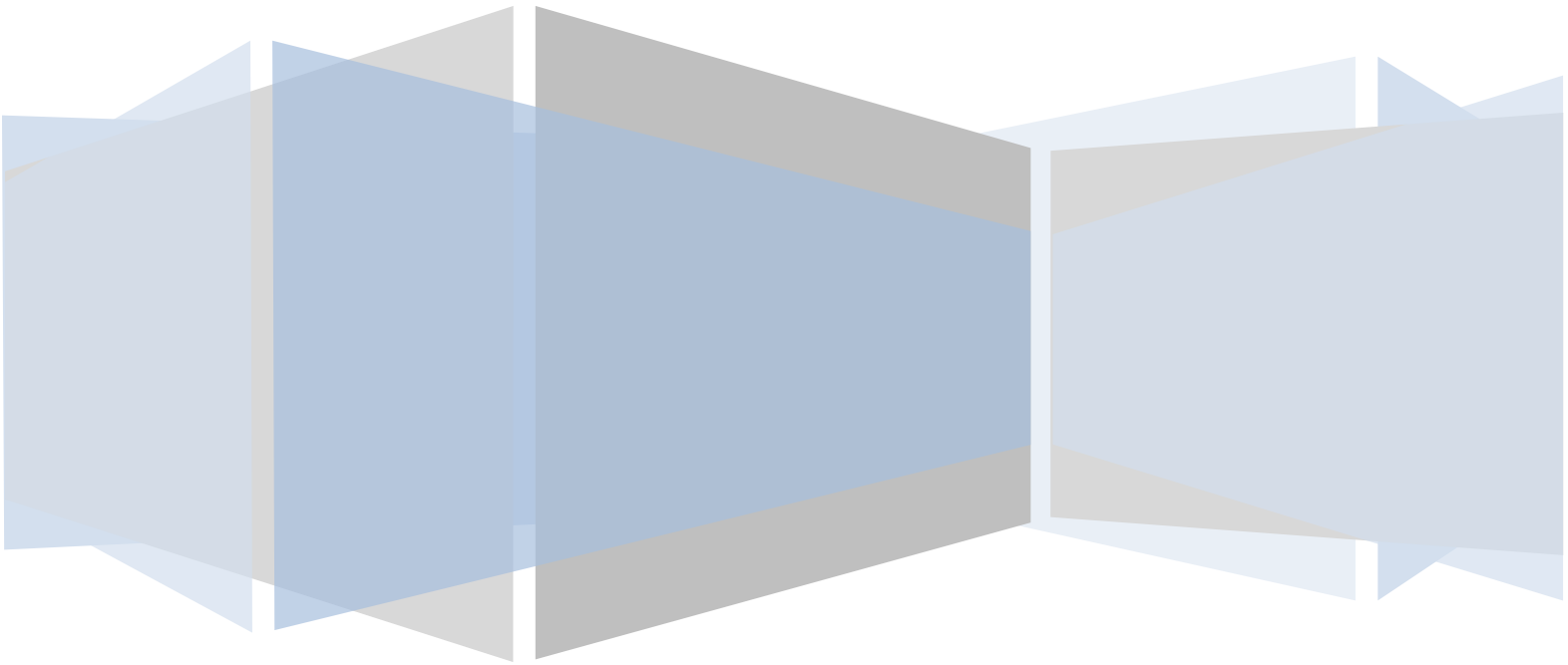
# SSO Plugin

## Installation for BMC AR System


### J System Solutions

**http://www.javasystemsolutions.com**


Version 3.6



# 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

Sun Solaris 5.x

HP-UX 11.x

Linux 2.4.x+

AIX.

## 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+, use the latest version of SSO Plugin.

For ITSM integrations we support version 7.03 to 8.0 including BMC OnDemand.

## Java web servers

We support Tomcat 5.5.23+, Weblogic 9.2.3+ and Websphere for the Mid Tier, running under a Java 1.6+ or 1.7.0_04+ Virtual Machine. Please use the latest version of the 1.6 JVM, ie 1.6.0_31, 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

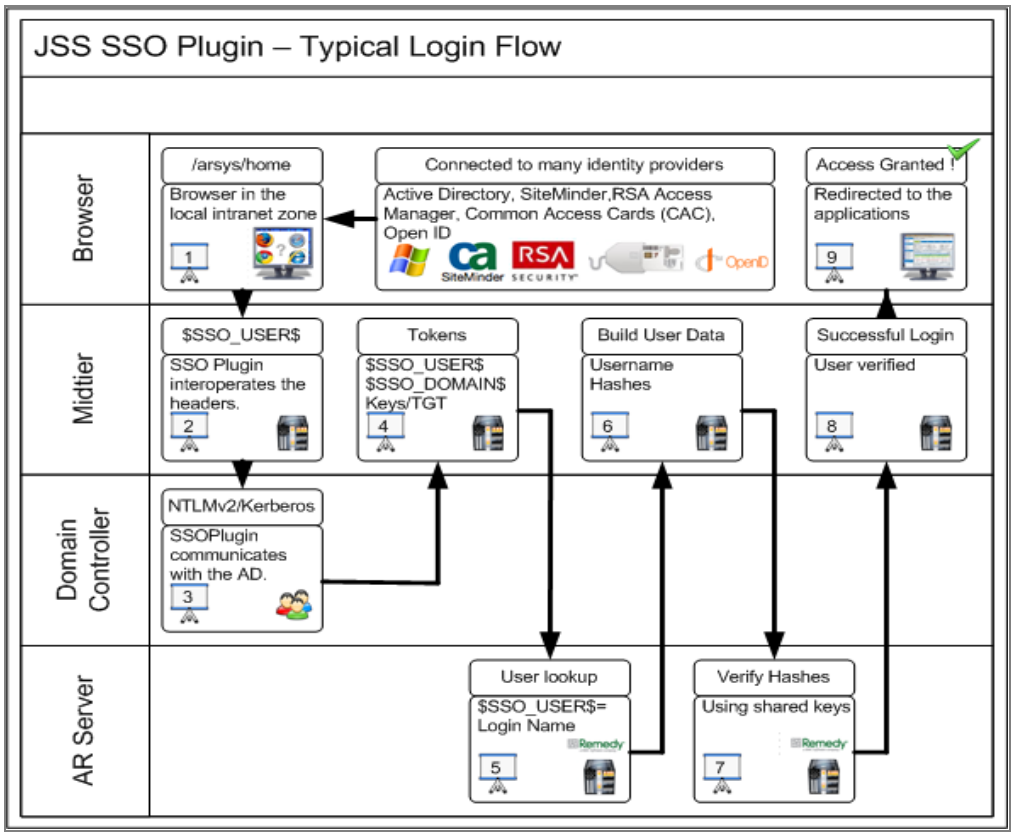
It is not recommended to mix versions of SSO Plugin within your infrastructure.

