAS to ensure the com.ibm.ws.jsp.jdkSourceLevel custom property is set to 14 or 15 on the web extension file or the custom WebContainer. This tells Websphere that the application was compiled for Java 1.5+.
5. Go to the SSO Plugin status page by pointing your browser at http://path-to-Mid Tier/arsys/jss-sso/index.jsp. You will be presented with a status page. The password field in the left navigation is used to enable configuration and accepts the Mid Tier configuration password.
6. Locate the document titled Configuring Mid Tier and Web Tier to configure the SSO Plugin.
7. Test the SSO configuration by clicking on the Test SSO link in from the SSO Plugin status page. This will attempt to perform an SSO login to the authentication server and report any errors. If the test is successful when you can click on the Mid Tier Home link in the navigation and you should be taken directly to the Mid Tier Homepage without being asked to login.
8. If SSO fails then review the troubleshooting document or contact JSS support.

Replacing the BMC Mid Tier login page

It is common to find users bookmark the BMC login page, ie /arsys/shared/login.jsp. This results in support enquiries as SSO will not be activated when this page is requested by users.

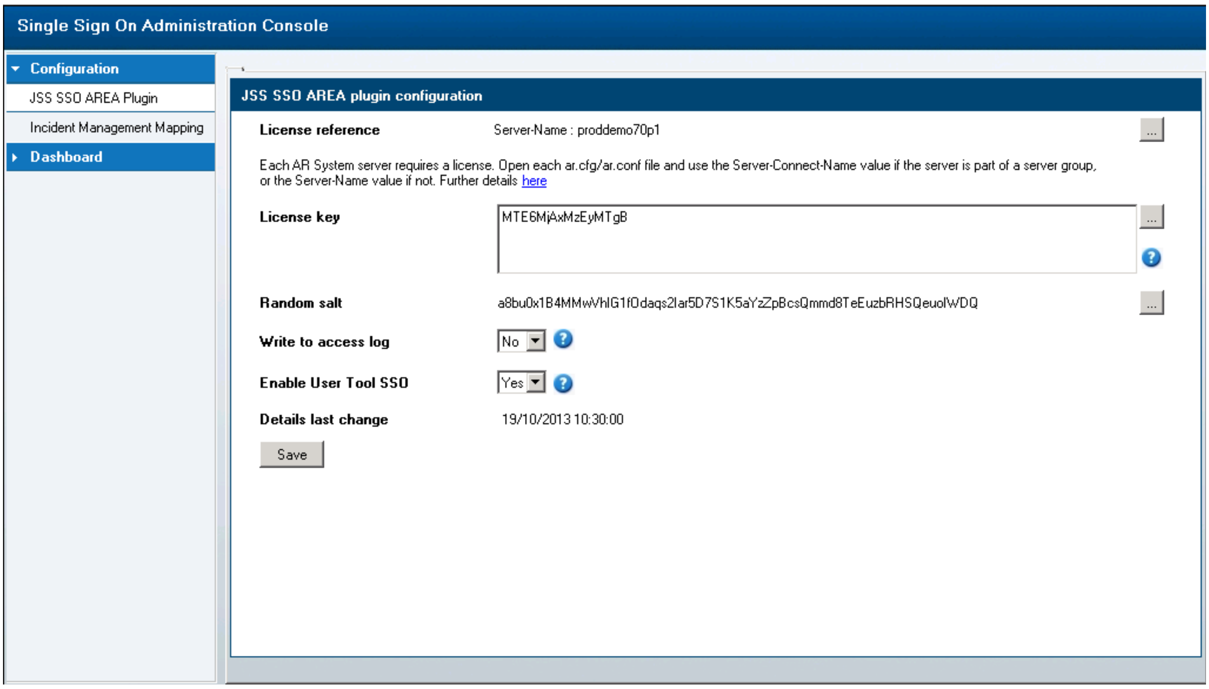
Therefore, a replacement login page has been provided that is consistent with BMC branding but also highlights the SSO facility to the user. To install the page, follow these steps:

1. Locate existing Mid Tier login.jsp page under the Mid Tier shared directory.
2. Rename the existing login.jsp to login.jsp.old.
3. Create a new file login.jsp and place the following in it:

```
<jsp:forward page="/jss-sso/manuallogin" />
```

SSO Administration Console

The product is supplied with AR System forms and workflow that provides an SSO Administration Console which looks like this:


Single Sign On Administration Console
Configuration
JSS SSO AREA Plugin
Incident Management Mapping
Dashboard
JSS SSO AREA plugin configuration
...
Save

License reference Server-Name : proddemo70p1

Each AR System server requires a license. Open each ar.cfg/ar.conf file and use the Server-Connect-Name value if the server is part of a server group, or the Server-Name value if not. Further details here

License key MTE6MjAxMzEyMTgB

Random salt a8bu0x1B4MMwVhIG1fOdaqs2Iar5D7S1K5aYzZpBcsQmmd8TeEuzbRHSQeuolWDQ

Write to access log No

Enable User Tool SSO Yes

Details last change 19/10/2013 10:30:00

The console allows the administrator to configure the JSS AREA Plugin by the license (populated with a default date restricted license during installation), and other information useful for debugging the product.

When an update is made to the SSO Administration Console and the server is part of an AR Server Group, connect to each server in the group, go to the console and press save. This will cause each JSS AREA plugin to reload its configuration.

