

SSO Plugin

Installation for BMC AR System and WUT

J System Solutions

<http://www.javasystemsolutions.com>

Version 3.4

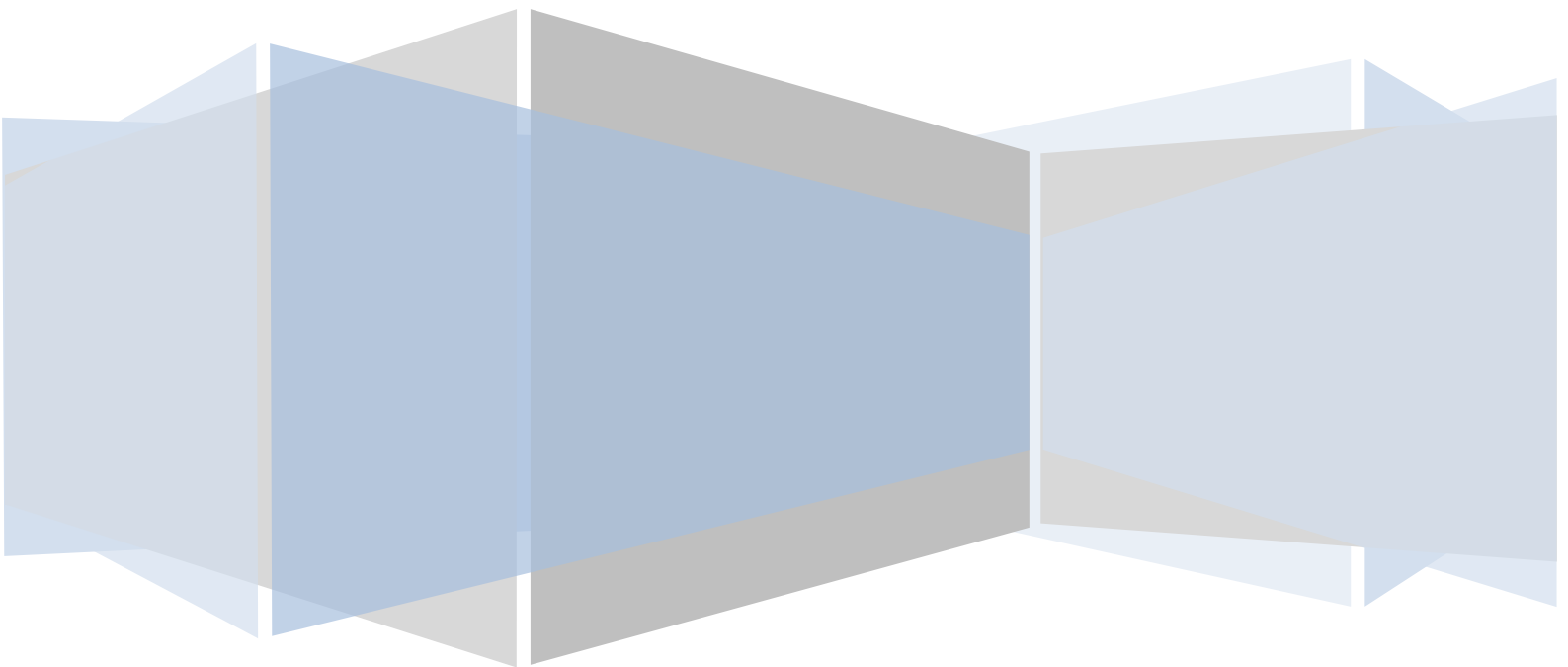


Table of Contents

Introduction.....	4
Compatibility.....	5
Mixing versions of SSO Plugin.....	5
Overview of the SSO Plugin.....	6
Extensions to AR System authentication.....	6
Installation.....	7
Configuring the AR System.....	7
Copy files to your AR System.....	7
Unix.....	7
Manually copying the Windows files (server groups).....	8
Using the SSO AREA plugin installer.....	8
Flashboards.....	18
Server groups.....	19
Load balancers and proxies.....	19
Enable logging for verification.....	19
SSO for the Windows User Tool.....	21
Explanation of the ARSSOInfo.ini file.....	21
General Section.....	21
ARServer section.....	21
Mapping Windows accounts to AR System login names.....	22
Recreating a lost ARSSOInfo.ini.....	22
Manually configuring the AR System.....	24
Import workflow.....	24
Updating repository details.....	25
Check AR External Authentication (AREA) is enabled.....	25
Disable 'Allow Guest Users'.....	26
Creating the ssoadmin account.....	26
Check the AREA Hub is installed and configured.....	27
Windows User Tool SSO - ARSSOInfo.dll.....	29
Copying the JSS AREA plugin to the AR System.....	29
Check the AREA LDAP configuration.....	29
Configure the AREA HUB to use the SSO Plugin.....	30
Upgrades.....	31
If using a version prior to 3.0.....	31
If using version 3.0, 3.1 or 3.2.....	31
If using version 3.3.....	31

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 Midtier, Dashboards).

The JSS support website can be found here:

<http://www.javasystemsolutions.com/jss/support>

Compatibility

The following tables present the supported product versions. If there is a separate product needed that it not displayed, please feel free to contact support.

Operating System				
Windows 2000, 2003, 2008	Sun Solaris 5.x	HP-UX 11.x	Linux 2.4.x+	AIX

BMC Action Request System			
6.3/7.0 (see 2)	7.1 (MT patch 6+)	7.5 (MT patch 1+)	7.6.03/4

Please note:

1. We support Tomcat 5.5.23+, Weblogic 9.2.3+ and Websphere for the Midtier. If you use another Java servlet engine, please contact us to confirm supportability.
2. If you require support for Midtier 6.3 or 7.0 then please contact us. The standard 3.2 build does not contain support for these two Midtier versions as there is little demand, but we are happy to supply a build of 3.2 with support if required.

The SSO Plugin will support many different URL protection products and methods. Popular products include:

Authentication Systems						
RSA Access Manager (ClearTrust)	SiteMinder	Quest QSJ	HTTP Basic	Novell Access Manager	OpenID	X509 client certificates

The SSO Plugin also provides a full Integrated Windows Authentication implementation (ie Kerberos and NTLMv2) out of the box.