However, if there is a requirement to run mixed versions, the following guidelines may be useful:

- Mid Tier with SSO Plugin 3.0-3.2 will work with AR System server running SSO Plugin 3.0-3.2.
- Mid Tier with SSO Plugin 3.3+ will work with AR System server running SSO Plugin 3.3+.
- You can not run AR System server running SSO Plugin 3.3-3.5 with a Mid Tier running a version of SSO Plugin prior to 3.3.
- SSO Plugin 3.6 must be run with an AR System server running SSO Plugin 3.6.

# 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"
```

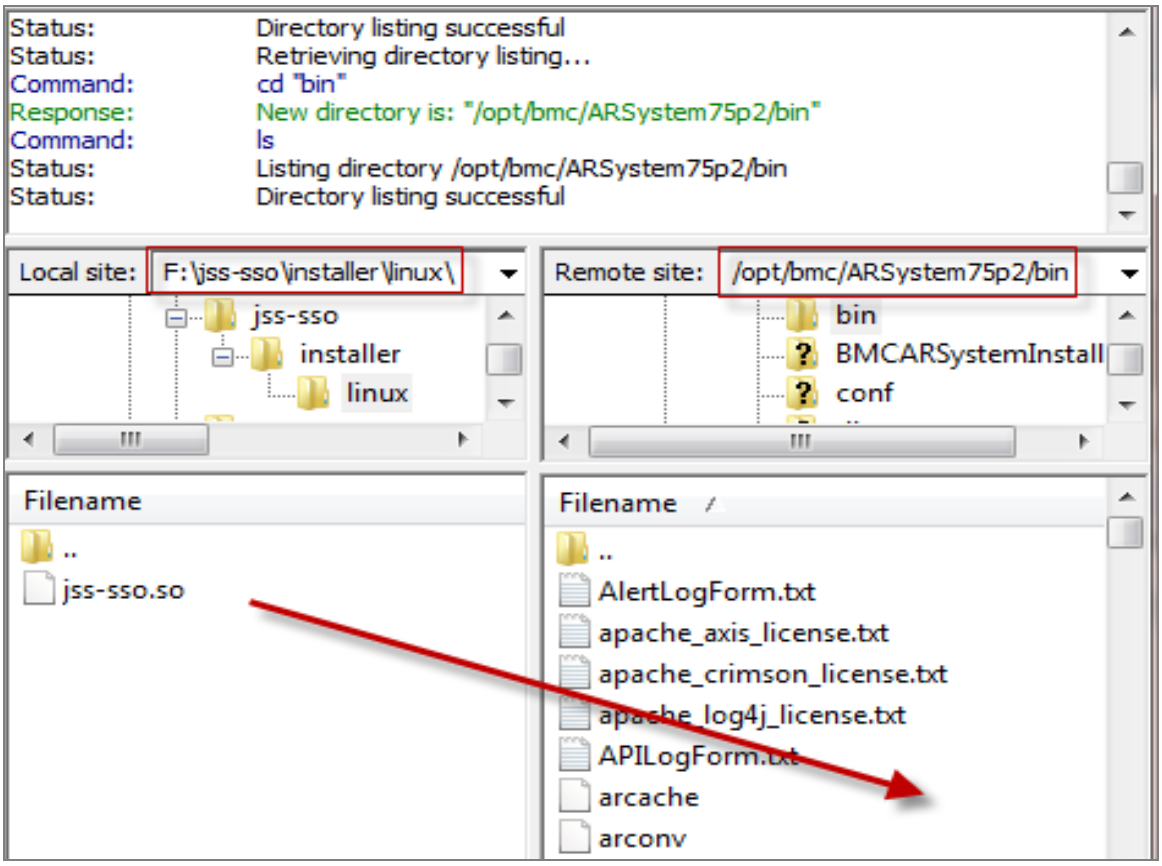
One final prerequisite is that you will need to copy file(s) to the AR System servers. So you will need operating system access.

## 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:




## 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).

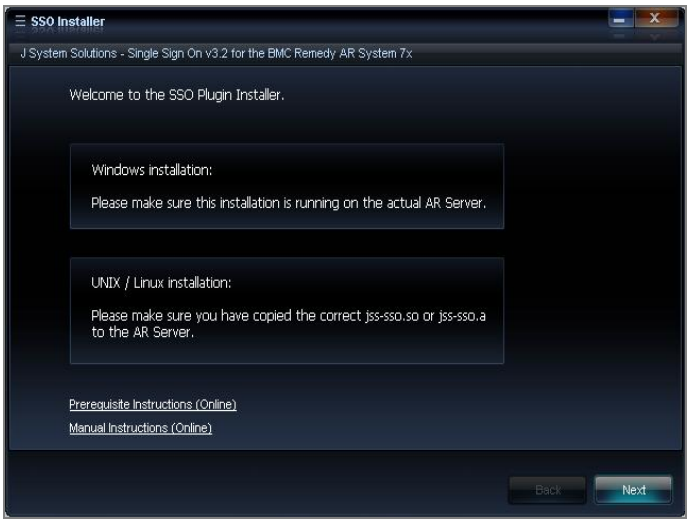
This is required to be set as the Plugin-Path in the ar.cfg file and is described later.

## 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.

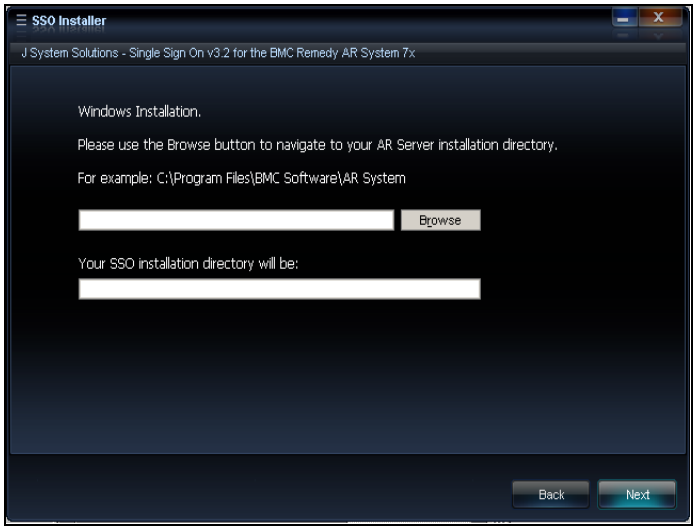
Below is a screenshot of the welcome page reminding you that if this is a Windows install to make sure this is running on the actual machine running AR System server or on UNIX or Linux, it's reminding you to place the correct file(s) on the AR System server.



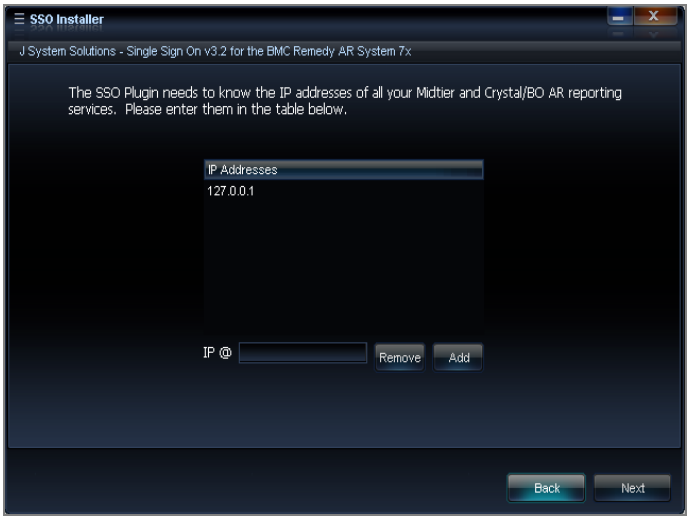

Once you have verified the above, tick the box and click Next

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.