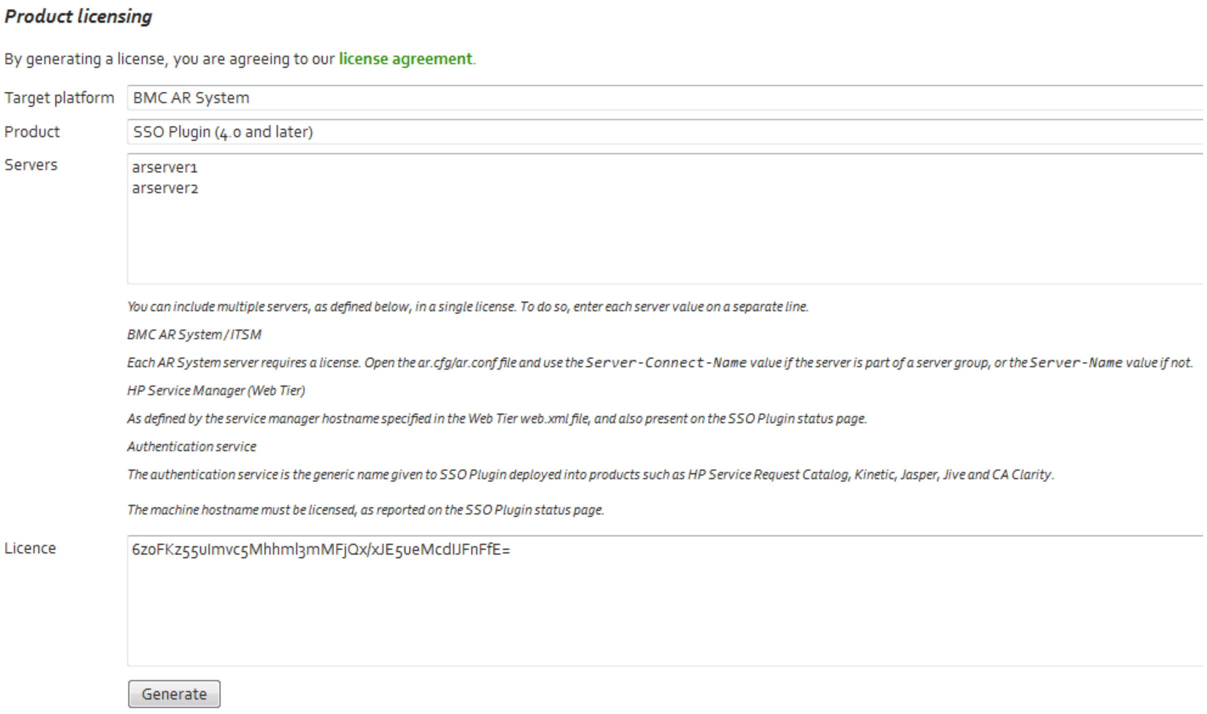
Access logging

The console contains a control called 'Write access log'. This logs each SSO authentication request, whether successful or not, in a form that can be used to create Flashboards. These can be found under the Dashboard navigation link.

Licensing

Both a 60 day evaluation license and a permanent instance license can be generated on our website. Permanent instance licenses are based on ar.cfg/conf entries Server-Connect-Name, if a server group exists, or Server-Name.

If the instance is configured as a server group, collect all Server-Connect-Names from the ar.cfg/conf files. Browse to the SSO Plugin License page. Enter each Server-Connect-Name on a separate line and click Generate. The license will be created as see in the example screenshot below.



Product licensing

By generating a license, you are agreeing to our license agreement.

Target platform: BMC AR System

Product: SSO Plugin (4.0 and later)

Servers:
arserver1
arserver2

You can include multiple servers, as defined below, in a single license. To do so, enter each server value on a separate line.

BMC AR System / ITSM

Each AR System server requires a license. Open the ar.cfg/ar.conf file and use the `Server-Connect-Name` value if the server is part of a server group, or the `Server-Name` value if not.

HP Service Manager (Web Tier)

As defined by the service manager hostname specified in the Web Tier web.xml file, and also present on the SSO Plugin status page.

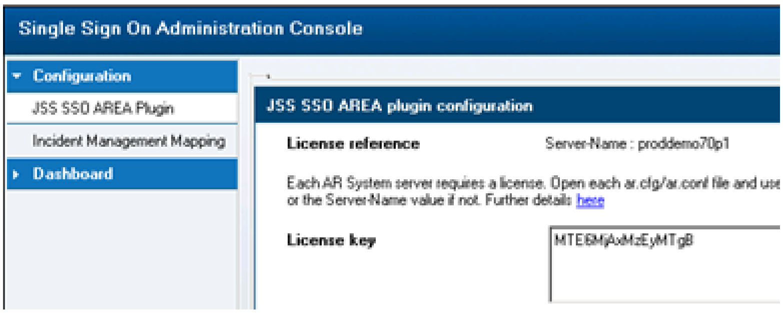
Authentication service

The authentication service is the generic name given to SSO Plugin deployed into products such as HP Service Request Catalog, Kinetic, Jasper, Jive and CA Clarity.

The machine hostname must be licensed, as reported on the SSO Plugin status page.

Licence: 6zoFKz55uImvc5Mhhml3mMFjQx/xJE5ueMcdIJFnFfE=

To apply the license, login to the application as an administrative user. Open the SSO Administration Console and replace the existing license with the one generated above. If the instance is configured as a server group, then it is recommended you restart all AR Server services.