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:

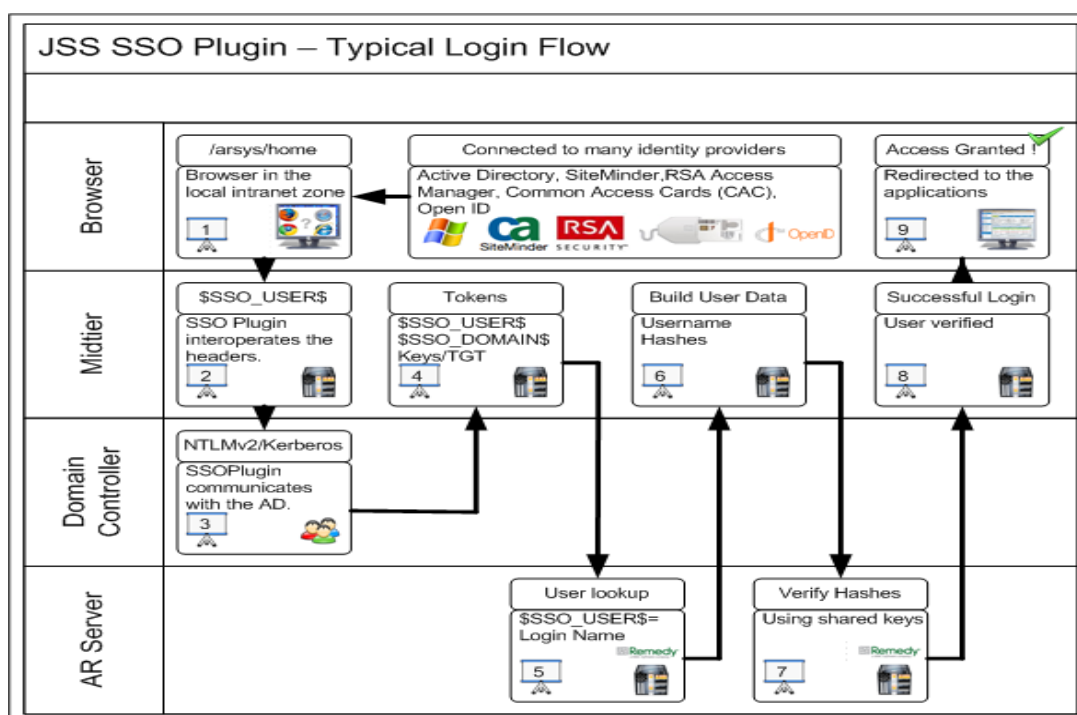
- Midtier with SSO Plugin 3.0-3.2 will work with AR System server running SSO Plugin 3.0-3.2.
- Midtier with SSO Plugin 3.3+ will work with AR System server running SSO Plugin 3.3+.
- You can not run AR System server running SSO Plugin 3.3+ with a Midtier running a version of SSO Plugin prior to 3.3.

Overview of the SSO Plugin

The SSO Plugin is invoked by the Midtier 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 Midtier, which in turn calls the AR System.

Assuming the JSS AREA plugin does not reject the connection - Midtier 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!

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 Midtier component does not, so you can disable AR System accounts by using this setting for all authentications passing through an SSO enabled Midtier.

Installation

The installation zip file contains two directories, mt and area-installer. The mt directory contains the files required by the Midtier, and the area-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 Midtier. The AR System is configured (and tested) before the Midtier 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 Server you are installing initially must have the Administrator thread. If you are installing to one AR Server then this is not an issue. If you are installing to an AR 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 current version of the product needs to communicate back to the AR 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. Thus 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: ardbcconf.dll
```

Solaris/Linux