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.



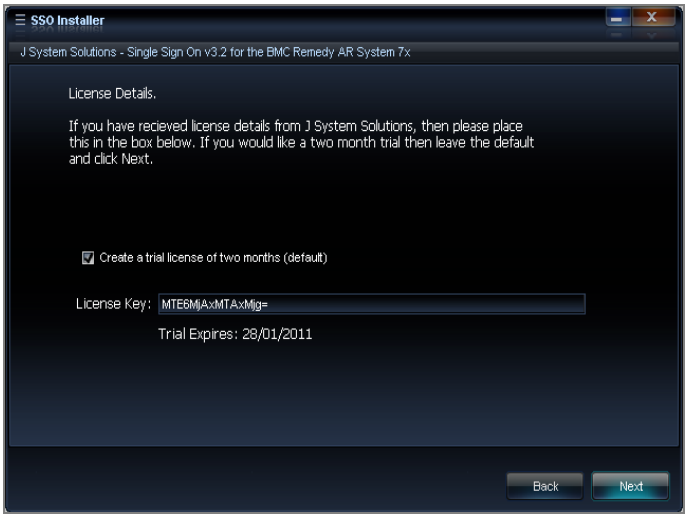
Make sure you enter all IP addresses of all Mid Tier servers and any Crystal Reports Server or Business Objects Reporting Servers, including the addresses of any load balancers.



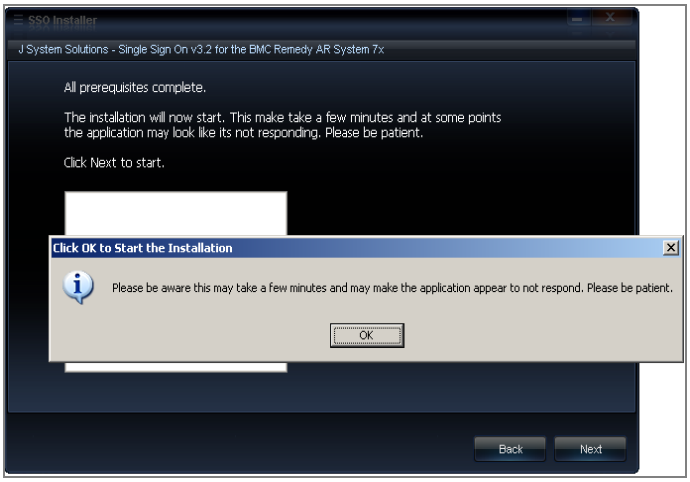
The following screen shows a configuration option for the JSS SSO Plugin for the Windows User Tool. The Microsoft Security API (SSPI) can present the user information in a number of salutations for the user name. E.g. Capitalisation etc. Like many customers, you may have your login names in lower case. The case must match whatever you login name is within the AR System. E.g. **Bob** is not the same user as **bob**. So this option allows the Plugin to manipulate the user name before being sent to the AR System server for authentication. The following options are:

- Use format delivered by SSPI
    - However the user name is stored in Active Directory, is how it will be sent to the AR System server
- Force lower case (default)
    - Modifies the whole user name to lower case
- Force upper case
    - Modifies the whole user name to upper case
- Capitalise the first letter
    - Changes bob to Bob

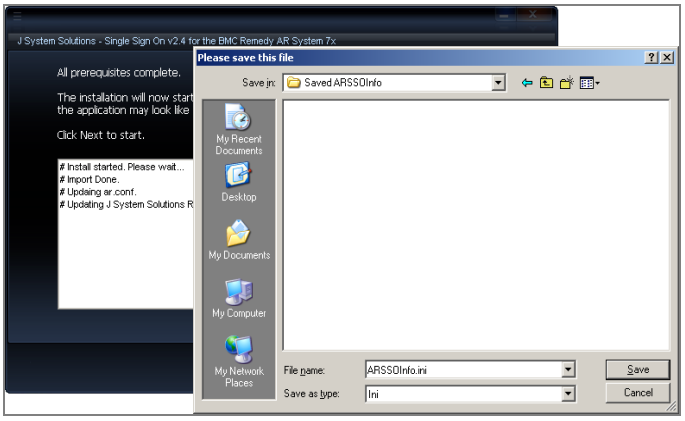
This screen allows you to install a two month trial license by ticking the check box, or if you have received a site license from JSS then deselect the box and place your code where it says License Key.