Single Sign On Administration Console
Configuration
JSS SSO AREA Plugin
Incident Management Mapping
Dashboard
JSS SSO AREA plugin configuration

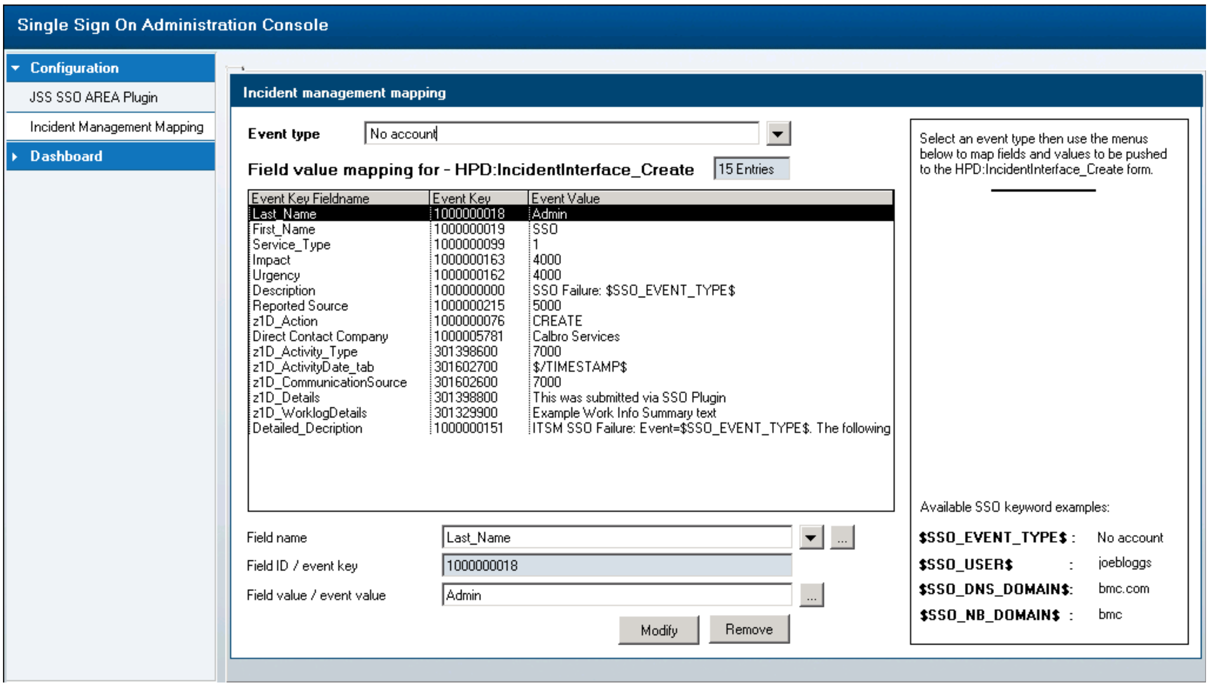
License reference: Server-Name : proddemo70p1

Each AR System server requires a license. Open each ar.cfg/ar.conf file and use
or the Server-Name value if not. Further details here

License key: MTE6MjAxMzEyMTgB

ITSM Incident Mapping

The product allows incidents to be raised when a user can not access the product. The configuration interface is linked from the SSO Administration Console and looks like this:



Single Sign On Administration Console
Configuration
JSS SSO AREA Plugin
Incident Management Mapping
Dashboard
Incident management mapping

Event type: No account

Field value mapping for - HPD:IncidentInterface_Create   15 Entries

Event Key Fieldname	Event Key	Event Value
Last_Name	1000000018	Admin
First_Name	1000000019	SSO
Service_Type	1000000099	1
Impact	1000000163	4000
Urgency	1000000162	4000
Description	1000000000	SSO Failure: SSO_EVENT_TYPE
Reported Source	1000000215	5000
z1D_Action	1000000076	CREATE
Direct Contact Company	1000005781	Calbro Services
z1D_Activity_Type	301398600	7000
z1D_ActivityDate_tab	301602700	$/TIMESTAMP$
z1D_CommunicationSource	301602600	7000
z1D_Details	301398800	This was submitted via SSO Plugin
z1D_WorklogDetails	301329900	Example Work Info Summary text
Detailed_Decription	1000000151	ITSM SSO Failure: Event=SSO_EVENT_TYPE. The following

Field name: Last_Name

Field ID / event key: 1000000018

Field value / event value: Admin

Select an event type then use the menus below to map fields and values to be pushed to the HPD:IncidentInterface_Create form.

Available SSO keyword examples:

SSO_EVENT_TYPE :	No account
SSO_USER :	joebloggs
SSO_DNS_DOMAIN:	bmc.com
SSO_NB_DOMAIN :	bmc

The event type drop down selects the type of SSO failure event that will be mapped to the incident and the default event type will be used if a specific type is not configured. When the mapping has been located, SSO Plugin will submit data to the BMC Incident Management application through the BMC out of the box HPD:IncidentInterface_Create form. This is completely configurable and easily configured using the Incident Mapping form showed in the screenshot.

The special variables ($SSO_USERNAME$, SSO_DNS_DOMAIN, etc), that are also used for the user aliasing feature, can be used when mapping text to a field.

Self-service ITSM user creation

This feature removes the need for daily synchronisation with a corporate Active Directory because new starters can register themselves with ITSM by virtue of passing through the configured SSO system.

The product provides a feature to allow user accounts to be created when a user does not have an account in ITSM. To use this feature, a Person Template must be configured in the SSO Plugin Mid Tier interface. The user is asked to supply their first name, last name, email address and phone number, which when combined with the Person Template, will be used to generate a new entry in the People form.