```
Plugin: ardbcconf.so
```

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

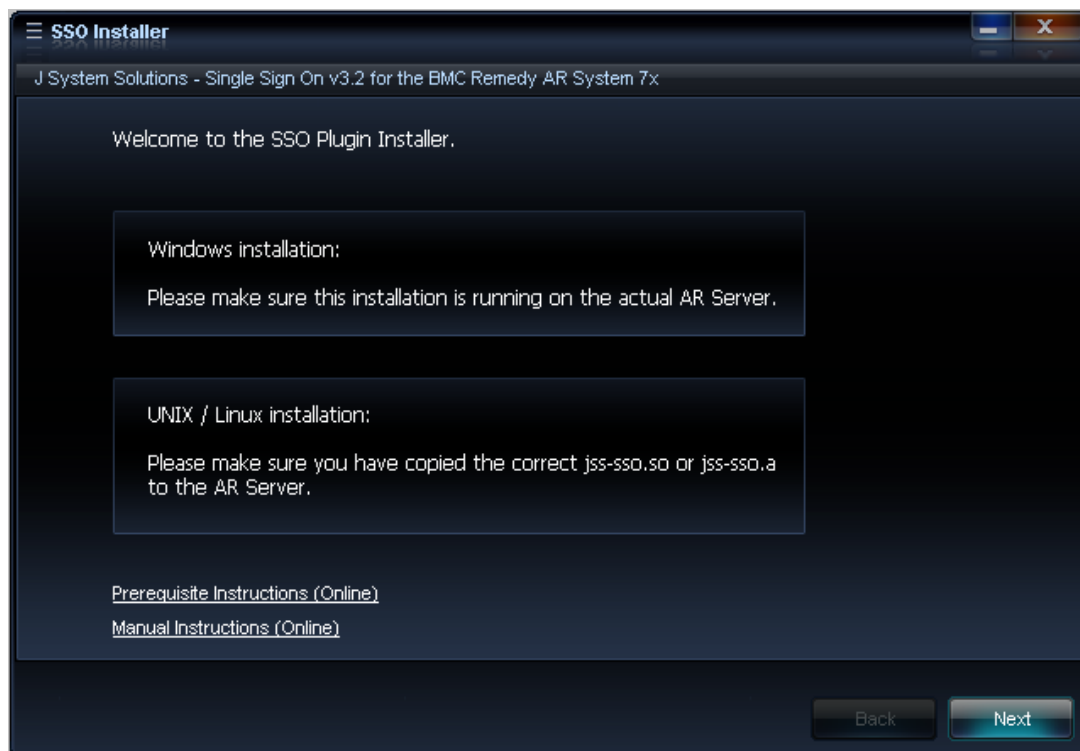
Copy files to your AR System

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 <http://filezilla-project.org/>. The relevant operating system file (Linux, Solaris, HP) needs to be copied to the AR Servers bin directory as seen in the following screenshot:

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 Server or on UNIX or Linux, its reminding you to place the correct file(s) on the AR Server. **Click Next.**



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

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



The screenshot shows a window titled "SSO Installer" with a subtitle "J System Solutions - Single Sign On v3.2 for the BMC Remedy AR System 7x". The window contains the following text and input fields:

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:

Password:

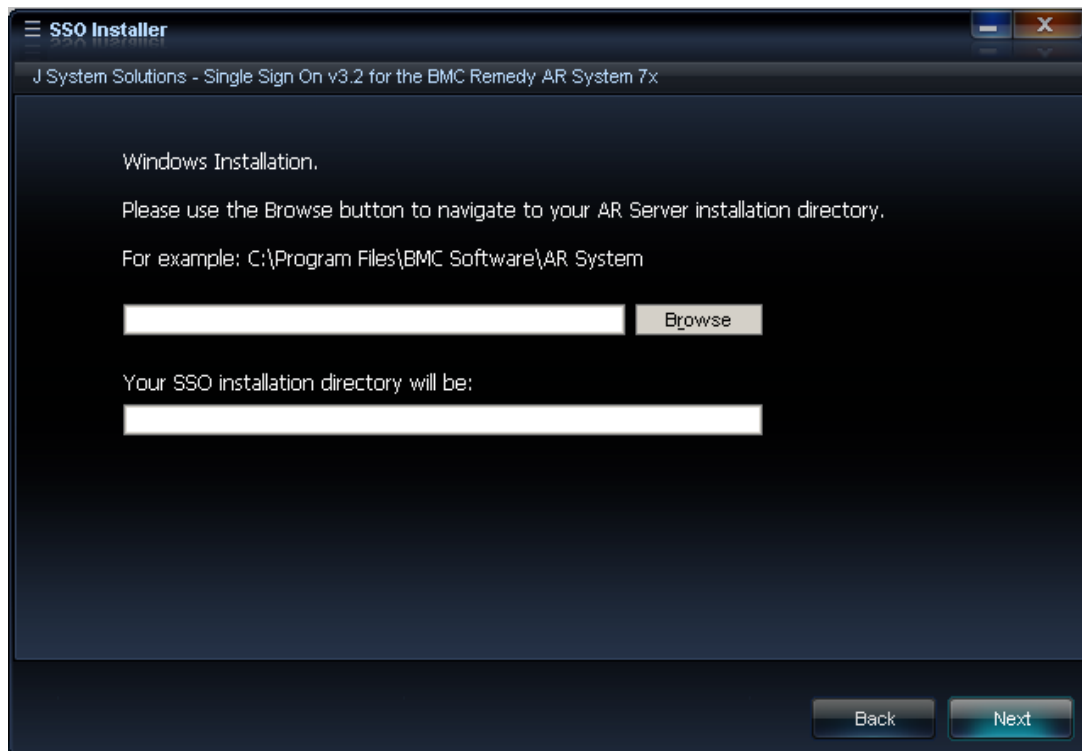
AR Server:

TCP Port:

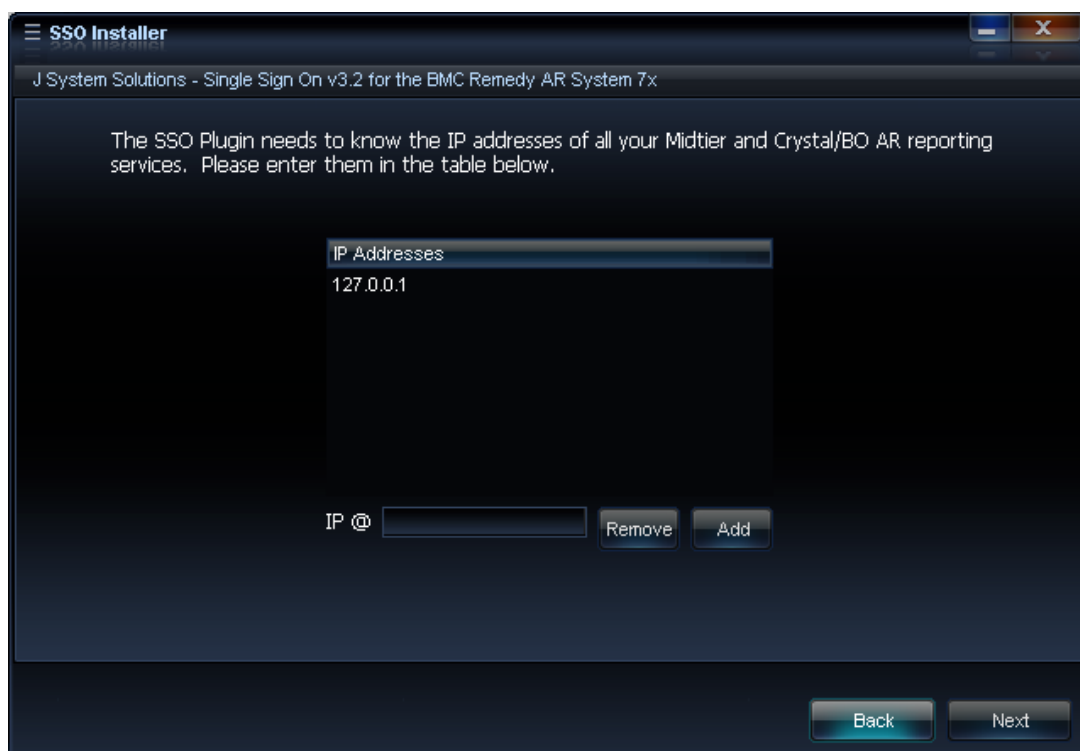
At the bottom right, there are two buttons: "Back" and "Next".

