SSO Plugin with Microsoft Active Directory™ (AD)

Our most common deployment explained

Many organisations use Active Directory (AD) as the authentication repository for their users. So when the decision is made to implement single sign on (SSO), the AD is the natural choice of identity provider. This document describes the terminology, typical architecture and configuration steps to enable SSO for your service management applications.

Contents

Introduction and terminology

A single sign on (SSO) with Active Directory implementation means that the end user logs into their desktop and from then on, the applications automatically know who they are and can trust that information. All without being prompted for their login credentials again.
This is also known as Integrated Windows Authentication (IWA). There are two protocols within IWA. Kerberos and NTLMv2.

SSO Plugin will utilise both protocols maximising the variations of operating system and browser installations.

Architecture and deployment summary

In all AD SSO deployments, it is only the Java web server that will communicate with the AD instances.

Network and protocol
This requires TCP ports 88 (for Kerberos) and 445 (Microsoft-DS/SMB) configured on any network devices.
Kerberos
A single user account is used with service principle names (SPN) assigned to the account.
Java web server deployed on non-Windows
A unique computer account for java web server instance will be required in the AD. JSS provides both a script and manual instructions to create and assign the relevant attributes.

Windows platforms and Non-Windows platforms

When the Java web servers (i.e. Apache Tomcat) connect to the AD using the NTLMv2 protocol, they have to authenticate as a **computer account** within the domain. The domain controller will not allow the communication needed by any other account type. The computer accounts need to be **unique for each Java web server.** If the operating system that the Java web server is installed on is Windows, then SSO Plugin will utilise that machines account.
If the operating system is UNIX/Linux then these unique computer accounts will need to be created within the Active Directory.

BMC Mid Tier / HP Web Tier installed on Microsoft Windows

Please note that the Windows machine will need to be part of the same forest/domain as the users. When the Java web servers is installed on Windows, for the NTLMv2 protocol there is no need for additional accounts to be created within the Active Directory. However, as recommended by JSS, if you would like Kerberos in addition to NTLMv2 then you will need a standard user account within the domain and a service principle name (SPN) created.

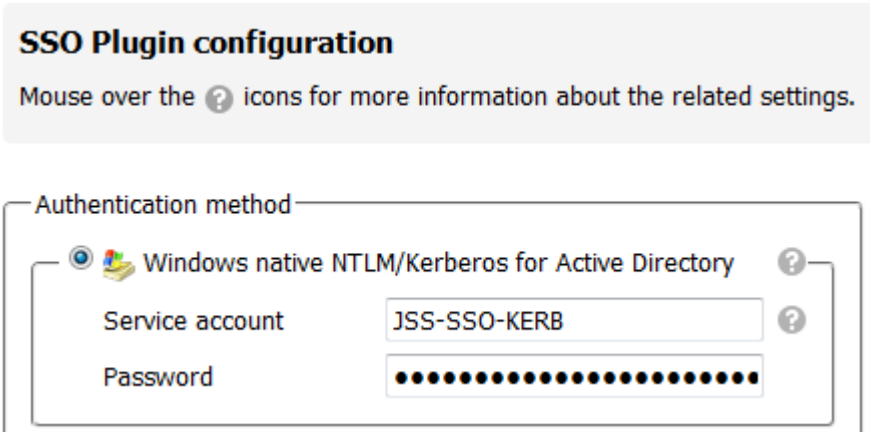
The Kerberos account can be a normal user account and assuming it is called JSS_SSO_KERB, the Active Directory administrator can enable Kerberos as follows:

setspn –A HTTP/loadBalancer.mydomain.com JSS_SSO_KERB
setspn –A HTTP/loadBalancer JSS_SSO_KERB

Please note, both the short hostname and fully qualified domain names are set uo to ensure that it wors whether a user types http://loadBalancer.mydomain.com or http://loadBalancer

The SSO Plugin configuration steps are very simple. Once the relevant files have been extracted from the SSO Plugin evaluation download and the Java web server restarted, browse to the SSO Plugin configuration page.