Manually configuring the AR System

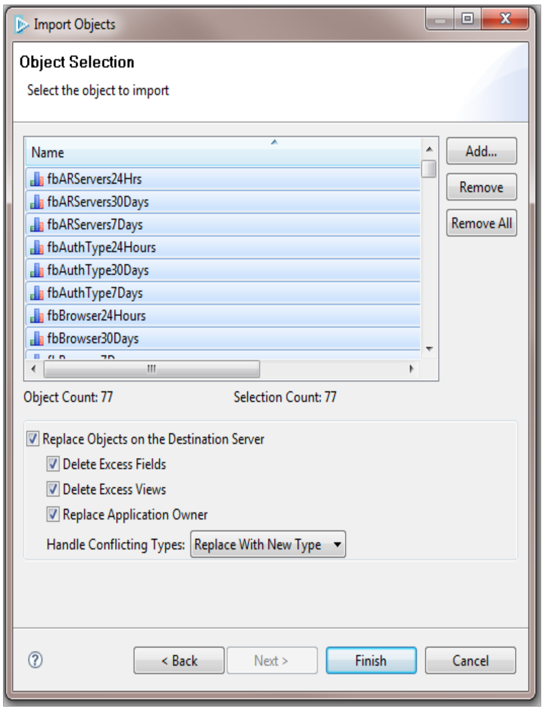
If for any reason the installation program fails. As always, you can contact JSS support. However, you can manually install the product with the following steps.

Please make sure you have copied the files as in section Copy files to your AR System

Import workflow

Before doing this, set the AR System cache mode to development. This is to ensure the definition file loads correctly.

Locate the ssoadm40.def file within the downloaded zip from the evaluation package. Depending on what version you have of your AR System depends on how this is imported. The screenshot below is taken from a 7.1 Administrator Tool. Please note that the option “Replace Objects on the Destination Server” is checked and the “Handle Conflicting Types” is set to “Replace with new type” and make sure ALL OBJECTS are imported from the def file including the flashboard variables and flashboards themselves.



Import Objects

Object Selection

Select the object to import

Name
fbARServers24Hrs
fbARServers30Days
fbARServers7Days
fbAuthType24Hours
fbAuthType30Days
fbAuthType7Days
fbBrowser24Hours
fbBrowser30Days

Object Count: 77

Selection Count: 77

☑ Replace Objects on the Destination Server

☑ Delete Excess Fields

☑ Delete Excess Views

☑ Replace Application Owner

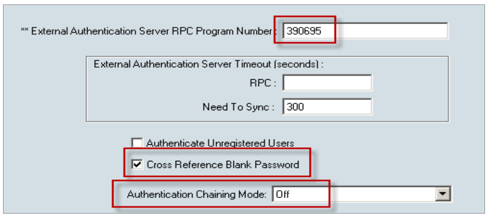
Handle Conflicting Types: Replace With New Type

Check AR External Authentication (AREA) is enabled

Login via the BMC Remedy User Tool with a user with administrative permissions. Open the AR System Administration Console and click on System and then General.

- Click on the EA tab.
- Make sure the RPC number is **390695**
- **Check** the Cross Reference Blank Password
- Authentication Chaining Mode set to **Off**

- Click Apply and Save.



** External Authentication Server RPC Program Number: 390695

External Authentication Server Timeout (seconds) :

RPC :

Need To Sync : 300

□ Authenticate Unregistered Users

☑ Cross Reference Blank Password

Authentication Chaining Mode: Off

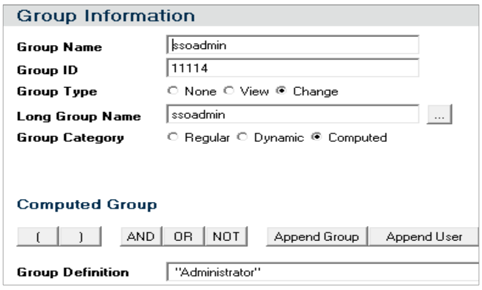
Disable 'Allow Guest Users'

This must be disabled or the AR System will allow login attempts for users that are not present in the User form. When enabled, the JSS AREA plugin is not called for guest users, and hence automatically accepting guest users poses a security risk.

Creating the ssoadmin account

The sso plugin needs to communicate with the AR System server. This is done through a specific user called ssoadmin. The password is generated and is system dependant.

Create a group with the following attributes:



Group Information

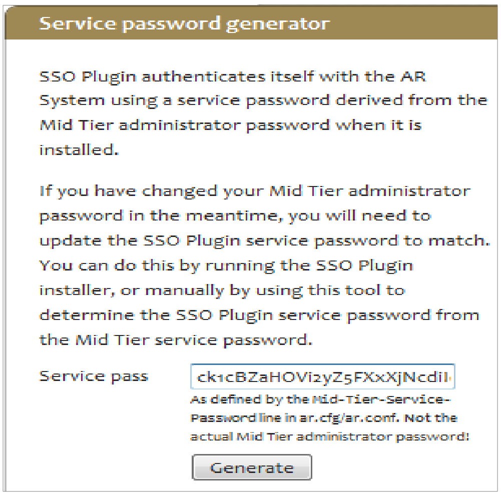
Group Name: ssoadmin
Group ID: 11114
Group Type: ○ None ○ View ● Change
Long Group Name: ssoadmin
Group Category: ○ Regular ○ Dynamic ● Computed

Computed Group

Group Definition: "Administrator"

Login to the JSS Support website through this URL

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



Service password generator

SSO Plugin authenticates itself with the AR System using a service password derived from the Mid Tier administrator password when it is installed.

If you have changed your Mid Tier administrator password in the meantime, you will need to update the SSO Plugin service password to match. You can do this by running the SSO Plugin installer, or manually by using this tool to determine the SSO Plugin service password from the Mid Tier service password.