Click Next.

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. Examples on the screen.



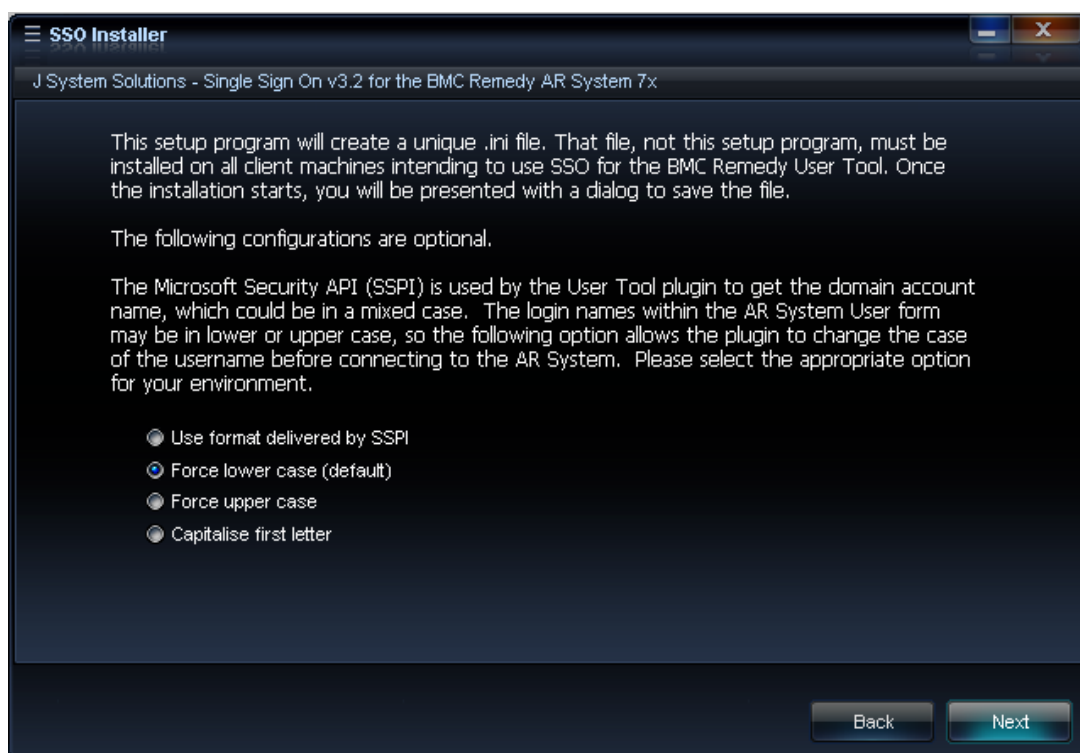
Make sure you enter all IP addresses of all Midtier servers and any Crystal Reports Server or Business Objects Reporting Servers, including the addresses of any load balancers.



Click Next.

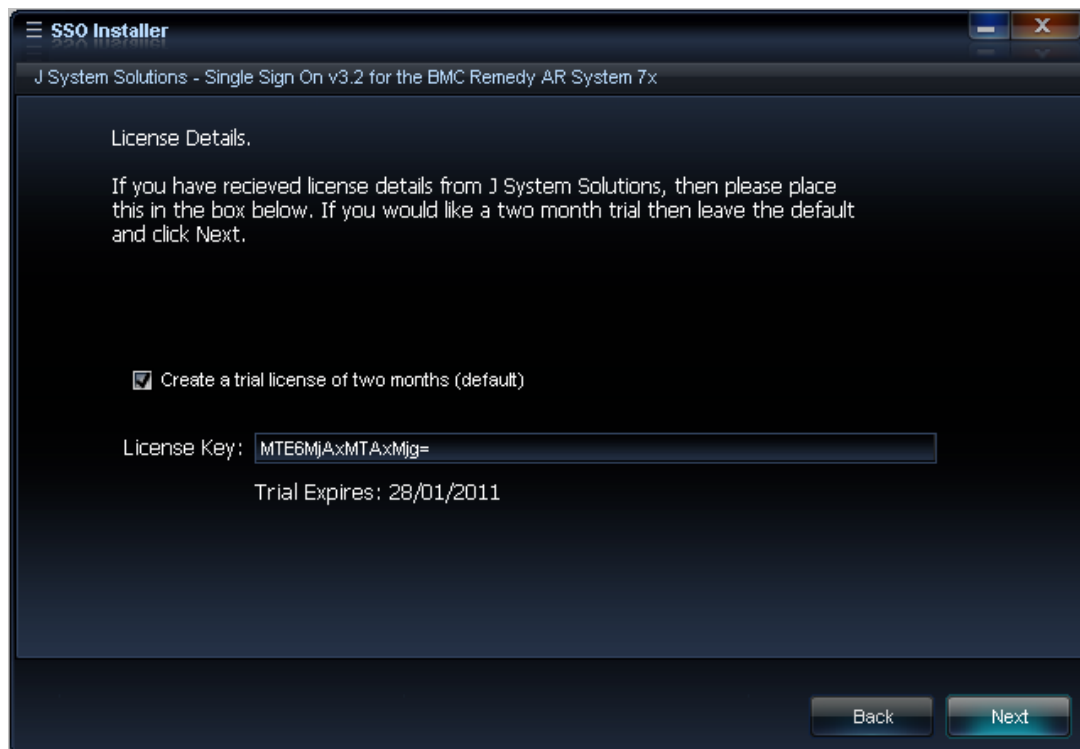
The following screen shows a configuration option for the JSS SSO Plugin for the Windows User Tool. The Microsoft Security API (SSPI) can present the user information in a number of salutations for the user name. E.g. Capitalisation etc. Like many customers, you may have your login names in lower case. 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 Server for authentication. The following options are:

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



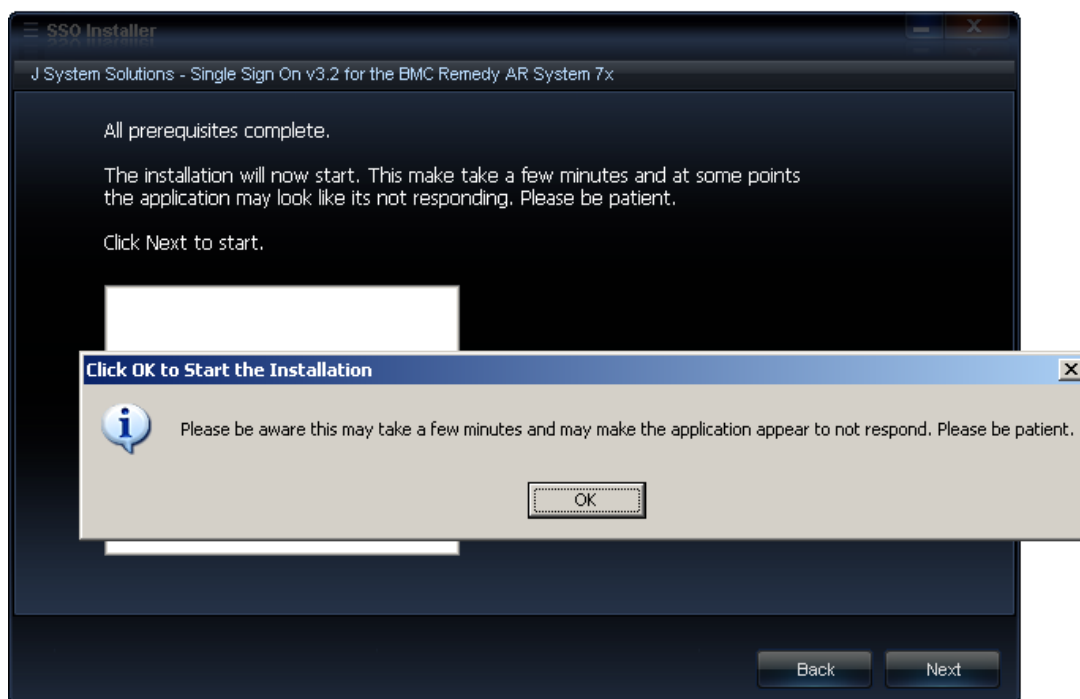
Click Next

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.



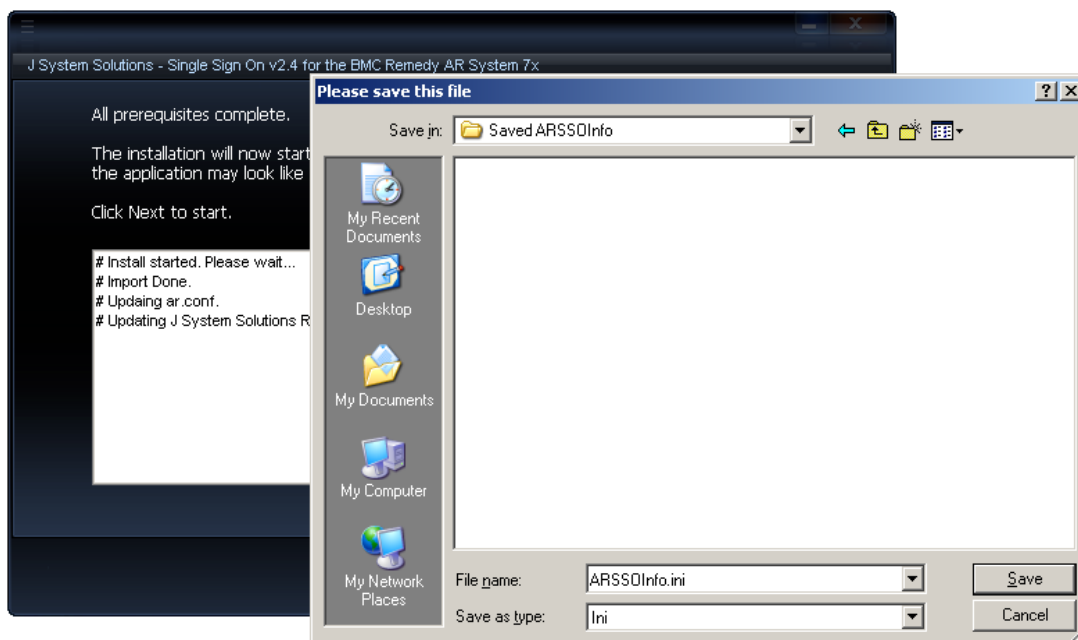
Click Next

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 Systems performance. At times the installation may look unresponsive but please be patient. Updates will appear within the white box.

