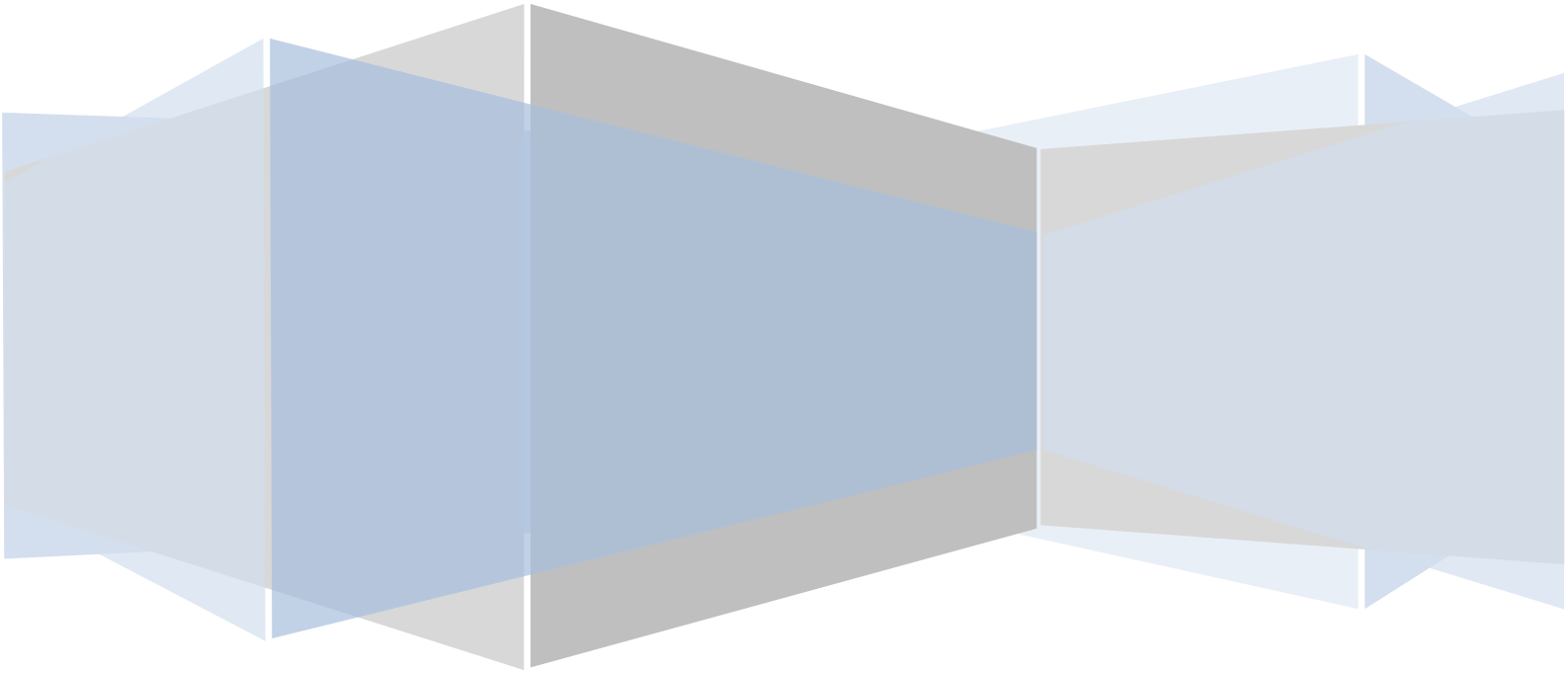
SSO Plugin v 3.3

Troubleshooting

J System Solutions

http://www.javasystemsolutions.com

Version 3.3



Troubleshooting

You will find a range of potential issues below, with advice on how to resolve them

Midtier

The Midtier can not find the jss-sso.jar file

If you've forgotten to put the jss-sso.jar file in the Midtier WEB-INF/lib directory, it will probably crash with one of the following stacktraces:

```
java.lang.ClassNotFoundException:
com.javasystemsolutions.mt.sso.JSSAuthenticator
org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLo
ader.java:1387)
org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLo
ader.java:1233)
java.lang.ClassLoader.loadClassInternal(ClassLoader.java:319)
```

or

```
11-Apr-2009 15:33:59 org.apache.catalina.core.StandardContext
filterStart
SEVERE: Exception starting filter spnego
java.lang.ClassNotFoundException:
com.javasystemsolutions.mt.sso.SPNEGOHttpFilter
org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLo
ader.java:1387)
org.apache.catalina.loader.WebappClassLoader.loadClass(WebappClassLo
ader.java:1233)
org.apache.catalina.core.ApplicationFilterConfig.getFilter(Applicati
onFilterConfig.java:249)
```

I'm using Windows Authentication. The plugin is installed but the Midtier keeps prompting me for a username/password in a Windows dialog box.