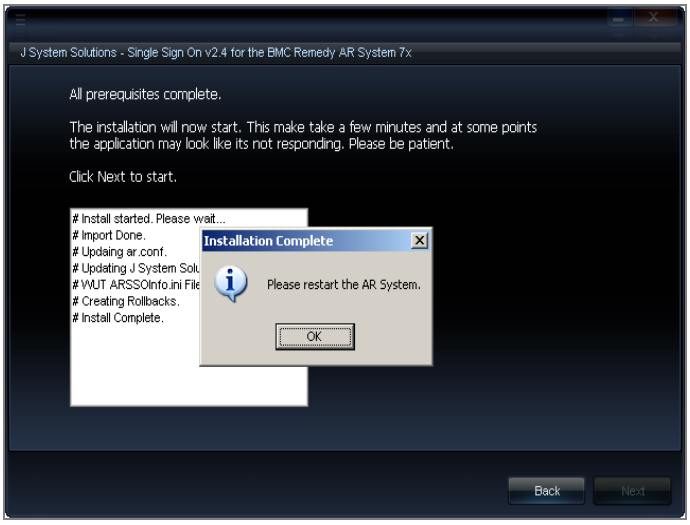

Now all prerequisites are complete, we are ready to start the installation. A warning is presented to remind the administrator that this may take some time depending on the AR System server performance. At times the installation may look unresponsive but please be patient. Updates will appear within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



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.




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

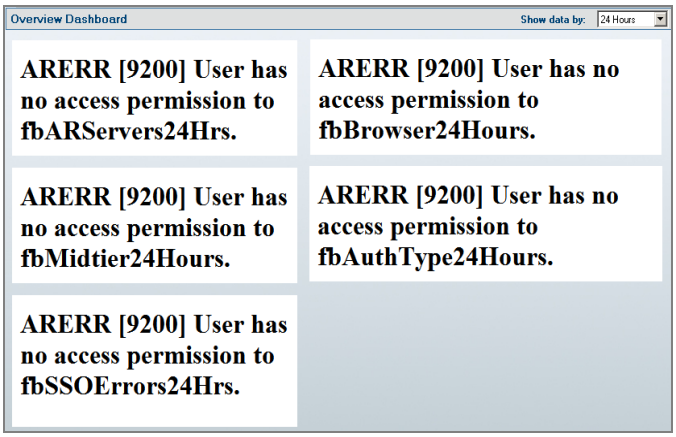



Installation of the AREA plugin is complete. You can now progress to install the Mid Tier plugin.

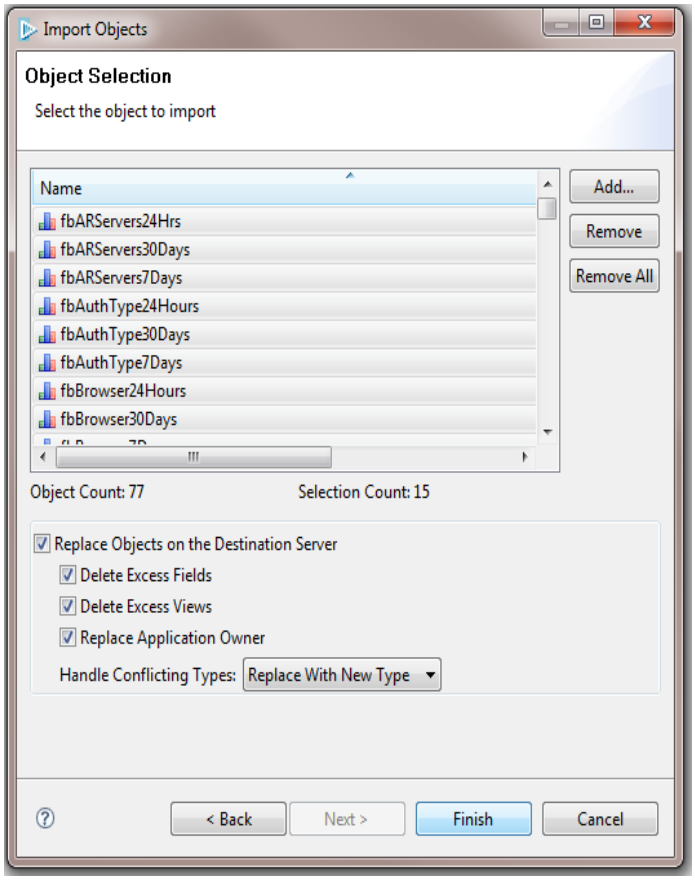
## Flashboards

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.




Using the BMC Developer Studio, import the Flashboards manually:



## 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.

## Load balancers and proxies

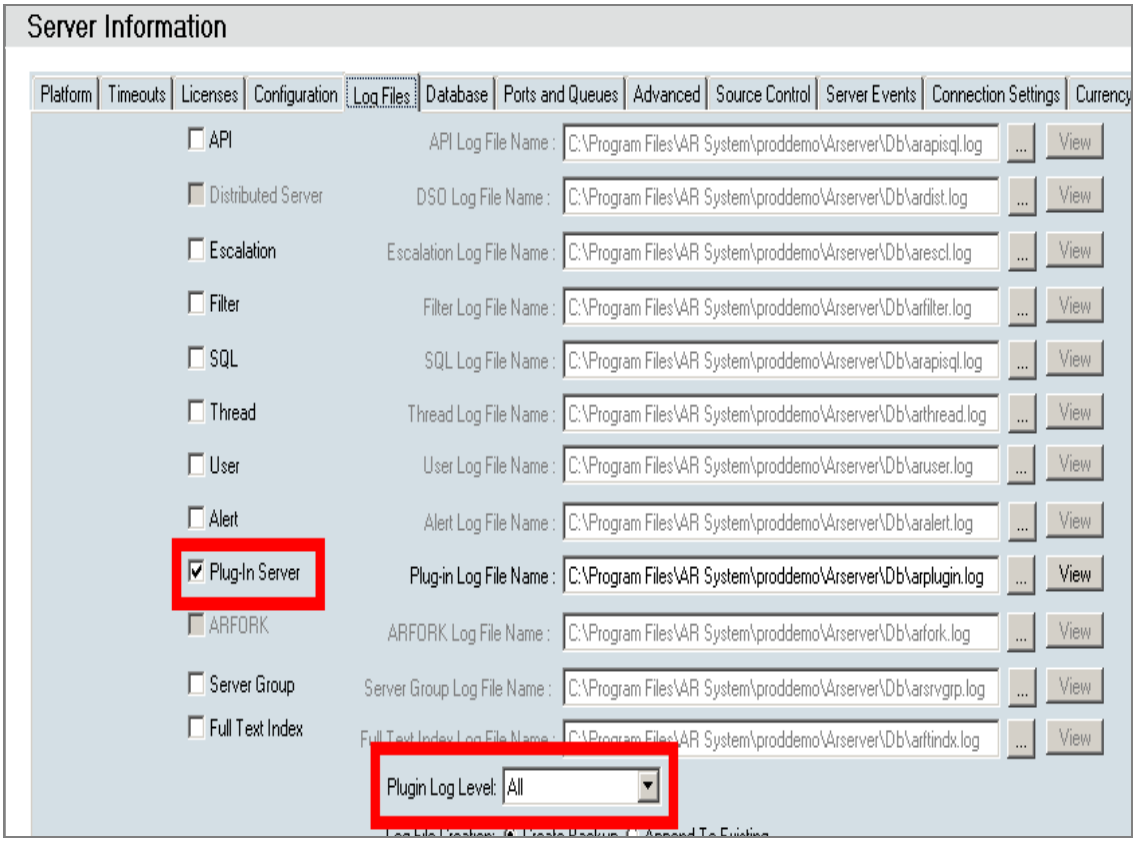
Ensure that the Mid Tier IP address you enter is the correct address if you're using a load balancer, proxy, etc. If you're unsure then ask your network administrators, and if in doubt, add all the relevant IP addresses!

## 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.

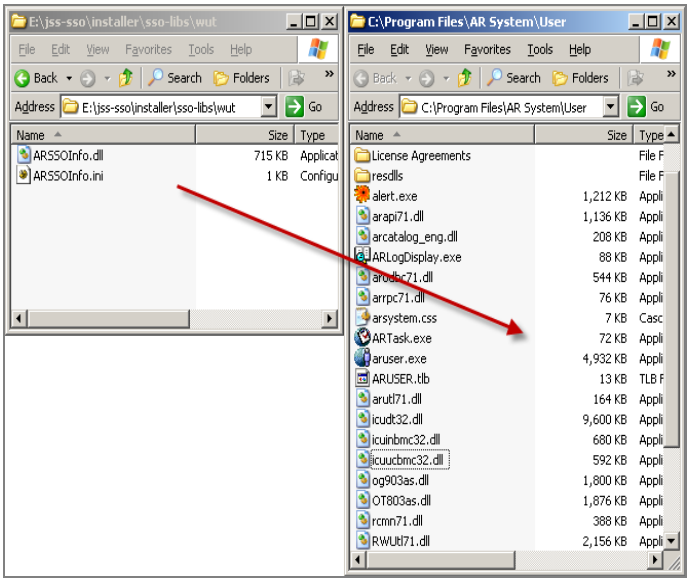
Login to AR System using the BMC Windows User Tool with an administrative user. Open the AR System Administration Console and click on System and then General.

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