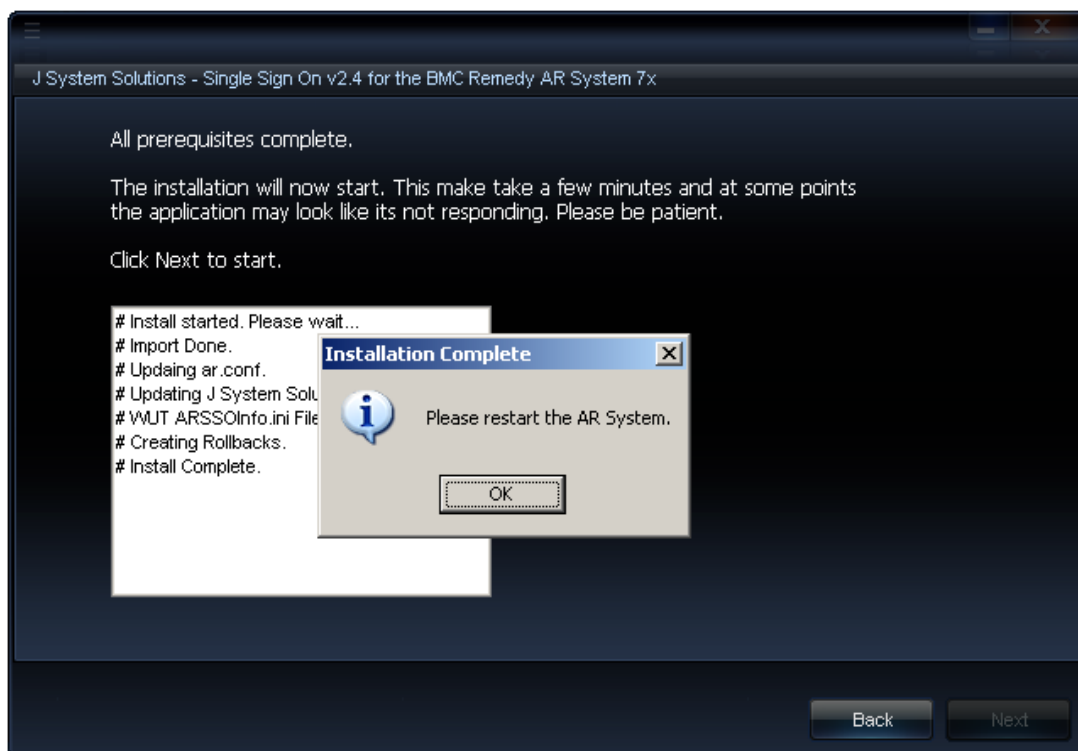


Click Next

After some time 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**.



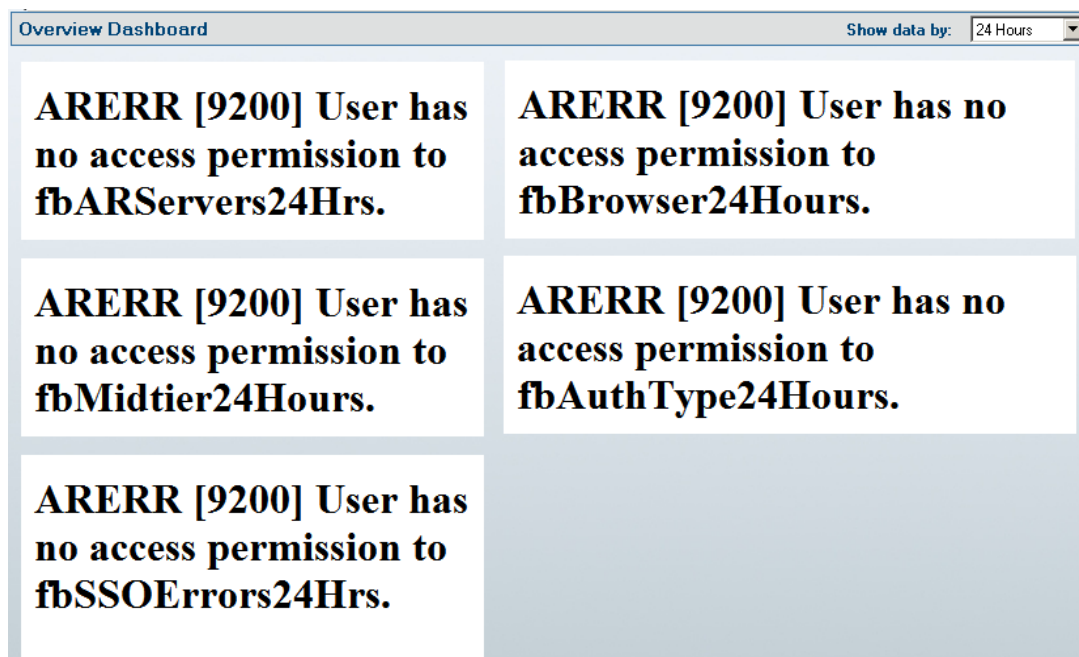
Installation of the AREA plugin is complete. Click Exit.

You can now progress to install the Midtier plugin.

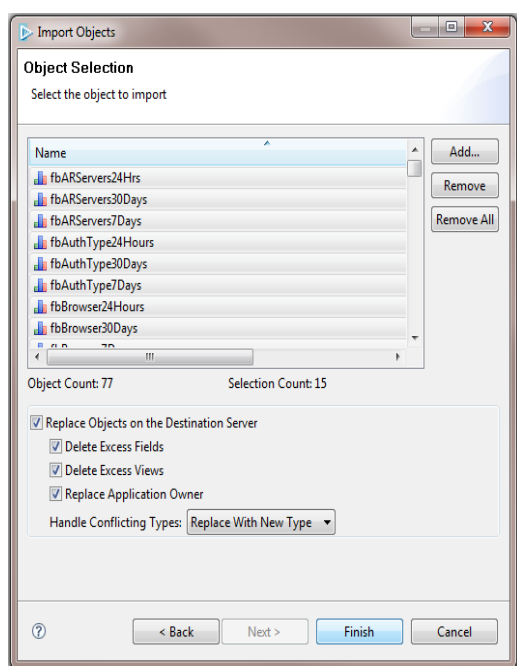
Flashboards

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 (J System Solutions Repository) within AR System. Therefore, when using AR System server groups, the installation steps are as follows:

1. Run the installer against the AR 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.
2. Make sure you follow the same steps as [Copy files to your AR System](#) on the remaining AR Servers in the server group
3. 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 Server with the **administrator** thread and copy the jss-sso-salt entry.
4. 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\SSOPluginXX (where XX is version)
Plugin: 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
```