In order to use SSO, your browser must support SSO and you must be logged into the domain. If a logon box, or unauthorised, is presented when you connect to the Midtier, please consider the following:

1. You must be logged into a domain for SSO to work!
2. The client must be Windows 2000, Windows XP, Windows Vista or Windows Server 2000/2003/2008. Older versions of Windows or the Home editions may not work.
3. The domain controller should be running Active Directory.
4. The user operating the browser must be logged into the Active Directory domain. To ensure this is the case, press ctrl+alt+del and look at the 'You are logged in as' dialog - the Windows Domain shown must be the target domain and not the local machine.

5. If using IE, check the following:
    1. The Midtier must be listed in the 'Local Intranet zone'. To check this, go to Internet Explorer -> Tools -> Internet Options -> Security -> Local Intranet and make sure that the Midtier is present in the list.
    2. Automatic login must be enabled. To check this, go to Internet Explorer -> Tools -> Internet Options -> Security -> Custom Level, scroll all the way to the bottom and make sure 'Automatic logon only in Intranet zone' is selected.
6. If using Firefox, type about:config, search for 'negotiate' and ensure the hostname of the Midtier is in the 'trusted-uris' and 'delegation-uris'.
7. If your browser is configured to use a proxy server, the target website may need to be added to the proxy exceptions list as SSO is known to be problematic through some proxies.
8. Ensure the clocks on the workstation and the AD are set correctly. Kerberos authentication can fail if the clocks are very skewed.

I'm using Firefox and it won't perform Windows Authentication

This information is required for both built-in authentication and an IIS front end. If you're using Firefox then you can configure it to perform Windows Authentication (and not prompt you for a username/password) as follows:

1. Type about:config into the URL bar.
2. Type trusted into the Filter text field.
3. Edit the network.automatic-ntlm-auth.trusted-uris preference and add the hostname of the Midtier.
4. Edit the network.negotiate-auth.trusted-uris preference and add the hostname of the Midtier.

Authenticating against multiple Windows Domains

If you've got multiple Windows domains (for example, A and B) and they trust each other, then the product can be configured to authenticate against domain A and should also be able to authenticate users for domain B. To check if the domains are in a trusted relationship, simply type:

```
netdom query /domain:fully.qualified.domain trust
Expected output:
↔ DOMAIN Direct
```

Ensuring a service account has not been locked out

Run the following command to retrieve account information for a user, including whether it's been locked out:

```
net user service_account
```

Constant redirection to error page

We believe this has been fixed in Midtier 7.1+, however the discussion is included to aid troubleshooting.

We discovered a bug with the Midtier and the way it handles a custom Authenticator. If an Authenticator plugin returns login details that turn out to be invalid, the Midtier redirects to a login page but refuses to ever return to /arsys/home. If you type /arsys/home into the browser, it simply tries to login again with the previous login details.

You can easily reproduce this by attempting SSO with a user that's got a password set in the User form. When this condition occurs, the Midtier redirects to the error page. This error page is located in the file [Midtier installation]/shared/error.jsp, and in order to 'fix' the bug, this file must be modified.

Open the file in your favourite text editor and apply the following patch (put it before the <html> tag):

```
<%
  // JSS SSO Patch. Clear the session so Midtier will
  // make another attempt to call the Authenticator plugin.
  session.invalidate();
%>
<html>
```

It is entirely possible that BMC will fix this bug in some patch to the Midtier – they are only missing one line of code. Therefore, if you are experiencing problems where by the Midtier redirects to an error page and then fails to let you go back to /arsys/home *using the same browser window*, apply the patch above.

We would appreciate your feedback if you need to apply this patch (please tell us the version of Midtier).

Manually creating the NTLM service account

If you can not use our set-service-account.cmd script, or wish to follow the manual steps, they are as follows – please note, we recommend you use our automated script as detailed in the installation manual!

Step 1 – Creating the service account

To do this, open the Active Directory Users and Computers utility and create a new Computer object (right click on Computers). Enter JSS-SSO-SERVICE as the Computer Name, which should auto complete the Pre-Windows 2000 name field too.

Step 2 - Set the service account password

This can not currently be performed through the Activity Directory Users and Computers utility, so we've provided a script to make this as easy as possible – it's called set-service-account.cmd and is included in the installation files. Run the script and you should be able to accept the

default values by pressing enter three times – it will create a password for you, please write this down!

If you are using any other utility (and you shouldn't need to), you may need to determine the service account distinguished name (DN) for setting the password – this can usually be derived from the account name and domain. For example if the service account name is JSS-SSO-SERVICE in the Active Directory domain demodomain.local, the dn will probably be:

cn=JSS-SSO-SERVICE,cn=computers,dc=demodomain,dc=local.