Service pass: ck1cBZaHOVi2yZ5FXxXjNcdil

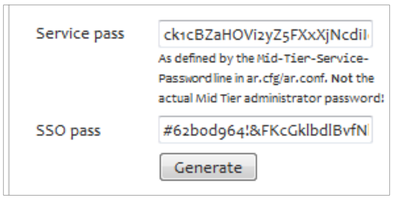
As defined by the Mid-Tier-Service-Password line in ar.cfg/ar.conf. Not the actual Mid Tier administrator password!

Place the text from the jss-ss-salt in the ar.cfg/ar.conf entry into the **Service pass** field and click **Generate**.

Example: If you see this in your ar.conf then copy everything after the colon.

jss-sso-salt: **asd9asda2313sd0as0dualpq78w4as09eqweas0uas0qwe7aswas09da**

After clicking Generate, you should see the SSO password.

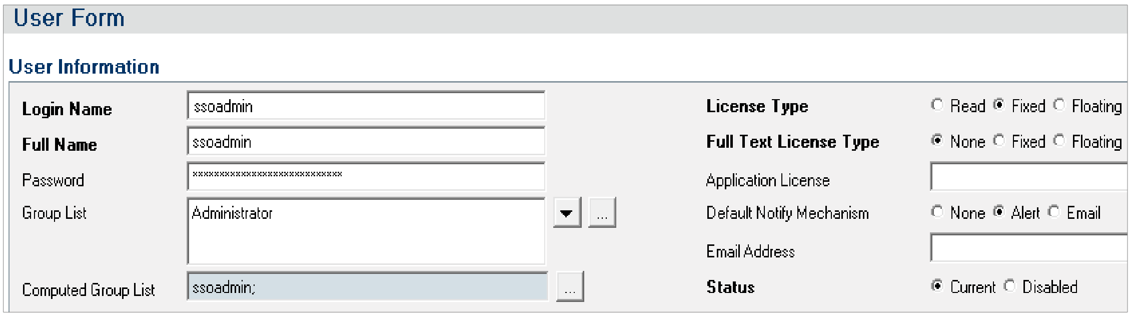


Service pass: ck1cBZaHOVi2yZ5FXxXjNcdil

As defined by the Mid-Tier-Service-Password line in ar.cfg/ar.conf. Not the actual Mid Tier administrator password!

SSO pass: #62bod964!&FKcGklbdlBvfN

Create a user with the following attributes



User Form

User Information

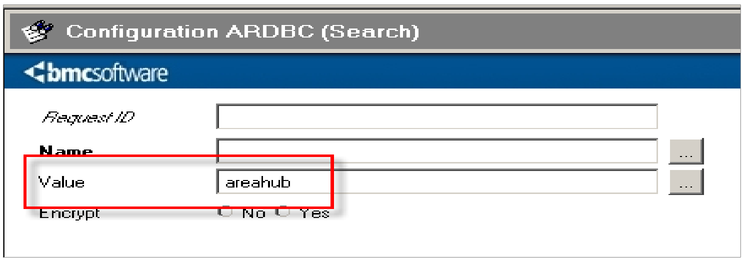
Login Name	ssoadmin	License Type	○ Read ● Fixed ○ Floating
Full Name	ssoadmin	Full Text License Type	● None ○ Fixed ○ Floating
Password	****************************	Application License	
Group List	Administrator	Default Notify Mechanism	○ None ● Alert ○ Email
		Email Address	
Computed Group List	ssoadmin;	Status	● Current ○ Disabled

Check the AREA Hub is installed and configured.

If you are using the BMC AREA LDAP plugin, then a prerequisite to enable SSO is that the AR System server in question has the BMC AREA-Hub plugin installed.

To check this is configured, you can either look directly at the ar.conf / ar.cfg file or you can use the AR System User Tool.

Open the User Tool and Search for the form Configuration ARDBC. Once opened place the value areahub in the name field and search:

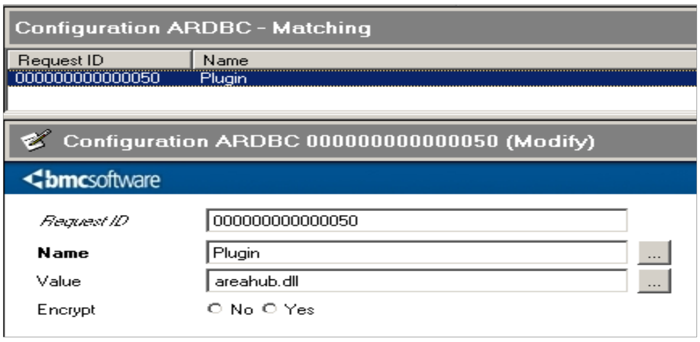


Configuration ARDBC (Search)

Request ID	
Name	
Value	areahub
Encrypt	○ No ○ Yes

Screenshot showing searching for the areahub

If this is configured, then you should observe a reply showing the areahub in the ar.conf / ar.cfg



Configuration ARDBC - Matching

Request ID	Name
000000000000050	Plugin

Configuration ARDBC 000000000000050 (Modify)

Request ID	000000000000050
Name	Plugin
Value	areahub.dll
Encrypt	○ No ○ Yes

Screenshot showing the results of the search if the areahub is installed.

If this setting is not found within the ar.cfg file or through the Configuration ARDBC form then you can quickly enable it by adding the following lines to your ar.cfg file.