5. Restart the AR System servers.

Load balancers and proxies

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

Server Information

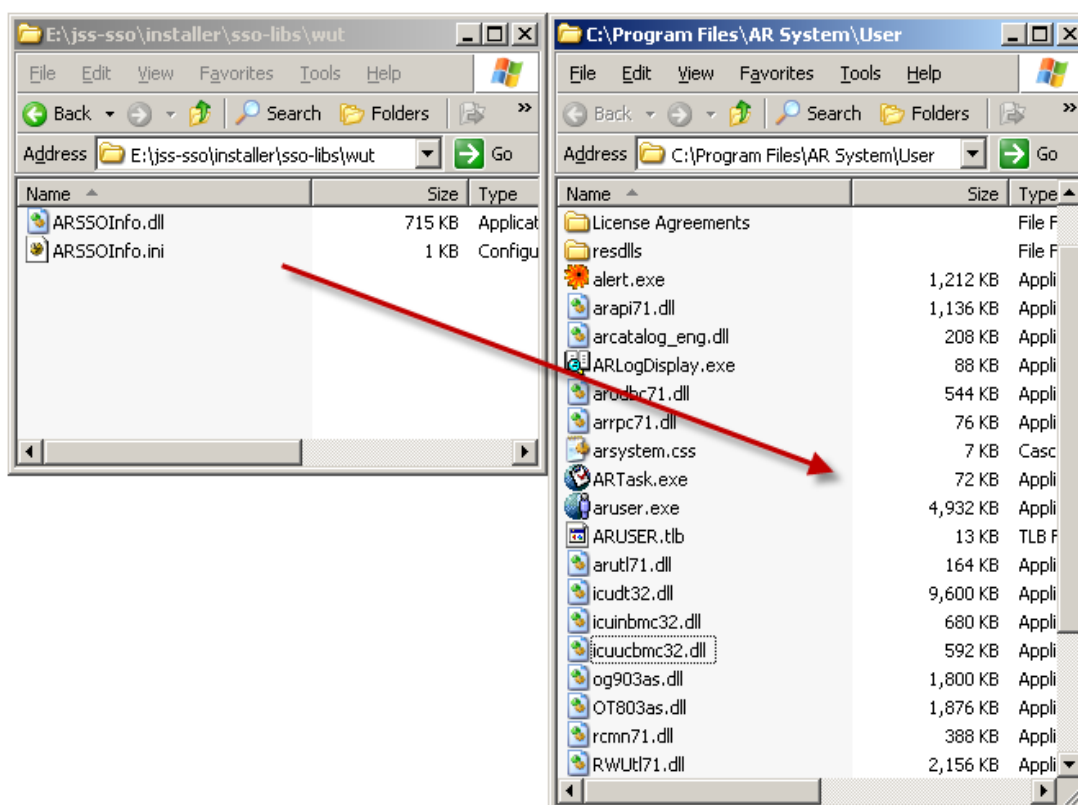
Platform | Timeouts | Licenses | Configuration | **Log Files** | Database | Ports and Queues | Advanced | Source Control | Server Events | Connection Settings | Currency

<input type="checkbox"/> API	API Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varapisql.log	...	View
<input type="checkbox"/> Distributed Server	DSD Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\vardist.log	...	View
<input type="checkbox"/> Escalation	Escalation Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varescl.log	...	View
<input type="checkbox"/> Filter	Filter Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varfilter.log	...	View
<input type="checkbox"/> SQL	SQL Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varapisql.log	...	View
<input type="checkbox"/> Thread	Thread Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varthread.log	...	View
<input type="checkbox"/> User	User Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varuser.log	...	View
<input type="checkbox"/> Alert	Alert Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varalert.log	...	View
<input checked="" type="checkbox"/> Plug-In Server	Plug-in Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varplugin.log	...	View
<input type="checkbox"/> ARFORK	ARFORK Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varfork.log	...	View
<input type="checkbox"/> Server Group	Server Group Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varsrvgrp.log	...	View
<input type="checkbox"/> Full Text Index	Full Text Index Log File Name :	C:\Program Files\AR System\proddemo\Arserver\Db\varftindx.log	...	View

Plugin Log Level: All

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 along with a dynamic link library, ARSSOInfo.dll must be copied to the clients machine. These files must be copied to the same directory as the 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 Server connection information that should be used to login.