When I access the Midtier using SSO, I see ARERR 8922

ARERR8922 is as follows: *The authentication service is not responding. Cannot connect to the system at this time. Contact your AR System Administrator for assistance.*

This can be caused when the Midtier IP address is not present in the list of allowed IP addresses in the JSS AREA Plugin configuration, accessed via the SSO Administration Console. To confirm this is the problem, look at the AR System plugin log for the following:

```
<PLGN> <TID: 003248> <RPC ID: 0000000020> <Queue: AREA      >
<Client-RPC: 390695> /* Sun Sep 19 2010 15:29:32.3600
*/<JSS.AREA.SSO> <FINEST> + AREAVerifyLoginCallback
<PLGN> <TID: 003248> <RPC ID: 0000000020> <Queue: AREA      >
<Client-RPC: 390695> /* Sun Sep 19 2010 15:29:32.3600
*/<JSS.AREA.SSO> <FINE>     Verifying administrator's IP@
192.168.0.2 with the Mid-tier IP@ 127.0.0.1
<PLGN> <TID: 003248> <RPC ID: 0000000020> <Queue: AREA      >
<Client-RPC: 390695> /* Sun Sep 19 2010 15:29:32.3600
*/<JSS.AREA.SSO> <FINE>     Verifying administrator's IP@
192.168.0.2 with the Mid-tier IP@ 192.168.0.54
<PLGN> <TID: 003248> <RPC ID: 0000000020> <Queue: AREA      >
<Client-RPC: 390695> /* Sun Sep 19 2010 15:29:32.3600
*/<JSS.AREA.SSO> <FINE>     Verifying administrator's IP@
192.168.0.2 with the Mid-tier IP@ 127.0.1.1
<PLGN> <TID: 003248> <RPC ID: 0000000020> <Queue: AREA      >
<Client-RPC: 390695> /* Sun Sep 19 2010 15:29:32.3600
*/<JSS.AREA.SSO> <FINE>    [80690] FAILED LOGIN FOR administrator.
The clients network address is 192.168.0.2
```

In this case, the Midtier is running on a server with IP address 192.168.0.2 and this is not present in the configuration. To resolve the issue, add 192.168.0.2 to the list of allowed IP addresses.

My Windows account keeps locking

In a nutshell, ensure all AR System servers configured with the Midtier are SSO enabled. Account locking can happen in a very specific set of circumstances when two or more AR System servers are configured with a Midtier, one of them is not SSO enabled, and the non-SSO enabled AR System server is configured to use the BMC AREA LDAP plugin. When you login to the Midtier and visit the Home page (but there may be other forms that cause the problem), the Midtier tries to login to all AR System

servers to retrieve the 'entry points'. It will pass the username and an SSO key to the non-SSO enabled AR System server, which will pass that to the BMC AREA LDAP plugin, causing an invalid Windows network login. After three invalid Windows network logins, the Domain Controller will lock out your account.

Using built-in Active Directory integration, some browsers authenticate and some do not

Have you ensured the IE browser is in the Local Intranet Zone?

If so, and IE reports status code 400 then it may be due to a large Kerberos token sent from the browser and rejected by Tomcat's HTTP connector.

By default, Tomcat has a hard coded limit of 4Kb for an HTTP header, and if the Kerberos token exceeds 4Kb then Tomcat returns status code 400 without passing the request to the Midtier. The standard BMC Tomcat distribution has been known to have 8Kb set, which can still be inadequate.

The reason it can happen on some instances of IE and not others is that the Kerberos token contains the user's Active Directory groups. If a user is a member of many groups, their Kerberos token can become very large, exceeding the limit in Tomcat. To resolve the problem, open the Tomcat server.xml file, look for the HTTP connector:

```
<Connector port="8080" protocol="HTTP/1.1"
```

and add a maxHttpHeaderSize attribute, which is given a value in bytes (24576 is 24Kb):

```
<Connector port="8080" protocol="HTTP/1.1" maxHttpHeaderSize=”24576”
```

Restart Tomcat and try again.

How to obtain a Fiddler trace (for reporting browser SSO issues)

If you report an issue with Midtier SSO, you may be asked to send a 'fiddler trace'. To do this, please visit http://www.fiddler2.com/fiddler2/ and download Fiddler. Once installed, open IE and go to Tools -> Fiddler2 (or just open IE and run Fiddler from the programs menu), use IE to demonstrate the problem, go to Fiddler and click File -> Save -> All sessions, take a screenshot of IE and send both the screenshot and the Fiddler '.saz' file to JSS support.