Windows

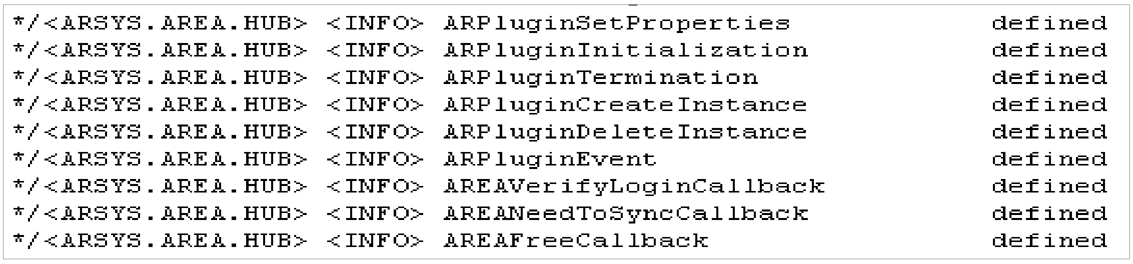
```
Plugin: “C:\Program Files\AR System\ServerName\areahub.dll”
```

Solaris/Linux

```
Plugin: “/opt/bmc/AR system/bin/areahub.so”
```

You will need to restart the AR System and this can be verified within the Plug-in log file as described in section Enable logging for verification

Below is an example of what to look for within the Plug-in log file to verify the areahub is installed and configured. If the file is large, you can easily search for ARSYS.AREA.HUB



```
*/<ARSYS.AREA.HUB> <INFO> ARPluginSetProperties          defined
*/<ARSYS.AREA.HUB> <INFO> ARPluginInitialization         defined
*/<ARSYS.AREA.HUB> <INFO> ARPluginTermination            defined
*/<ARSYS.AREA.HUB> <INFO> ARPluginCreateInstance         defined
*/<ARSYS.AREA.HUB> <INFO> ARPluginDeleteInstance         defined
*/<ARSYS.AREA.HUB> <INFO> ARPluginEvent                  defined
*/<ARSYS.AREA.HUB> <INFO> AREAVerifyLoginCallback        defined
*/<ARSYS.AREA.HUB> <INFO> AREANeedToSyncCallback         defined
*/<ARSYS.AREA.HUB> <INFO> AREAFreeCallback               defined
```

Windows User Tool SSO – ARSSOInfo.dll

Deploying SSO for WUT involves placing two files in the same directory as aruser.exe on the client machine.

Please continue to this section SSO for the BMC Remedy Windows User Tool

Copying the JSS AREA plugin to the AR System

Windows

Unpack the win32.zip file found in the installation directory (installer\sso-libs\windows) into a directory called SSOPluginVERSION (where VERSION is 34, etc) and add the following to the ar.cfg file:

```
Plugin-Path: c:\path\to\SSOPluginVERSION
```

Please note: If you do not set this then the plugin server will respond slowly as it tries to search for the libraries required by the JSS AREA plugin.

If you are not using the BMC AREA LDAP plugin, add the following to the ar.cfg:

```
Plugin: "c:\path\to\SSOPluginVERSION\jss-sso.dll"
```

If you are using the BMC AREA LDAP plugin then review the Configure the AREA HUB to use the SSO Plugin section below.

Solaris/Linux

Copy the relevant jss-sso.so plugin from the installation files (locate the relevant installer\sso-libs\os directory) to the same directory as the arplugin binary.

If you are not using the BMC AREA LDAP plugin, add the following to the ar.cfg:

```
Plugin: "/opt/bmc/AR system/ServerName/jss-sso.so"
```

If you are using the BMC AREA LDAP plugin then review the Configure the AREA HUB to use the SSO Plugin section below.

Check the AREA LDAP configuration

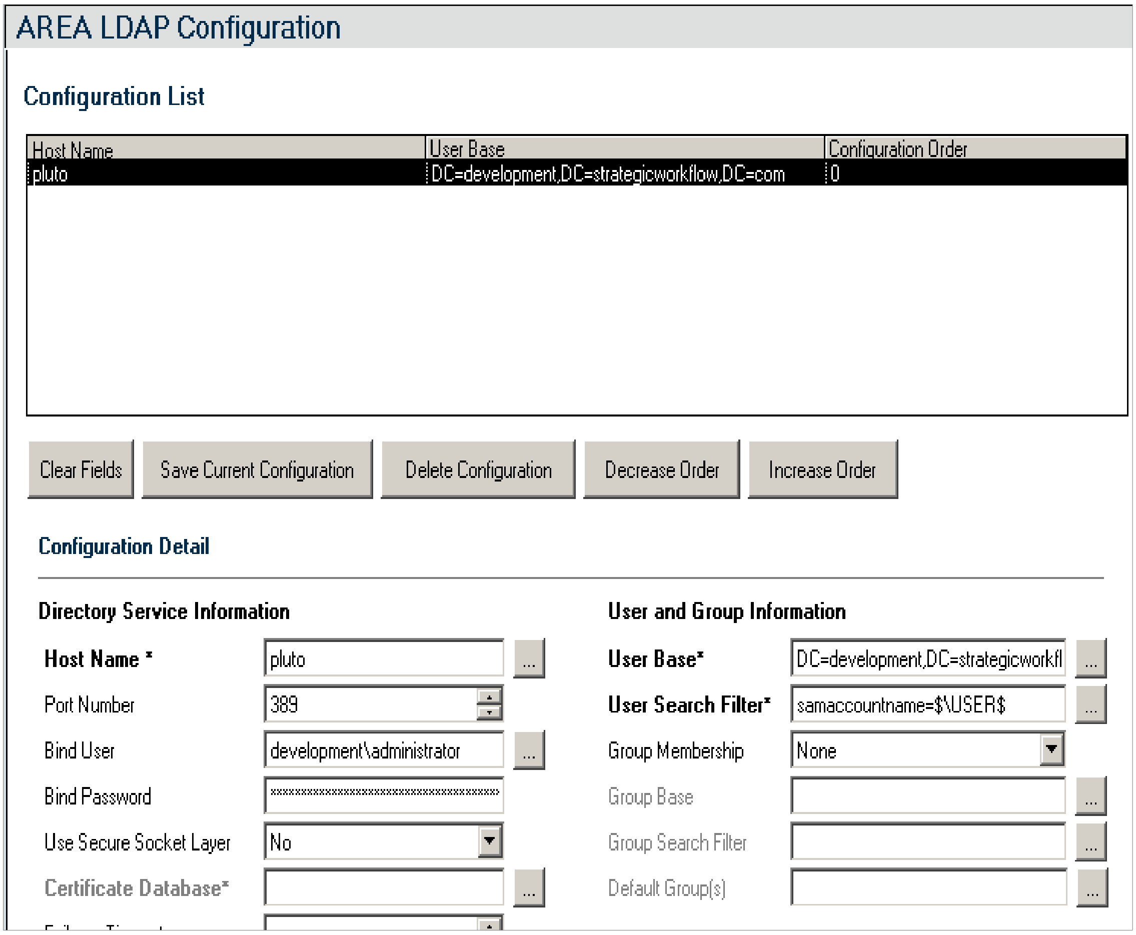
Only follow this section if you are using an LDAP or Active Directory to store your user information. Alternatively, if you are just using the AR Systems USER table to verify then skip to Configure the AREA HUB to Use the JSS SSO Plugin.