BMC Mid Tier: http://loadBalancer/arsys/jss-sso/index.jsp
HP Web Tier: http://loadBalancer/webtier/jss-sso/index.jsp



When presented with the list of authentication methods, select the first as demonstrated in the above screenshot. The Service Account and password are optional for those customers who wish to use Kerberos in addition to NTLMv2 but we stress this is optional only. Upon selecting the authentication method, click on Set Configuration button, this section is complete.

BMC Mid Tier / HP Web Tier installed on Non-Windows

When the Java web servers (i.e. Apache Tomcat) connect to the AD using the NTLMv2 protocol, they have to authenticate as a **computer account** within the domain. The computer accounts need to be **unique for each Java web server (i.e. each BMC Mid Tier or HP Web Tier)** and following the NetBIOS standard, the computer account name has a **maximum length of 15 characters**. Finally, when creating these computer accounts, they need to be **uppercased**.

Here is a table of examples

Java Web Server Host Name	Service (Computer) Account
midtierhost**1**	MTHOST**1**SSOSVC
midtierhost**2**	MTHOST**2**SSOSVC
midtierhost**n**	MTHOST**N**SSOSVC

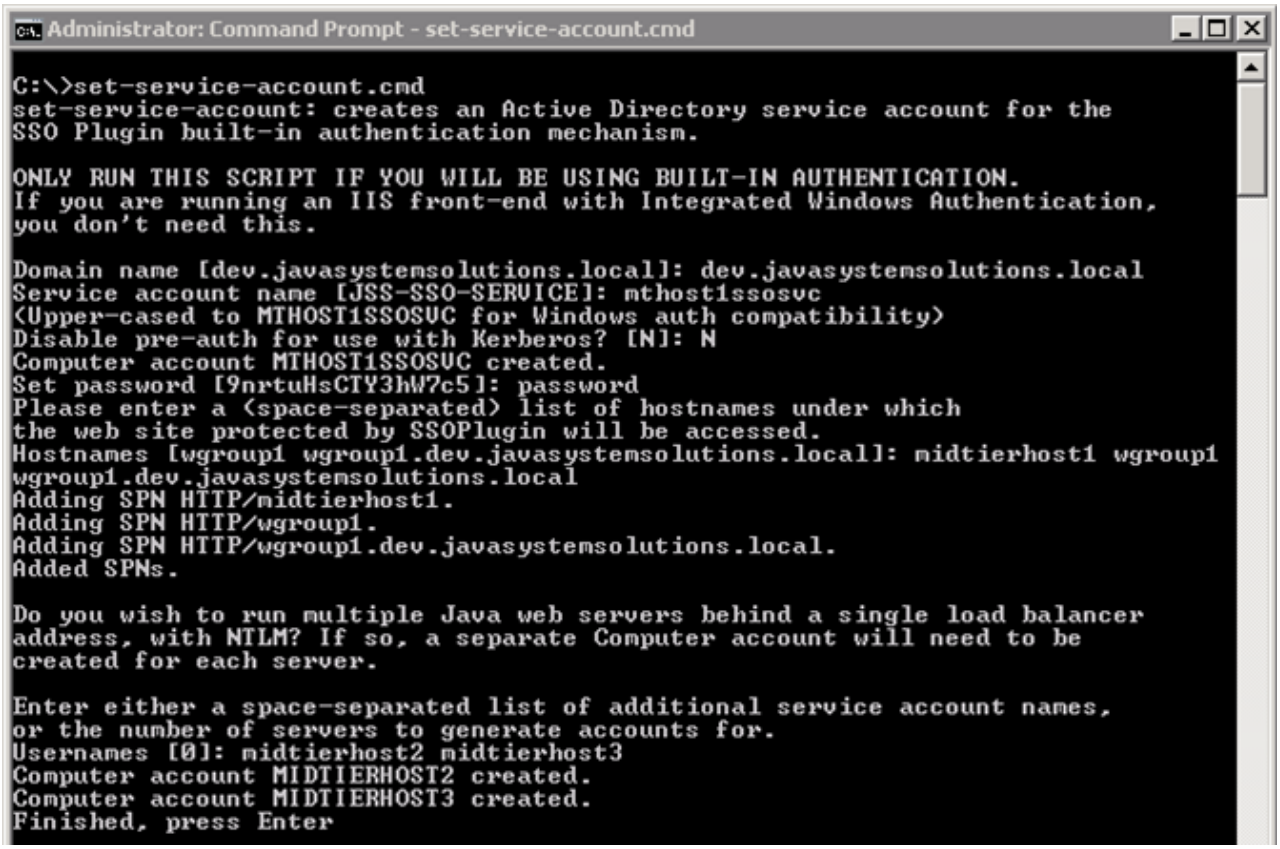
Service (Computer) accounts :: Creation using the JSS script