Advanced Kerberos troubleshooting

Ensuring your workstation has obtained a Kerberos token

The following will help diagnose why a Kerberos token is not being sent from your browser:

1. Use the kerbtray tool to see if you're getting an HTTP/ ticket for the Midtier. If not, check the SPN was setup correctly on the Active Directory.
2. Check there are not multiple SPNs set against the Midtier host. Use an LDAP tool (such as ldp.exe) to search the AD.
3. Check the user does not have a blank password. The AD will never issue a Kerberos ticket for users with blank passwords.

Ensuring the Kerberos token is reaching the SSO Plugin

The following will help diagnose why a Kerberos token is not reaching the SSO Plugin:

1. Use a network monitor (such as Fiddler) to see if your browser is sending a Kerberos token.
2. If using IIS as a front end to Tomcat, check it is not interfering with authentication (at both site object and virtual directory) by ensuring that 'Enable anonymous access' is checked, and the 'Authenticated access' check boxes are unchecked.
3. Kerberos tokens are large and Tomcat/mod_jk have restrictions set on the maximum header size.
    1. If you're connecting directly to Tomcat, edit the Tomcat server.xml file, find the HTTP Connector and set the maxHttpHeaderSize to 16384 (16k in bytes).
    2. If you're using an IIS front end then a value needs to be set in the mod_jk workers.properties file and the Tomcat server.xml file.
        1. Open workers.properties and set max_packet_size to 16384.
        2. Open the Tomcat server.xml file, find the AJP Connector and set (you may need to add it) the packetSize attribute to 16384.

Kerberos causes a stack trace in the logs and in the browser window when using the Test SSO page

If you see the following error in the browser and/or Tomcat logs:

```
javax.security.auth.login.LoginException: Pre-authentication
information was invalid (24)
```

then check the configuration details. Possible causes are:

2. If you entered a Windows Domain instead of a Kerberos realm (which is often the Windows Domain DNS name - see installation manual) – you will see this error.
3. If the service account has now expired.

Ensuring IIS is performing Kerberos authentication

If you are using IIS as a front end to Tomcat, and you will to let IIS perform Windows Authentication, the following will help diagnose why IIS is not performing IWA:

1. Use the kerbtray tool to see if you're getting an HOST/ ticket for the machine. If not, check the SPN was setup correctly on the Active Directory.
2. Check there are not multiple SPNs set against the machine hostname. Use an LDAP tool (such as ldp.exe) to search the AD.

Kerberos failure, checking for duplicate SPNs

Kerberos will not work if there are duplicate SPNs, ie the same hostname (HTTP/mymidtier.domain.com) is registered to two different computer or user accounts.

Microsoft's update to setspn (KB970536) has a new feature which can search for duplicate accounts. Simply run: setspn -X. If any duplicates are listed the remove the incorrect entries using: setspn -D.

IIS and Tomcat

I can view the default IIS home page but I can't access the Midtier at all.

The issue is that whilst the Midtier on Tomcat appears to be running, and IIS serves static files like /iisstart.htm correctly, attempting to connect to Midtier via IIS gives an IE "Cannot find server or DNS Error" error page.

Checking the Windows Event Viewer shows that IIS is crashing when an attempt is made to access Tomcat via the Jakarta ISAPI Redirector.

It is not clear whether this is an isolated incident on one particular server, or whether it might recur in future. The server in question was a 64-bit Windows 2003 Server Hyper-V VM, with IIS configured to run 32-bit ISAPI extensions. However other VMs with the same setup have not demonstrated this behaviour.

It is not a well-known bug or one that has affected us before. It occurs whether or not SSO Plugin is installed. The version of Midtier installed was 7.1.

The solution is to replace the isapi_redirect.dll file with an up-to-date version from Apache, such as:

http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.30/isapi_redirect-1.2.30.dll

(For a 64-bit machine running native 64-bit ISAPI extensions, the file under 'win64' should be used instead.)

To replace the ISAPI extension, go to Administrative Tools -> Services and shut down the World Wide Web Publishing service and HTTPS SSL. Find the DLL in 'Program Files' - (x86) if running 32-on-64 - 'Apache Software Foundation\Jakarta ISAPI Redirector\bin' and rename it to isapi_redirect-old.dll. Save the new DLL here and rename it simply isapi_redirect.dll.

Restart the stopped services.

I am prompted for my Windows login and they are not accepted

If you have run the set-service-account.cmd script on the Active Directory and entered the hostname of the machine running IIS, the IIS server will not be able to authenticate the tokens sent to it by your browser. Running this script is not required when using an IIS front end – it's only used when configuring SSO Plugin's built-in authentication (i.e. that provides Windows authentication without the need for IIS).