After confirming the AREA Hub is installed, the next configuration task is to configure or confirm the configuration of the BMC AREA LDAP Plugin. The JSS SSO product will enable the user to login to the AR System via SSO but for those users who are not configured to use SSO may have to verify via other means.

Details can be found in the following documentation:

- Page 152 of the BMC Remedy Action Request System 7.0 Integrating with Plug-ins and Third-Party Products
  http://www.bmc.com/supportu/documents/84/67/58467/58467.pdf
- Page 133 of the BMC Remedy Action Request System 7.1.00 Integrating with Plug-ins and Third-Party Products
  http://www.bmc.com/supportu/documents/93/94/69394/69394.pdf
- Page 143 of the BMC Remedy Action Request System 7.5.00 Integration Guide
  http://www.bmc.com/supportu/documents/53/80/95380/95380.pdf

Open the form AREA LDAP Configuration form and make sure the details are populated and that a user can use the User Tool or Mid Tier to login via AREA.



AREA LDAP Configuration

Configuration List

Host Name	User Base	Configuration Order
pluto	DC=development,DC=strategicworkflow,DC=com	0

Configuration Detail

Directory Service Information

Host Name *	pluto
Port Number	389
Bind User	development\administrator
Bind Password	************************************
Use Secure Socket Layer	No
Certificate Database*	

User and Group Information

User Base*	DC=development,DC=strategicworkfl
User Search Filter*	samaccountname=$\USER$
Group Membership	None
Group Base	
Group Search Filter	
Default Group(s)	

Screenshot of the AREA LDAP Configuration form

Configure the AREA HUB to use the SSO Plugin

The BMC AREA Hub allows multiple AREA plugins to be installed within AR System. When using the BMC AREA LDAP plugin, the hub must be enabled and both the JSS AREA plugin and the BMC AREA LDAP plugin must be configured to run with it.

The jss-sso.dll (using the Windows library for demonstration purposes) has to be configured to be the first AREA plugin used within the AREA Hub.

To enable this, please edit the ar.cfg and ensure the following is present in this order:

```
Plugin-Path: c:\path\to\SSOPluginVERSION
Plugin: "c:\path\to\arealdap\areahub.dll"
AREA-Hub-Plugin: "c:\path\to\SSOPluginVERSION\jss-sso.dll"
AREA-Hub-Plugin: "c:\path\to\arealdap\arealdap.dll"
```

Note, both order and case are important.

Alternative Java AREA plugin

The SSO Plugin product has been supplied with a C based AREA plugin for many years because the AR System C based plugin server was proven to be stable. However, the Java based plugin server has now been tested by BMC customers and is becoming more popular. Also, the Java based plugin server is easier to support in less common UNIX environments such as HP UX Itanium.

The Java AREA plugin can be found in the SSO Plugin installation files, within the java-area-plugin directory. To install the Java AREA plugin, follow these steps:

1. Unpack the jss-sso-area.zip file.
2. Locate the AR System server pluginsvr_config.xml file, typically found in the C:\Program Files\BMC Software\ARSystem\pluginsvr directory.
3. Copy the jss-sso-area.jar and jss-workflow.def files to the pluginsvr directory.
4. If the AR System server is running on Windows, copy the jss-sso-area.bat file to the pluginsvr directory.
5. On Windows, run the jss-sso-area.bat file, which will launch a setup tool in a command prompt window.
6. On Unix, run the jss-sso-area.jar file using the following command line syntax:

```
java -jar jss-sso-area.jar
```

7. If upgrading from the C AREA plugin, do not re-import workflow when prompted.
8. Restart the AR System server and test the SSO solution.
9. The Java AREA plugin log file can be used to diagnose problems, or sent to JSS support for analysis.