JSS has produced a script to negate the complexity. This script can be found here. You will need a login to the JSS website. If you do not have one you can create an account here. This must be run from Windows machine, logged into the domain as a domain administrator.

Here is a list of questions and information needed when running the script.

1. The fully qualified domain name e.g. dev.javasystemsolutions.com
2. The service (computer) account names
3. The passwords for each account. **Note this down. This is needed to configure SSO Plugin**
4. The hostnames and fully qualified hostnames of each Java web server and any load balancer names which will be situated in front of the those servers.

Here is an example of the script being run.



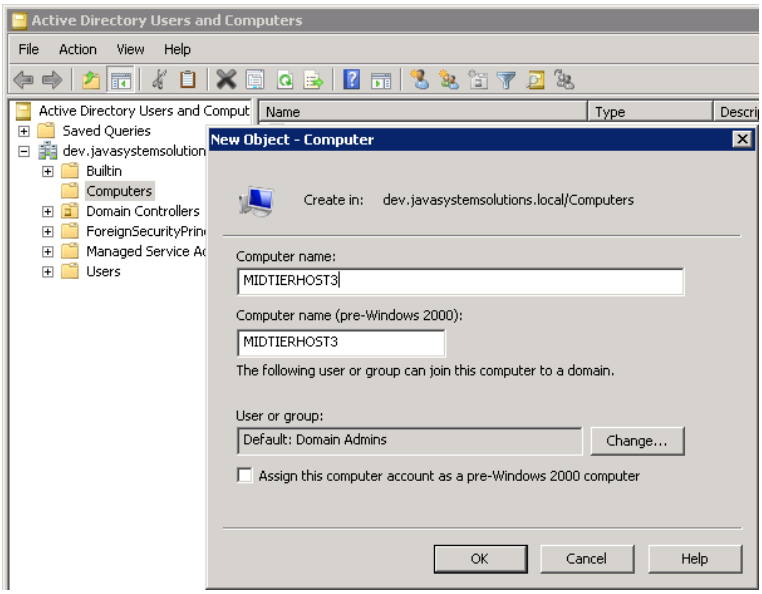
Service (Computer) accounts :: Manual creation steps (dsa.msc & ADSI Edit)

For some customers who are unable to run the script, here are the manual instructions. The following steps need to be run as a domain administrator logged into the domain.

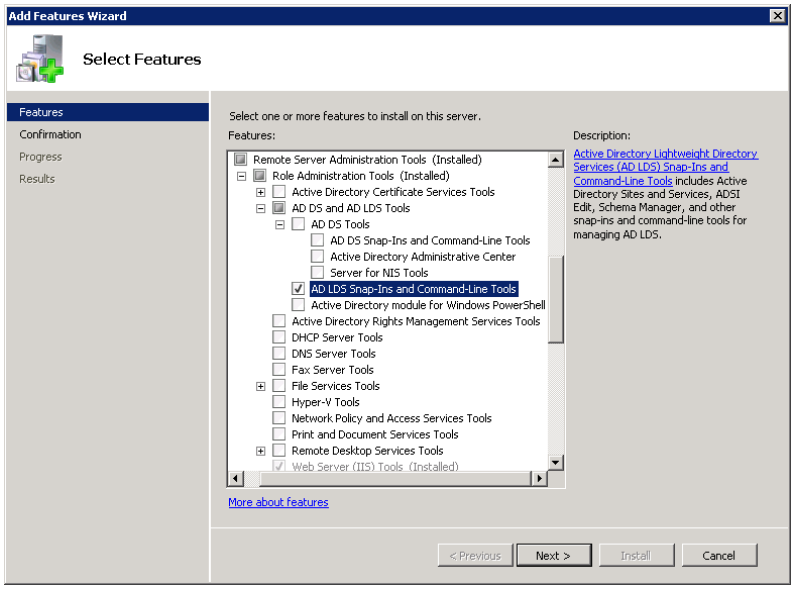
If run on the server where AD is installed then run Start > Administrator Tools > ADSI Edit