To resolve the problem, remove the JSS-SSO-SERVICE Computer account created in the Active Directory by the set-service-account.cmd script, and then clear the Kerberos tokens cached on the client desktop using the kerbtray.exe tool provided in the Windows 2000 Resource Kit, or wait ten minutes for the local machine to remove the tokens from its cache.

I am prompted with a Windows username/password dialog and can not login

This happens if IIS refuses to authenticate the browser.

1. Is your browser in the Local Intranet Zone? If not, add it.
2. Are you upgrading from a previous version of SSO Plugin which had a service account **with an SPN** setup on the AD, registered to the hostname running IIS? If so, remove the old service account (and SPN) from AD.
    1. This is likely if your previous configuration uses built-in Active Directory authentication and you ran the JSS set-service-account.cmd script to create the JSS-SSO-SERVICE computer account in Active Directory.

To verify whether IIS is able to authenticate a browser independently from SSO Plugin, follow these steps:

1. Open the IIS administration tool and find the 'default website'.
2. Check the iisstart.htm file is present (in the file listing under the site).
3. Go to a browser and navigate to this file. It should provide the “Under construction” web page (iisstart.htm).
4. Right click on the default website, click Directory Security, disable allow anonymous login and enable Integrated Windows Authentication.
5. Refresh the browser window. If prompted for a login then IIS is not working as expected. Resolve this issue before proceeding with SSO

Plugin. The issue is usually resolved by adding an SPN for the computer running IIS, ie:

setspn -A HTTP/hostname domain\computer

setspn -A HTTP/fully.qualified.hostname domain\computer

Windows User Tool

The message " [80685] AR User SSO Failed.” appears when I try an SSO login.

The AR System User Tool has not negotiated with the AR System server using the ARUSER-Shared-Key. If the product is licensed then contact JSS Support.

The message " [80686] AR User Tool SSO but ARUSER-Shared-Key is NULL.” appears when I try an SSO login.

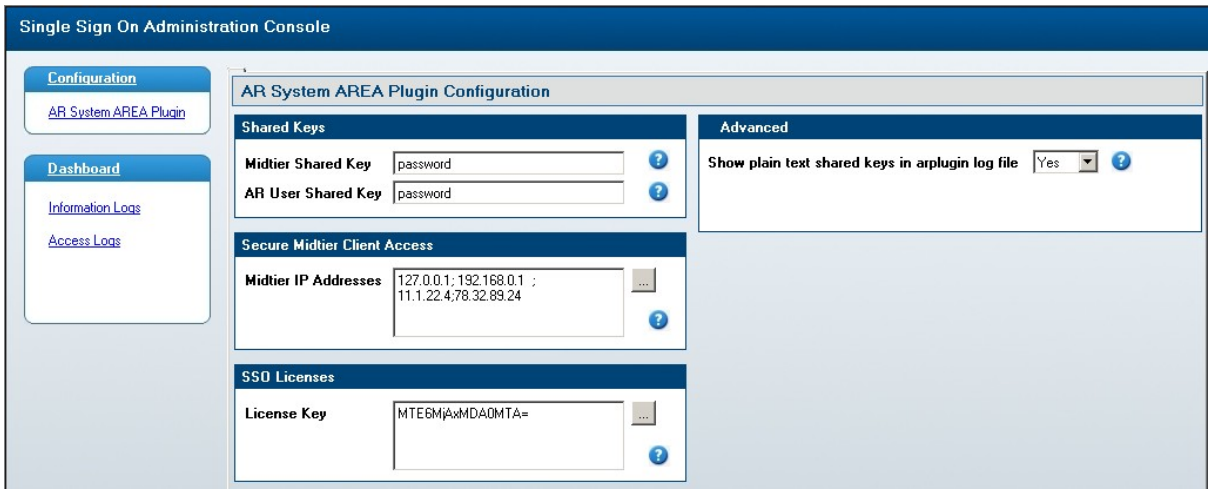
The AR System User Tool has not negotiated with the AR System server using the ARUSER-Shared-Key. If the product is licensed then contact JSS Support.

AR System

The message "SSO Request found from a valid SSO Midtier but MidTier-Shared-Key was incorrect.” appears in the AR System plugin log when I try an SSO login.

The Midtier-Shared-Key is an encrypted set of characters that is used when the SSO protected Midtier authenticates a user with the AR System. This value needs to match the one entered when configuring.

To view what the jss-sso plugin believes to be the shared keys, turn on ARPlugin log file as per Enable logging for verification Then open SSO Administration application in the user tool and make sure the following field is set to yes:



Restart the AR system.

