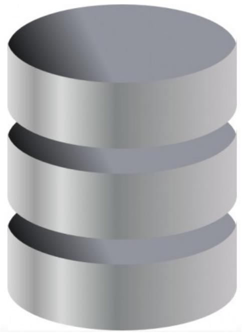
Re-enabling SSO Plugin after a database restore

This article is intended for customers using BMC AR System



Introduction

Migrating AR System databases has become the easiest way to synchronise application instances. The most frequent use case of migrating production to a test or development environment, this article provides instructions on how to re-enable SSO Plugin.

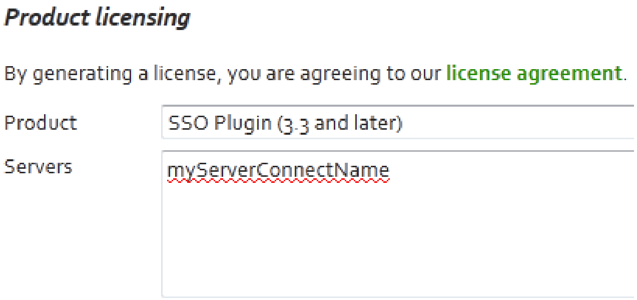
The instance from where the restore came from will be known as the source system and the instance that refresh is taking place on will be known as the destination system.

Step 1: Copy the jss-sso-salt value from the ar.cfg / ar.conf on the source instance to the destination ar.cfg / ar.conf

The external authentication plugin (AREA) module of SSO Plugin connects to the AR System as a user with the login name of ssoadmin. The password to this account is encrypted within the jss-sso-salt parameter that is found in the ar.cfg or the ar.conf depending on your operating system.

Step 2: Create / restore the SSO Plugin license

The product license is generated from the ar.cfg / ar.conf parameter Server-Connect-Name if the instance is in a server group or Server-Name if the Server-Connect-Name doesn't exit. Copy this value to the Servers box at the following URL http://www.javasystemsolutions.com/jss/licensing



Product licensing

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

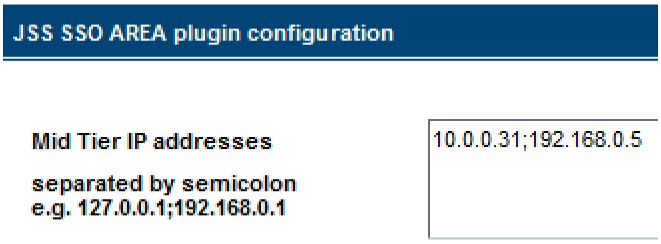
Product: SSO Plugin (3.3 and later)

Servers: myServerConnectName

Once the license is generated, login to the destination AR System as an Administrator, open the SSO Administration Console and replace the existing license key.

Step 3: Update the Mid Tier IP addresses in the SSO Admin Console

Verifying the Mid Tier IP address that the user is authenticating from is a feature of SSO Plugin. When a database is restored, the IP addresses will likely be for a different Mid Tier instance than the one accessing the destination application. Therefore the correct IP of the Mid Tier will need updating in the SSO Administration Console. Login to the destination AR System as an Administrator, open the SSO Administration Console and replace the existing IP addresses.



JSS SSO AREA plugin configuration

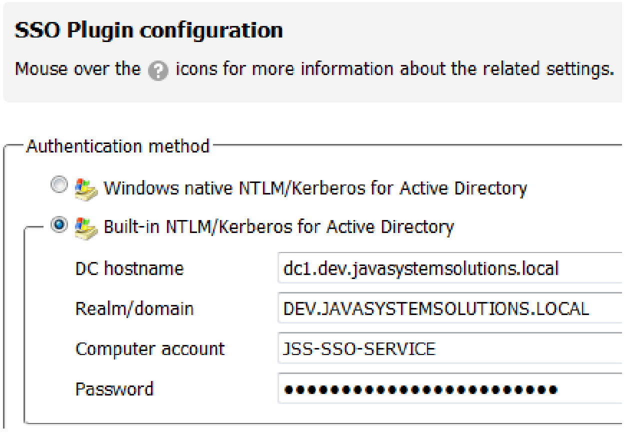
Mid Tier IP addresses

separated by semicolon
e.g. 127.0.0.1;192.168.0.1

10.0.0.31;192.168.0.5

Step 4: Update the authentication methods configuration

Depending on your authentication method used, certain information is unique to the Mid Tier instance. For example, if the customer is using "Built-in NTLM/Kerberos for Active Directory", the computer account can not be shared between Mid Tier instances. Therefore this configuration needs updating to include the computer account specifically created for the Mid Tier connecting to the destination AR Server.



SSO Plugin configuration

Mouse over the ? icons for more information about the related settings.

Authentication method

○ Windows native NTLM/Kerberos for Active Directory

● Built-in NTLM/Kerberos for Active Directory

DC hostname	dc1.dev.javasystemsolutions.local
Realm/domain	DEV.JAVASYSTEMSOLUTIONS.LOCAL
Computer account	JSS-SSO-SERVICE
Password	••••••••••••••••••••••••

Other integration types may need updating. It is recommended that the customer review all the information in the console.

Java System Solutions

Java System Solutions have been the market leader in single sign on and security since 2007. We have deployed SSO Plugin to some of BMC's largest enterprise and security conscious customers. We continue to consistently gain recognition for our service and support.
http://www.javasystemsolutions.com/jss/quotes