

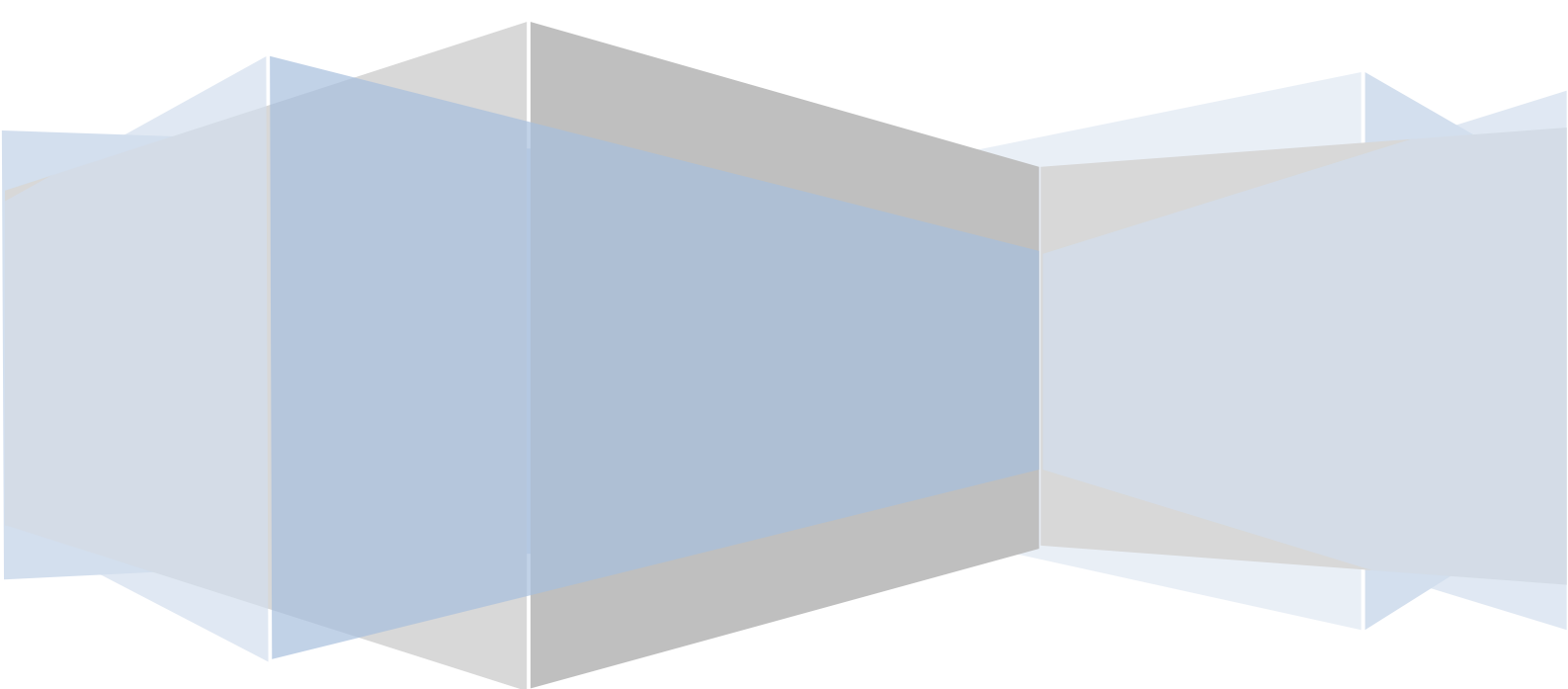
SSO Plug-in

Midtier built-in AD integration installation video commentary

J System Solutions

<http://www.javasystemsolutions.com>

Version 3.3



Copying files to Midtier

Welcome to the Java System Solutions SSO Plugin installation video walkthrough.

Having installed the JSS SSO AREA plugin on the AR System server, we can proceed to set up single-sign-on on the Mid Tier.

We start by copying the contents of 'mt' into the Mid Tier Program Files directory. Only new files are dropped into place here; nothing is overwritten. Then we restart Mid Tier and navigate to the SSO Plugin configuration page.