View the plugin log and search for “UnEncrypted” Example screenshot below:

```
*/<JSS.AREA.SSO> <CONFIG>   MidTier-Shared-Key              CYkkdPJiPHehAu76b/LIdQ==
*/<JSS.AREA.SSO> <CONFIG>   showPasswords                   T
*/<JSS.AREA.SSO> <CONFIG>   UnEncrypted_MidTier-Shared-Key_fxtzicKYGNApsGWZ
```

If you believe the value to be incorrect, then replace the value showed in the SSO Administration form and restart your AR System.

[81211] ARERR90 Unable to connect to AR System, sleeping 30 seconds....

If you see the following in the arplugin log file, then this indicates that there is a connection problem for the plugin to communicate back the the AR Server.

```
<JSS.AREA.SSO> <CONFIG>  AR Server Connection          ARSSP-[SRV:proddemo70p1m][TCP:7000][RPC:390626]
<JSS.AREA.SSO> <SEVERE> [81211] ARERR90 Unable to connect to AR System, sleeping 30 seconds....
<JSS.AREA.SSO> <SEVERE> Error: messageNum:90 messageText:Cannot establish a network connection to the AR System server
```

Look at the log for <JSS.AREA.SSO> <SEVERE> AR Server Connection ...

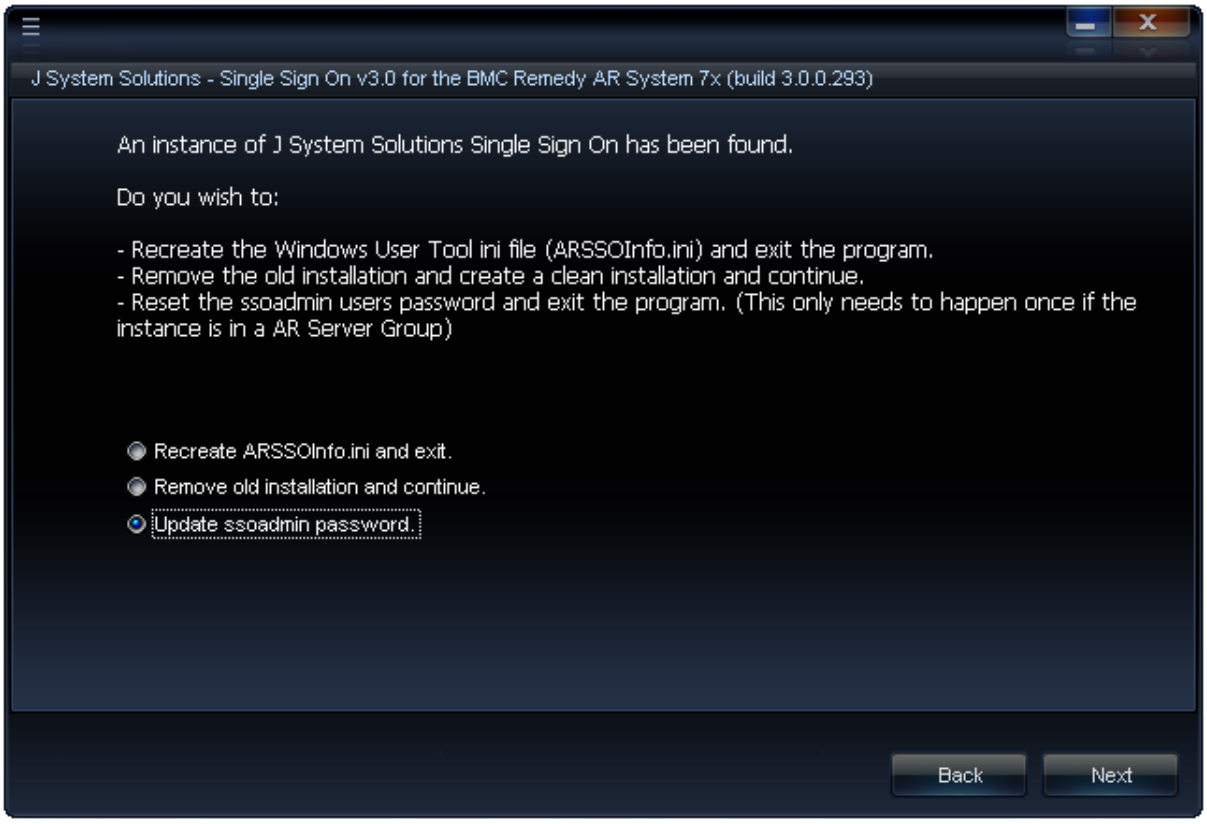
And verify the connection details including the TCP and RPC port. You may see this at the start of your arplugin log but then after a few 30 second intervals the plugin continues. This is due to some AR Servers being slow to start up which is fine and thus can ignore this error.