# 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.




## 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.

**newsharedkey:** 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. Restart Mid Tier.
3. 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+.
4. 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.
5. Locate the document titled Configuring Mid Tier and Web Tier to configure the SSO Plugin.
6. 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.
7. If SSO fails then review the troubleshooting document or contact JSS support.

## Replacing the BMC Mid Tier login page

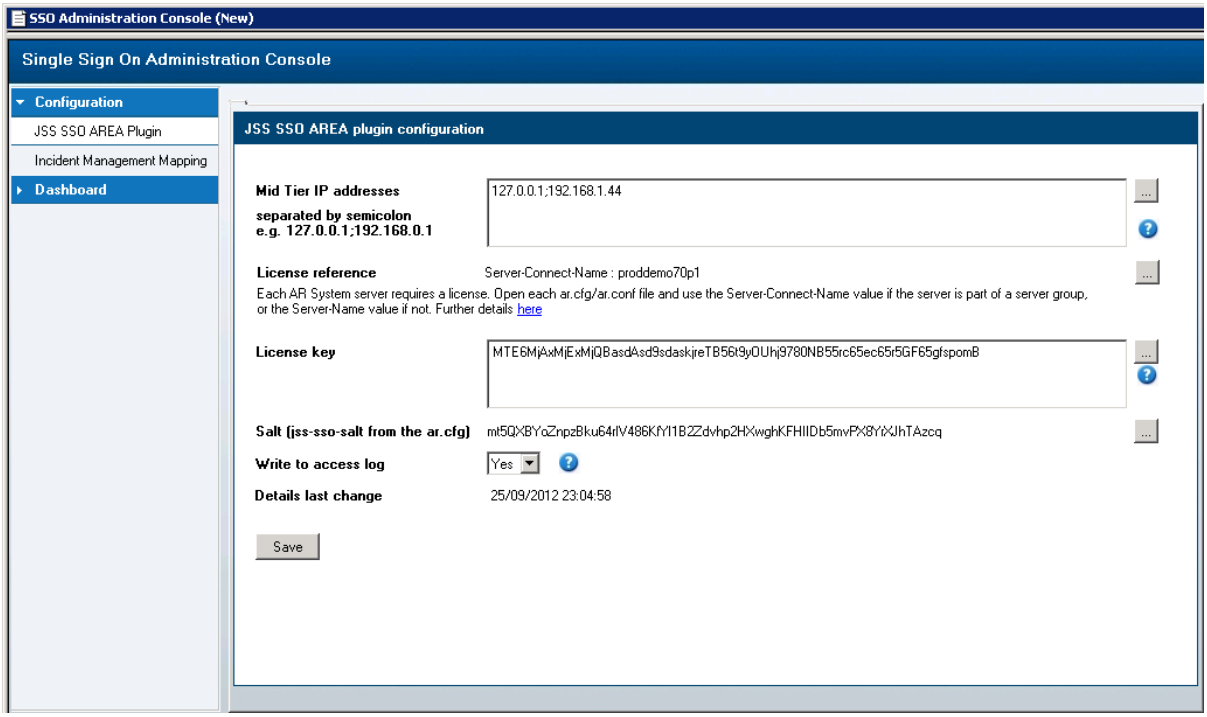
It is common to find users bookmark the BMC login page, ie /arsys/shared/login.jsp. This results in support enquiries as SSO will not be activated when this page is requested by users.

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 the builtin-login.jsp page in the SSO Plugin installation files, under the midtier/jss-sso directory.
2. Locate existing Mid Tier login.jsp page under the Mid Tier shared directory.
3. Rename the existing login.jsp to login.jsp.old.
4. Copy the builtin-login.jsp page to the location of the existing login page, renaming to login.jsp, ie copy [ssoplugin-installation]/midtier/jss-sso/builtin-login.jsp [midtier]/shared/login.jsp.

# SSO Administration Console

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