Enabling AREA plugin logging

The BMC plugin server log files can become very large and it is helpful to separate the SSO Plugin logging. To do this, add the following to the log4j_pluginsvr.xml file:

```
<appender name="SSOPluginLog" class="org.apache.log4j.RollingFileAppender">
  <param name="File" value="c:/jss-area-ssoplugin.log" />
  <param name="MaxFileSize" value="5MB"/>
  <param name="MaxBackupIndex" value="10"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
           value="%d %-5p [%t] %C (%F:%L) - %m%n"/>
  </layout>
</appender>
<logger name="com.javasystemsolutions">
  <!-- Change info to debug or all in order to generate more logging -->
  <level value="info" />
  <appender-ref ref="SSOPluginLog" />
</logger>
```

Enabling Windows User Tool SSO

The Java AREA plugin setup tool does not create the ARSSSOInfo.ini file required to SSO enable the Windows User Tool. The Windows setup.exe tool can be used to create this file when provided with the details of an SSO enabled AR System server.

Manually importing workflow

Some AR System instances struggle to load workflow and this can affect the stability of the setup tool. If the tool fails to import the jss-workflow.def file (located within the zip file) using the BMC Developer Studio tool, and then run the setup tool passing the -DskipImportWorkflow=true JVM parameter. This is included in the jss-sso-area.bat file and is passed on the command line as follows:

```
java -DskipImportWorkflow=true -jar jss-sso-area.jar
```

BMC Premium Encryption

For customers wishing to use the BMC Premium Encryption add-on, an extra manual installation step is required. The SSO library is compiled with the BMC Remedy API version 7.6.04 and therefore needs that version of the BMC Remedy Encryption library. From the 7.6.04 BMC Remedy Encryption installation directory, typically C:\Program Files\BMC Software\PremiumSecurity\PremiumEncryption, copy the file with the following name format of arencrypt7604_build001.[operating system file extension]

Example: Windows operating system, the file to copy is arencrypt7604_build001.dll

This file needs to be copied to the location of our jss-sso[.dll or .so depending on the operating system].

Upgrades

When upgrading SSO Plugin, unless upgrading in a minor release, ie 4.0.0 to 4.0.1, we recommend SSO Plugin is uninstalled. Alternatively, instructions for upgrading in a major release are below.

If using a version prior to 3.6

Ensure the SSO Plugin is disabled on the Mid Tier (through the SSO Plugin status page). Re-install the product from scratch.

If using version 3.6, 4.0

Please check the CHANGES.txt file for upgrade information specific to a minor build. If in doubt:

1. Stop AR System.
2. Replace the AR System JSS AREA Plugin (jss-sso.dll/jss-sso.so). The Windows jss-sso.dll is located in the win32.zip file within the installation files.
   a) On Windows deployments, while not essential to the upgrade, it is useful to rename the SSO Plugin directory in which the AREA plugin resides to reflect the new version, and alter the references to this path in the ar.cfg file.
3. Start AR System.
4. Import the ssoadmin40.def file found in the installer directory. If you are not familiar with how to do this:
   a) Using the BMC AR System Developer Studio, go to the File menu and select import.
   b) Select Object Definition.
   c) Select the AR System server.
   d) Select the ssoadm40.def file.
   e) Select “Replace objects on destination server”, “Delete excess fields” and “Delete excess views”.
   f) Press finish.
5. Go to the SSO Plugin status page (ie http://midtier/arsys/jss-sso/index.jsp), login and disable SSO Plugin on Mid Tier.
6. Stop Tomcat running Mid Tier.
7. Replace the Mid Tier files, ie copy the contents of the midtier directory into the Mid Tier.
8. Delete the Tomcat 'work' directory, which is a temporary cache directory re-created when Tomcat starts.
9. Start Tomcat.
10. Go to the Mid Tier SSO configuration, check it is still correct and press 'set configuration'.

If using version 4.1

When the current release of SSO Plugin is already deployed, ie you have version 4.1.0 installed and you wish to update to version 4.1.1, the following steps should be followed unless the CHANGELOG.txt file states differently:

1. Stop AR System.
2. Replace the AR System JSS AREA Plugin (jss-sso.dll/jss-sso.so). The Windows jss-sso.dll is located in the win32.zip file within the installation files.
3. Start AR System.
4. Stop Tomcat running Mid Tier.
5. Replace the Mid Tier files, ie copy the contents of the midtier directory into the Mid Tier.
6. Delete the Tomcat 'work' directory, which is a temporary cache directory re-created when Tomcat starts.
7. Start Tomcat.

BMC Analytics, Dashboards, ITBM and Jasper Reports.

Copy the relevant jar files from the installation files to the third party application.

For example, copy the jar files in businessobjects/WEB-INF/lib (from the installation files) to the relevant location in the Business Objects installation, as per the original deployment.

Uninstalling SSO Plugin

To uninstall SSO Plugin, follow these steps:

1. Go to the SSO Plugin Mid Tier status page and click the disable Mid Tier button. Mid Tier will require restarting.
2. Delete the files copied from the installation set to the Mid Tier web application directory. If you are going to upgrade SSO Plugin, this can be skipped as the new files will overwrite the old files.
3. Locate the JSS AREA plugin, called jss-sso.so or jss-sso.dll, within the AR System server directory. The file is located in a directory called arplugin.exe.local or SSOPluginVersionNumber – in both cases, the entire directory can be removed.
4. Locate the ar.cfg/conf file in the AR System server directory and remove the line that loads SSO Plugin, ie. Plugin: c:\path\to\jss-sso.dll or AREA-Hub-Plugin: c:\path\to\jss-sso.dll.
5. Remove the JSS workflow (forms, active links and filters) prefixed with JSS.
6. Restart both AR System and Mid Tier.