[81211] ARERR623 ssoadmin unable to authenticate. Please check the User Form for the Login Name ssoadmin

If this error message is detected in the arplugin log then this means the ssoadmin account is incorrect, missing or password is wrong. If you are upgrading from version 2 then you will need to reset the password.

```
<JSS.AREA.SSO> <CONFIG>  AR Server Connection          ARSSP-[SRV:proddemo70p1][TCP:7000][RPC:390626]
<JSS.AREA.SSO> <SEVERE> [81211] ARERR623 ssoadmin unable to authenticate. Please check the User Form for the Login Name ssoadmin
<JSS.AREA.SSO> <SEVERE> Note: messageNum:623 messageText:Authentication failed
<JSS.AREA.SSO> <FINEST> - ARGetJssInfo
<JSS.AREA.SSO> <FINEST> + jssParseLicCRC
<JSS.AREA.SSO> <SEVERE>  [80479] ##################################################################################################################
<JSS.AREA.SSO> <SEVERE>  [80479] Unable to connect to AR System. Unable to verify license. Please contact support@javasystemsolutior
<JSS.AREA.SSO> <SEVERE>  [80479] ##################################################################################################################
<JSS.AREA.SSO> <FINEST> - jssParseLicCRC
```

To reset or recreate the account, run the installation program downloaded with the v3 SSO evaluation. Login as an administrator then the application should prompt you with the following screen. Make sure you select “Update ssoadmin password” and restart the AR Server.



The AR System will cache user credentials until you log off.

The AR System seems to cache authentication details for successful logins. Therefore, if you were to login with a username and password that is looked up through LDAP (via the JSS AREA plugin), future login requests will result in the plugin not being called and LDAP not being checked. Hence, if you were to immediately change a user's password in LDAP, the original password will carry on working for a certain (unknown) time period because it's been cached by ARS! You can see this behaviour by switching on the AREA plugin logging and logging in twice with a valid LDAP username and password; the second login attempt will result in no call to the AREA plugin.

BMC are apparently aware of the issue.

Log files

The JSS Midtier plugin writes informational level messages to the Midtier log, and additional logging when the Log Level is configured in the setup page.

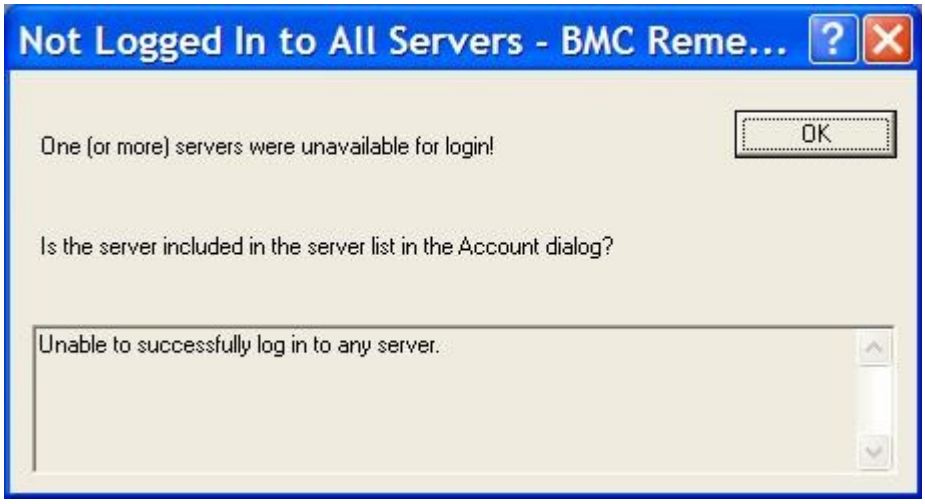
The JSS AREA plugin writes all errors to the arerror.log, and debugging messages are sent to arplugin.log depending on the value of Plugin-Log-Level in the ar.cfg file (100 is "all", 1000 is "none").

If you are reporting errors to JSS, please include the Midtier logs (with the Log Level set to debug), the arerror.log and arplugin.log with the Plugin-Log-Level set to 100. Please ensure the logs are concise and annotated if it all possible (i.e. please add notes above pertinent timestamps, such as "We did this and then this appeared...").

Windows User Tool SSO (ARSSOInfo.dll)

Make sure the ARSSOInfo.dll exists. I it doesn't then copy from the evaluation zip file, downloaded from the JSS web site.

If the user is receiving the following dialog, check the ARSSOInfo.ini file section arserver1. This must contain a server name that is valid.



End to end testing of the SSO Plugin

The AR System does not come with a simple mechanism to facilitate the installation of single sign-on (SSO) plugins. Installation problems can often be tricky to resolve. If you are experiencing installation problems then please work through the following instructions to help diagnose the problem.