This video details configuration for SSO Plugin's built-in Active Directory single-sign-on support. The configuration steps will be slightly different for other types of SSO integration such as OpenID, RSA, Siteminder, Common Access Cards or other client-side certificates; see the documentation for details. In particular if you're planning to use IIS with Integrated Windows Authentication as a front-end to Mid Tier, then see the separate video walkthrough entitled "Configuring IIS and SSO Plugin".

Interface walkthrough

The SSO Plugin administration interface can be accessed using the same login as for the rest of the Mid Tier admin site. Proceed to the 'Configuration' link to see the range of options.

The left-hand column of the configuration page allows the basic type of SSO deployment to be chosen and set up.

The right-hand column provides extended options for mapping SSO user accounts to AR System User form entries. There are in-depth options here to find users by searching the User form with AR System queries, which can be used for more complicated mapping requirements, typically for companies with multiple domains or customised user schemas. But the default setting of 'ignore case' and 'strip domain' is normally appropriate for Active Directory users - especially where the BMC AREA LDAP plugin is already in use. SSO Plugin can be used concurrently with the BMC AREA LDAP plugin, or, for simplicity, can completely replace it.

There are also options to deal with users who don't have an entry in the User form yet. They can be returned to the standard non-SSO login page, an ITSM incident can be raised, or a Userform entry can be created automatically for them.

Service account setup

The pre-requisite for a built-in Active Directory integration is that a service account needs to be created in the domain for SSO Plugin to use. The trick is that, for NTLM authentication, the account has to be a Computer account and not a normal User account. And whilst it's possible to create a Computer account manually, Windows currently provides no manual interface to set up a password for it. So we provide a simple setup script to take care of it: this should be run on a machine inside the domain, by a domain administrator.

The script will suggest the current domain and a default service user name with a randomised strong password. You can change these details if you like; here, we'll use a weak password for demonstration purposes. For Kerberos authentication, we now need to set up the Service Principal Name or SPN property on the account, which map hostnames seen by web browsers to the service user we just created. The script suggests the current server name, which might not be what you want. In that case, replace the suggested value with the list of hostnames end-users will be using to access the site. The script will ensure that there are no clashes in SPN names automatically.

Configuring the Midtier

Now we can set up the Mid Tier SSO plugin. Under the Active Directory authentication type, we need to identify the Domain Controller with which the plugin will communicate, the domain it's controller for, and the username and password of the service account we just created. The DC name must be a fully-qualified hostname (not an IP address) and the Windows domain should be the fully-qualified domain name. Here, localdomain.local for demonstration purposes; if you're not sure what your fully-qualified domain name is, use the 'net config workstation' command to list it.

The first time you set the configuration, SSO Plugin will enable itself by making automatic patches to the Mid Tier configuration file. This is a safely reversible process, but it means for it to take effect you'll have to restart the JEE server, typically Tomcat, as prompted. After restarting, return to the SSO status page and the plugin reports it is running.

Testing the integration

Now we can test SSO on the Mid Tier. Note that for Kerberos and NTLM to work on any site, the web browser must be configured to allow them. In IE this is done by putting the hostname used to access the site in the "Local Intranet Zone". Check that the SSO Status page is indeed being accessed

in that zone before continuing. If it's not, you'll need to configure the browser security zone options. Normally, group policy should roll out suitable Intranet Zone settings throughout the company, but you may find it not set up on server or test machines.

Now click the 'Test SSO' link. If there are any problems with the SSO setup, this will detect them. In this case we're the Windows user Administrator, and there's a User form entry called Administrator with the blank password required by AR System SSO, so the login proceeds successfully. And indeed, going to the Mid Tier home page link, we are logged into AR System as administrator without typing passwords.

That completes the walkthrough of a typical SSO Plugin installation. As you can see, SSO Plugin is quick and simple to install and configure, but also offers many advanced configuration options. For details of some of these see the 'features and function' video walkthrough.

Thank you for watching this video walkthrough, and if you have any feedback on improving SSO Plugin for your organisation's requirements, please do get in touch.