The console allows the administrator to configure the JSS AREA Plugin by supplying a list of trusted Mid Tier IP addresses, the license (populated with a default date restricted license during installation), and other information useful for debugging the product.

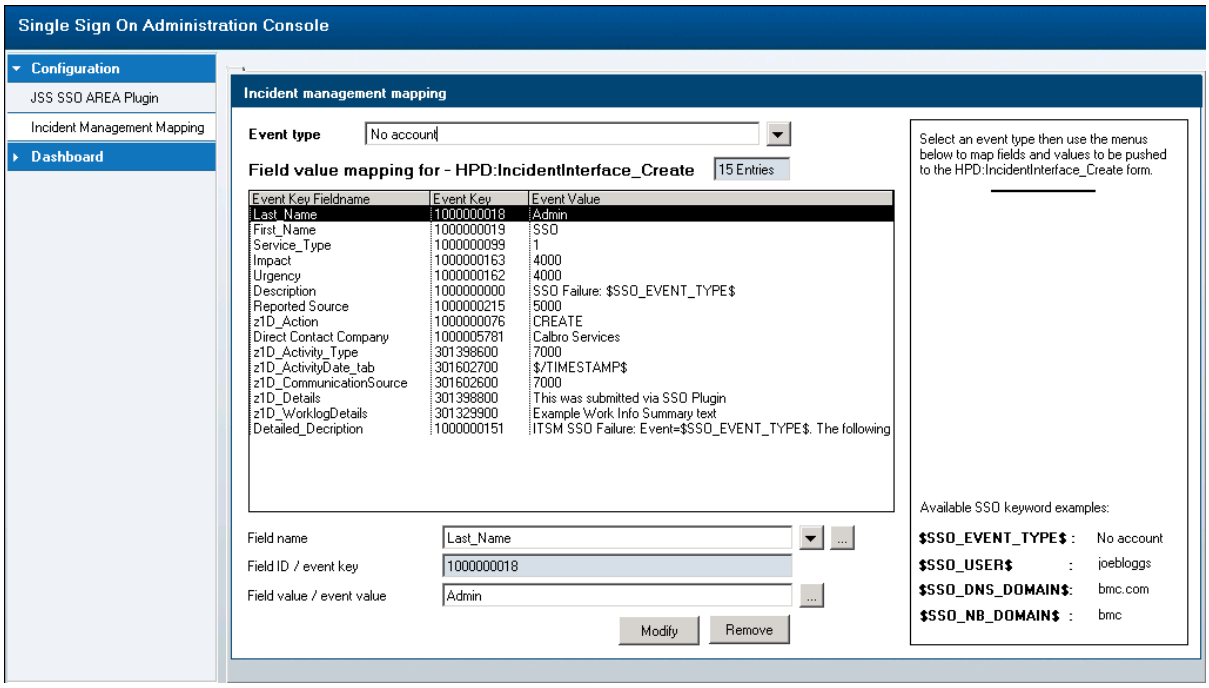
When an update is made to the SSO Administration Console and the server is part of an AR Server Group, connect to each server in the group, go to the console and press save. This will cause each JSS AREA plugin to reload its configuration.

## 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.

# 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:




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

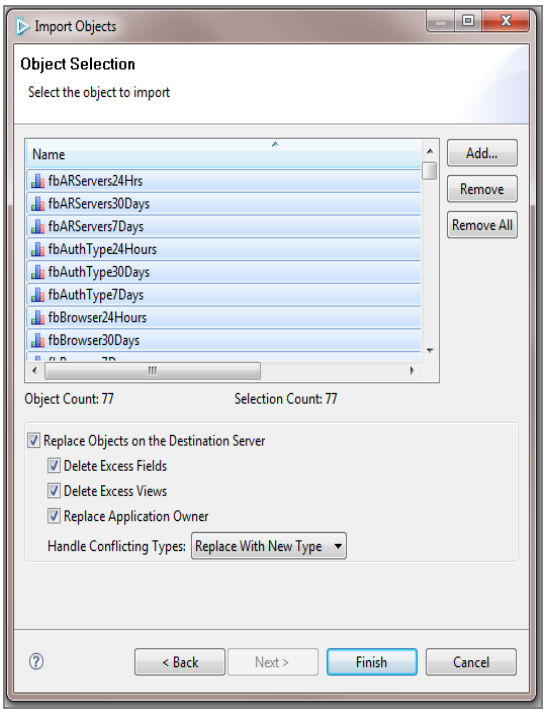
If for any reason the installation program fails. As always, you can contact JSS support. However, you can manually install the product with the following steps.

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 ssoadm30.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.




## Updating repository details

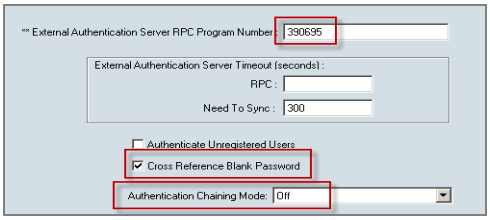
Locate the SSO Administration Console and configure the plugin by supplying the Mid Tier IP addresses.

## 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.



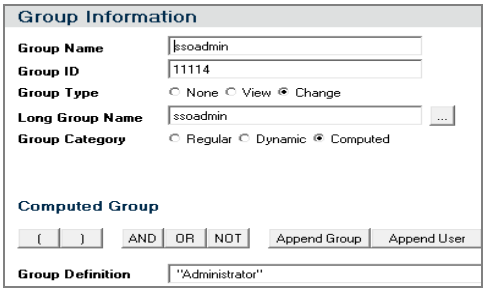

## Disable 'Allow Guest Users'

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

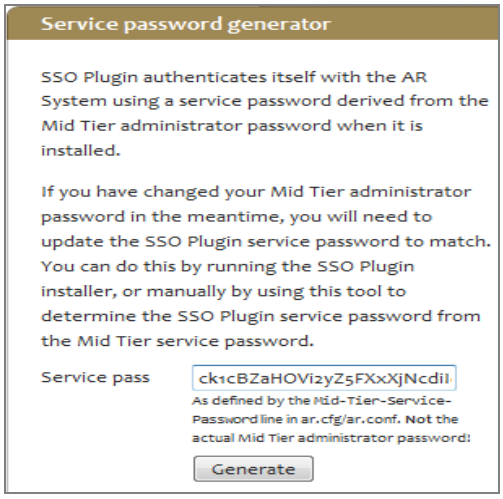
The sso plugin needs to communicate with the AR System server. This is done through a specific user called ssoadmin. The password is generated and is system dependant.