Create the computer account via dsa.msc

Using the dsa.msc, expand your domain name. Right click on Computers. Click New. Click Computer. Fill in the new computer account name remembering to use uppercase.



Creating a password for the computer account using ADSI Edit



For those who are not running this on the AD server, this can be installed by selecting Add Features on any Windows 2003 or 2008 server.

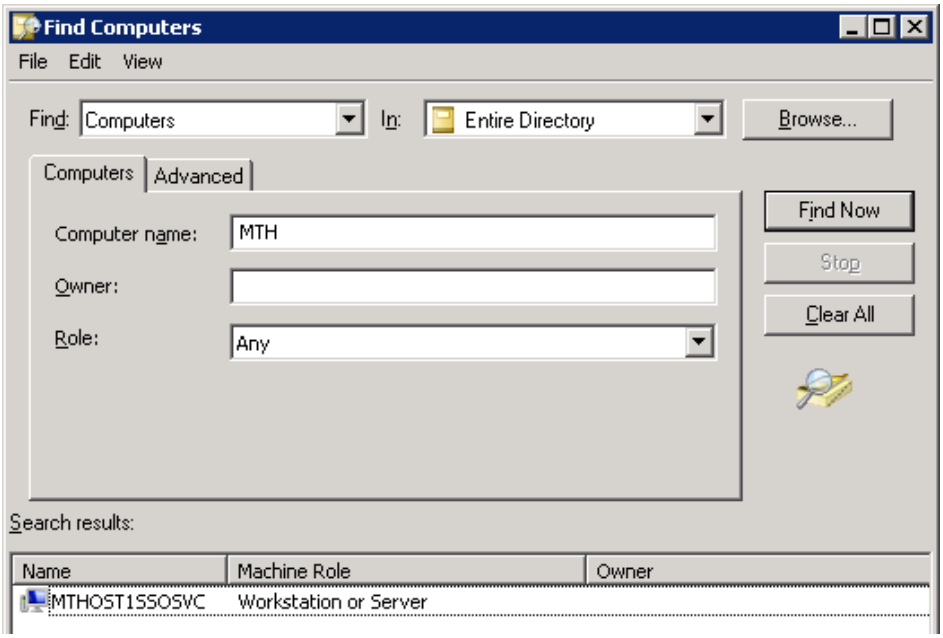
When installed, start ADSI Edit. Expand the computers. Find your new computer account. Right click on the computer name. Select Reset Password.

Service (Computer) accounts :: Verifying the accounts exist

Here are the steps to verify the accounts exist and have been created as a computer account. On a Windows machine copy the following text onto the Run box or a command prompt.

```
%SystemRoot%\SYSTEM32\rundll32.exe dsquery,OpenQueryWindow
```

The following dialog will appear. Select **Computers** from the **Find** menu. From here you can type the service account.



Configuring SSO Plugin with the new service account

Once the SSO Plugin files have been copied to the machine, the Java web server has been restarted. Browse to
BMC Mid Tier: http://loadBalancer/arsys/jss-sso/index.jsp
HP Web Tier: http://loadBalancer/webtier/jss-sso/index.jsp
Fill in the new details. Example screenshot below.