Userpreferenceserver: Values are arserver1, arserver2. This points to the section of AR 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 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. This should be left as is.

newsharedkey: If your shared key changes within the AR Server, then you can get the library to encrypt the data and replace the existing shared key. Place the plain text shared key with this value and restart the aruser.exe

forcemode: 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 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:

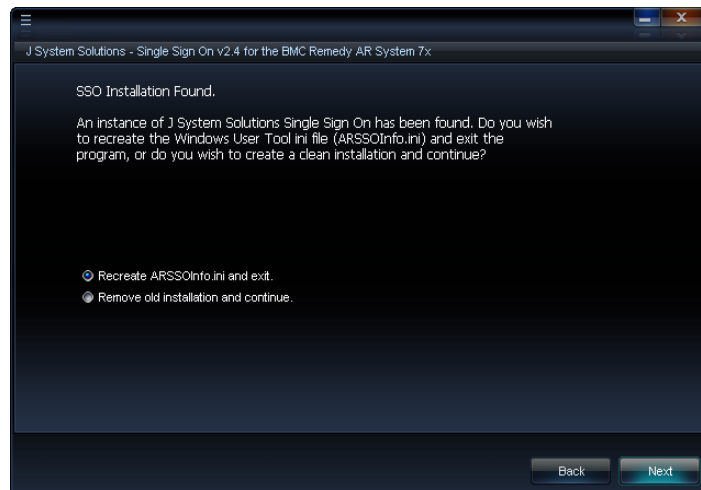
- **useralias=\$SSO_DOMAIN\$\\$SSO_USER\$** creates a login name JAVASYSTEMSOLUTIONS\dkellett
- **useralias=\$SSO_DOMAIN_LONG\$\\$SSO_USER\$** creates a login name javasystemsolutios.com\dkellett

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 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. Please see the screenshot below for an example:



Manually configuring the AR System

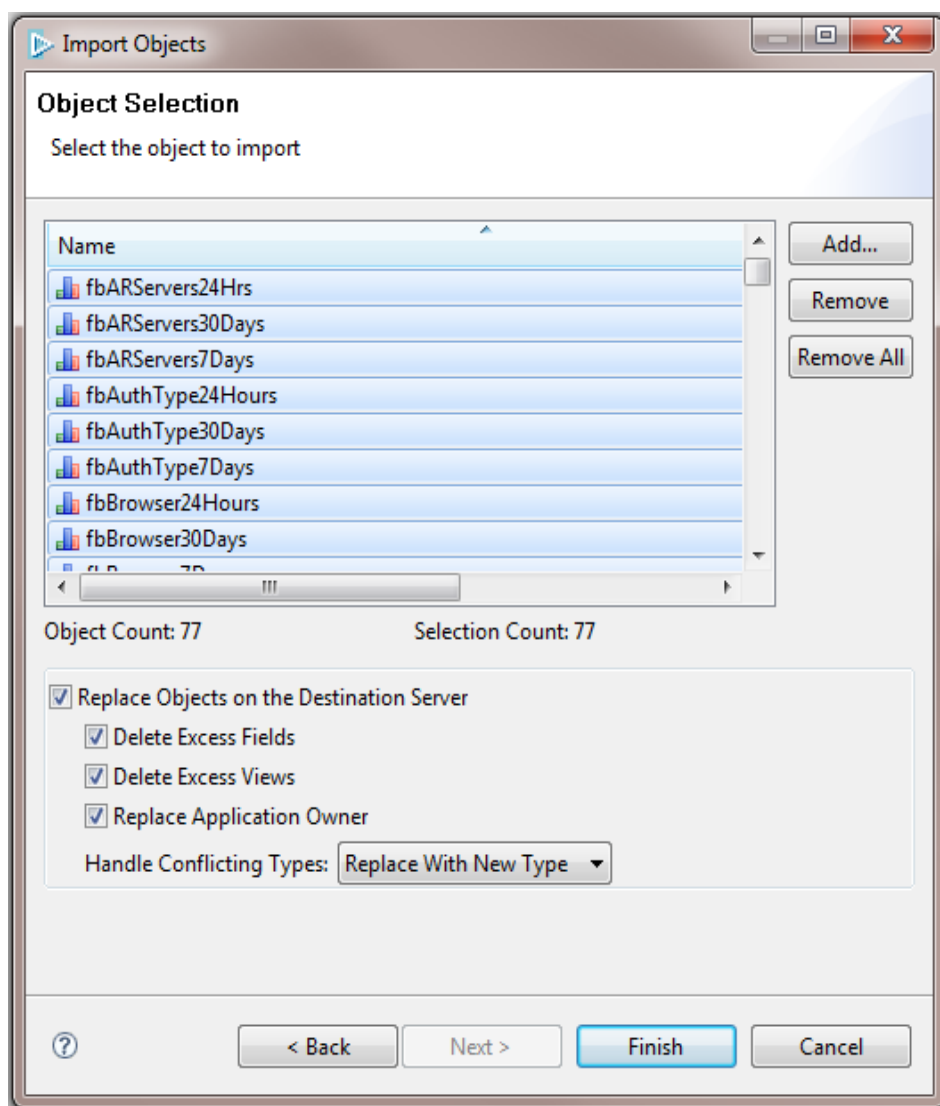
If for any reason the installation program fails. As always, you can contact JSS support. However, you can manually install the product with the following steps.

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

The .def file import installs an application called “SSO Administration”. This enables administrators only, to update SSO configuration.

Midtier Shared Key: plain text key. For the initial install, use password

ARUSER Shared Key: plain text key. For the initial install, use password

Midtier IP Address: insert the IP addresses of the SSO enabled midtiers.

License: This is the license key delivered by JSS. You can request a trial key from JSS.

Show Password in the arplugin log file: This will verify if the correct values are being passed from all the clients. While verifying the installation, it is a good idea to have this enabled. This can be turned off at any time.

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 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	<input type="text" value="jssoadmin"/>
Group ID	<input type="text" value="11114"/>
Group Type	<input type="radio"/> None <input type="radio"/> View <input checked="" type="radio"/> Change
Long Group Name	<input type="text" value="jssoadmin"/> ...
Group Category	<input type="radio"/> Regular <input type="radio"/> Dynamic <input checked="" type="radio"/> Computed
Computed Group	
	() AND OR NOT Append Group Append User
Group Definition	<input type="text" value="'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

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 Mid-Tier-Service-Password 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.