Create a group with the following attributes:




Login to the JSS Support website through this URL

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

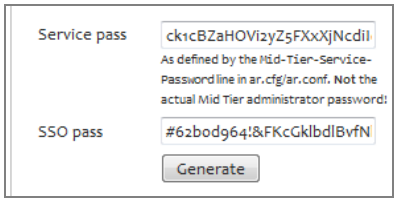



Place the text from the jss-ss-salt in the ar.cfg/ar.conf entry into the **Service pass** field and click **Generate**.

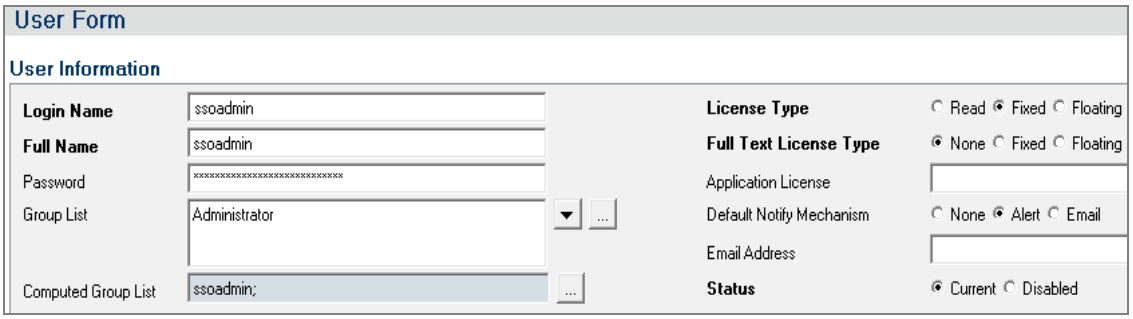
Example: If you see this in your ar.conf then copy everything after the colon.

jss-sso-salt: **asd9asda2313sd0as0dualpq78w4as09eqweas0uas0qwe7aswas09da**

After clicking Generate, you should see the SSO password.




Create a user with the following attributes

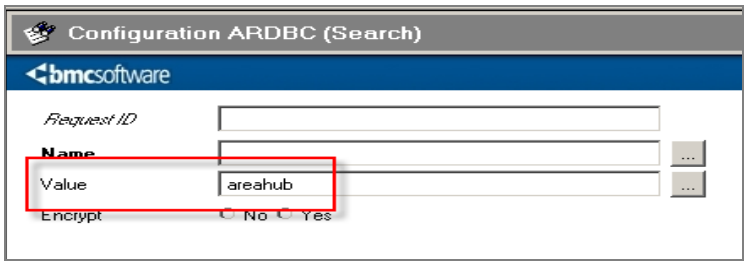



## Check the AREA Hub is installed and configured.

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.

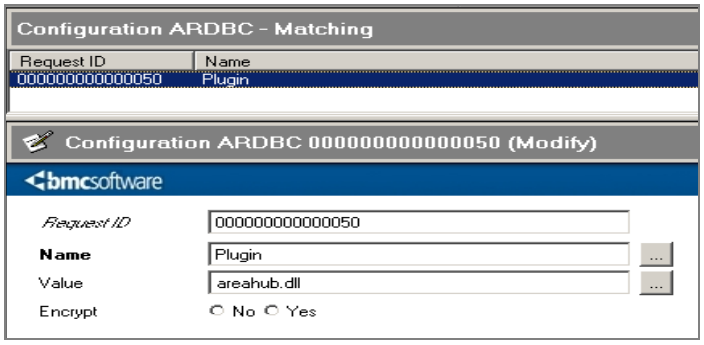
To check this is configured, you can either look directly at the ar.conf / ar.cfg file or you can use the AR System User Tool.

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




**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




**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

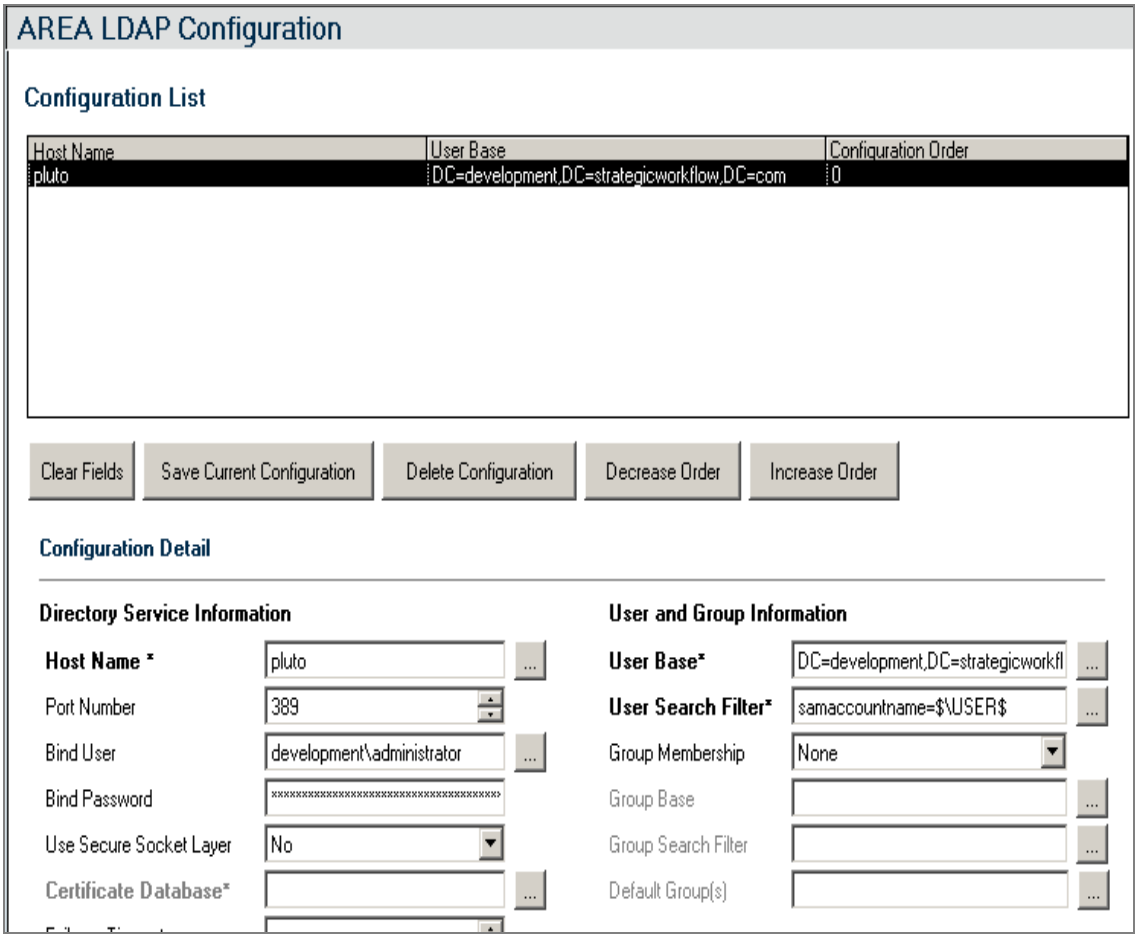
Only follow this section if you are using an LDAP or Active Directory to store your user information. Alternatively, if you are just using the AR Systems USER table to verify then skip to Configure the AREA HUB to Use the JSS SSO Plugin.

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.




**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.

# BMC Mid Tier and timezones

The user's timezone is submitted through the normal BMC login page, and this will not work when going directly to /arsys/home. Unfortunately, the SSO functionality provided by BMC does not recognise that users will be using SSO and require the correct timezone.

To work around this, a JSP file has been provided by JSS to correctly set the timezone. This will require users to access the following link in order to gain access to /arsys/home:

http://host/arsys/jss-sso/home-timezone.jsp

This file can be renamed if necessary.

If you want users to automatically access Mid Tier with the timezone fix, edit the Mid Tier web.xml file and replace <welcome-file>/home<welcome-file> with <welcome-file>/jss-sso/home-timezone.jsp</welcome-file>.

# Upgrades

When upgrading SSO Plugin, unless upgrading in a minor release, ie 3.5.2 to 3.5.12, we recommend SSO Plugin is uninstalled. Alternatively, instructions for upgrading in a major release are below.

## If using a version prior to 3.3

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 3.3, 3.4, 3.5

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).
   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 ssoadmin30.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 ssoadm30.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.
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'.

## 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.