JSS AREA plugin

To start testing the installation, the JSS AREA plugin should be tested separately without using the Midtier. This can be achieved by using the Windows User Tool as a test harness.

Check AD login against the Windows User Tool

If you are using the BMC AREA plugin, check you can login to the WUT using your Windows/Active Directory username and password to ensure your BMC AREA plugin is configured correctly. If you can not complete this test then please refer to the BMC documentation.

Testing the JSS AREA plugin

This test ensures the correct Midtier IP was set during the installation process, and you can use the Windows User Tool to perform the test. Due to a WUT limitation, you can only run this test if the Midtier Shared Key is 30 characters or less, which can be found in the SSO Administration Console.

For this test to work, the WUT must be running on the same machine as the Midtier. If it's not then the IP address of the WUT machine must also be set in the list of Midtier IPs configured with the JSS AREA plugin.

To run the test, open the WUT and enter your Windows username and the Midtier Shared Key in the password box. The WUT should log you in. If it did not, re-check the Midtier IP addresses in the SSO Administration Console.

JSS SSO Midtier plugin

After successfully completing the JSS AREA plugin tests, proceed to check the Midtier plugin setup.

The Midtier requires a relatively modest amount of configuration, but some of the error messages one can encounter may be misleading, masking the real problem. In general, always check the servlet container (Tomcat etc.) log files when debugging.

If you're using Tomcat then these are located in the tomcat/logs directory (catalina.out and stdout.log are popular log file names, but you may wish to just look at the most recently modified files).

Checking you copied the files into the Midtier

Can you find the jss-sso.jar file in the Midtier WEB-INF/lib directory? If not, you have not copied the files into the Midtier. Consult the installation instructions.

Checking the Midtier has been reconfigured correctly

During the installation process you will have pointed your browser at http://your-host/arsys/jss-sso/index.jsp and configured the SSO Plugin. Go back to this form and reconfigure the plugin.

If an error occurs that mentions ClassNotFound, check to make sure the jss-sso.jar file has been placed in the Midtier WEB-INF/lib directory.

If the error mentions an IOException then check to make sure the system account used by the webserver can write to the WEB-INF/classes directory (it will need to for Midtier's configuration to operate correctly) and the WEB-INF/web.xml file.

Assuming you have reconfigured the plugin, check to make sure the jss-sso.config file is present in the WEB-INF/classes directory. Also, open up the WEB-INF/classes/config.properties and ensure the plugin has been enabled by searching for the following line:

```
arsystem.authenticator=com.javasystemsolutions.mt.sso.JSSAuthenticator
```

If you do not see this then the SSO Plugin installation has failed. It is very unlikely this should happen so please contact support immediately if you are seeing this behaviour.

Also check to ensure there is no mention of

```
arsystem.authenticator.config= ...
```

in the config.properties file as this causes the Midtier to fail for various version 7.0 releases.

Errors reported when submitting the Midtier SSO Plugin setup page

When you submitted the Midtier SSO Plugin setup page, were there errors or warnings reported at the top of the page? If so, review them and speak to JSS for further assistance if required.

Checking the web.xml if using built-in authentication / IIS / OpenID

The web.xml file should be patched when the Midtier SSO Plugin setup page is submitted. Open the web.xml and search for the string *com.javasystemsolutions*. If it does not exist then contact JSS for help on manually patching the web.xml file.

Checking the Midtier functions without the SSO Plugin enabled

Go to the JSS configuration page (http://your-host/arsys/jss-sso/index.jsp) and click ‘disable the plugin’.

Restart the Midtier and go to http://your-host/arsys/home . If you are sent to the normal Midtier home page and can login then the problem is definitely due to the JSS SSO Midtier plugin configuration, however if the Midtier still fails to work with the SSO Plugin disabled then there is a separate problem. At this point it's best to contact JSS.

SSO appears to work but an alert box is displayed with ARERR9215

This issue was discovered on Midtier 7.0.

If you open the Tomcat logs and see this:

```
Caused by: ARERR [9357] Unsupported timezone XXX
```

Copy the GMT.js file from the mt/resources installation directory into the Midtier/resources/standard/javascript/timezone directory and call it XXX.js.

Please contact JSS support so we can supply this missing Javascript file with the product.

It appears BMC included GMT.js in Midtier 7.1.

What to do if the problem still remains

If you can not resolve the problem then contact JSS support and include the following information:

- an overview of the problem and the steps you've taken to resolve it.
- a copy of the AR System plugin log file (with the Plugin-Log-Level set to 100) showing a user logging into the WUT and a user attempting to log in to the Midtier.
- the ar.cfg file from the AR System.
- screenshot of your SSO Administration AR System Plugin settings form.
- webserver log files, i.e. the contents of the Tomcat logs directory.
- details of the AR System server and Midtier.