Mid-Tier-Service-Password:

ck1cBZaHOVi2yZ5FXxXjNcdiloJE5cxoFsk2L6r/MbdNvB+rY4/wraW/cyRcX/ABAgT MQttH+v73sinLGqdcwvOfygyhEwxXvB2z00r/Xk3gc2qp8J7dZg==

After clicking Generate, you should see the SSO password.

Service pass

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

SSO pass

Create a user with the following attributes

User Form																							
User Information																							
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Login Name</td> <td><input type="text" value="ssoadmin"/></td> </tr> <tr> <td>Full Name</td> <td><input type="text" value="ssoadmin"/></td> </tr> <tr> <td>Password</td> <td><input type="password" value="*****"/></td> </tr> <tr> <td>Group List</td> <td><input type="text" value="Administrator"/> <input type="button" value="..."/></td> </tr> <tr> <td>Computed Group List</td> <td><input type="text" value="ssoadmin;"/> <input type="button" value="..."/></td> </tr> </table>	Login Name	<input type="text" value="ssoadmin"/>	Full Name	<input type="text" value="ssoadmin"/>	Password	<input type="password" value="*****"/>	Group List	<input type="text" value="Administrator"/> <input type="button" value="..."/>	Computed Group List	<input type="text" value="ssoadmin;"/> <input type="button" value="..."/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td>License Type</td> <td><input type="radio"/> Read <input checked="" type="radio"/> Fixed <input type="radio"/> Floating</td> </tr> <tr> <td>Full Text License Type</td> <td><input checked="" type="radio"/> None <input type="radio"/> Fixed <input type="radio"/> Floating</td> </tr> <tr> <td>Application License</td> <td><input type="text"/></td> </tr> <tr> <td>Default Notify Mechanism</td> <td><input type="radio"/> None <input checked="" type="radio"/> Alert <input type="radio"/> Email</td> </tr> <tr> <td>Email Address</td> <td><input type="text"/></td> </tr> <tr> <td>Status</td> <td><input checked="" type="radio"/> Current <input type="radio"/> Disabled</td> </tr> </table>	License Type	<input type="radio"/> Read <input checked="" type="radio"/> Fixed <input type="radio"/> Floating	Full Text License Type	<input checked="" type="radio"/> None <input type="radio"/> Fixed <input type="radio"/> Floating	Application License	<input type="text"/>	Default Notify Mechanism	<input type="radio"/> None <input checked="" type="radio"/> Alert <input type="radio"/> Email	Email Address	<input type="text"/>	Status	<input checked="" type="radio"/> Current <input type="radio"/> Disabled
Login Name	<input type="text" value="ssoadmin"/>																						
Full Name	<input type="text" value="ssoadmin"/>																						
Password	<input type="password" value="*****"/>																						
Group List	<input type="text" value="Administrator"/> <input type="button" value="..."/>																						
Computed Group List	<input type="text" value="ssoadmin;"/> <input type="button" value="..."/>																						
License Type	<input type="radio"/> Read <input checked="" type="radio"/> Fixed <input type="radio"/> Floating																						
Full Text License Type	<input checked="" type="radio"/> None <input type="radio"/> Fixed <input type="radio"/> Floating																						
Application License	<input type="text"/>																						
Default Notify Mechanism	<input type="radio"/> None <input checked="" type="radio"/> Alert <input type="radio"/> Email																						
Email Address	<input type="text"/>																						
Status	<input checked="" type="radio"/> Current <input type="radio"/> 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 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)

bmcsoftware

Request ID:

Name:

Value:

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)

bmcsoftware

Request ID:

Name:

Value:

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: areahub.dll

Solaris/Linux

Plugin: 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

SSO for the User Tool was introduced in version 2.3 This involves placing two files on the clients PC or laptop within the same directory as the aruser.exe

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: 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: 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 Plugins 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 Midtier to login via AREA.

AREA LDAP Configuration

Configuration List

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

Clear Fields
Save Current Configuration
Delete Configuration
Decrease Order
Increase Order

Configuration Detail

Directory Service Information		User and Group Information	
Host Name *	pluto	User Base*	DC=development,DC=strategicworkfl
Port Number	389	User Search Filter*	samaccountname=\$\USER\$
Bind User	development\administrator	Group Membership	None
Bind Password	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Group Base	
Use Secure Socket Layer	No	Group Search Filter	
Certificate Database*		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-ss0.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: areahub.dll
AREA-Hub-Plugin: jss-ss0.dll
AREA-Hub-Plugin: arealdap.dll
```

Note, both order and case are important.

Upgrades

If using a version prior to 3.0

Remove all existing SSO Plugin files and re-install the product from scratch.

This includes any JSS work flow that may be in the AR System – use AR System Developer Studio (or the old Remedy Administration Tool) and remove all forms/filters and active links that have the prefix JSS). If you do not do this, you may see unexpected errors when running the installation tool (setup.exe).

If using version 3.0, 3.1 or 3.2

Upgrading the AR System

You can either perform a manual upgrade by following the manual steps or use the Windows setup program. If you run the program, select 'remove old installation and continue'.

When the installation is complete, please stop AR System server and follow the relevant step below:

1. On Windows, remove the previous SSO Plugin AREA plugin directory from the AR System server directory. In version 3.0/3.1 it was called arplugin.exe.local. In version 3.2+ it's called SSOvX where X is the previous version. This can not be removed by the installer as AR System is running and has loaded the AREA plugin, therefore it can only be removed when AR System is stopped.
2. On Unix, copy the .so for the correct operating system to your AR System server directory, replacing the existing jss-ss0.so.

Use the Windows User Tool to test the SSO implementation after restarting AR System. If it fails, re-run the setup program and select 'update ssoadmin password' and restart AR System. If it continues to fail then contact JSS providing the ar.cfg and plugin log file.

Upgrading the Midtier

As with any normal installation, copy the contents of the mt directory into your Midtier. Restart the Midtier.

If you're using version 3.0 with built-in authentication and NTLM, you will need to reconfigure the SSO Plugin so please review the Configuring NTLM section of this manual.

If using version 3.3

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-ss0.dll/jss-ss0.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. Stop Tomcat.
 6. Replace the Midtier files, ie copy the contents of the mt directory into the Midtier.
 7. Delete the Tomcat 'work' directory, which is a temporary cache directory re-created when Tomcat starts.
 8. Start Tomcat.
 9. Go to the Midtier SSO configuration, check it is still correct and press 'set configuration'.