SSO Plugin

Release notes

J System Solutions

http://www.javasystemsolutions.com

Version 4.0

What's new

We are pleased to announce the next major release of the JSS SSO Plugin, the industry standard SSO implementation for BMC and HP products, featuring new integrations and enhanced existing functionality.

This document presents the notable changes and key bug fixes to the SSO Plugin.

Java support

The minimum version of Java supported by SSO Plugin is 1.6. Previous versions supported Java 1.5, a version that Oracle had stopped supporting a long time ago.

This also means that HP Service Manager 7.1 can not be supported, but we will continue to support this version of Service Manager with SSO Plugin 3.6.

Improved user interface

The SSO Plugin configuration interface has been re-written and includes the following changes:

- The Built-in Active Directory integration type has been renamed Integrated Windows Authentication (IWA). The integration with Active Directory had become far too complicated, with three different ways of achieving it. There is now just one and when deployed to a Windows platform, SSO Plugin will automatically detect and enable IWA.
- The X509/client certificates support is now configured via an integration type, rather than being automatically detected through Generic, because this allows the product to more easily adapt to customer feature requests specific to X509.
- The configuration page has been split in two, with the SSO integrations and related options moved to a new Integrations page.

Hostname based integrations

Some organisations wish to use a single Java web server (ie running BMC Mid Tier or HP Web Tier) to integrate with different SSO systems, whether in the same organisation or to external third party organisations.

For example, a Multi-Service Provider may be providing a BMC ITSM service to three different organisations, with a shared pool of Mid Tiers for those organisations. Yet each organisation runs its own SSO system.

This release of SSO Plugin allows integrations to be mapped to the URL that a user types into a web browser, ie a user who types in http://mycorp.outsourcer.com/arsys can be integrated with MyCorp's SAML Identity Provider, and a user who types http://bigbusiness.outsourcer.com/arsys can be integrated with BigBusiness's Integrated Windows Authentication service (ie Active Directory).

The key to this service is the hostname, ie configuring a SAML integration with mycorp.outsourcer.com and an IWA integration with bigbusiness.outsourcer.com.

Client IP and hostname restrictions

For any given integration, client IP and hostname restrictions can be applied. When a client does not fall into the configured IP and/or hostname restriction, they are sent to the login page.

Exclusions for automatically SSO enable users

The automatically SSO enable users feature is popular for administrators who do not wish to worry about whether a user's account is SSO enabled, ie setting a blank password in BMC AR System.

However, some administrators reported that it would be helpful to exclude some users from this feature.

Therefore, one or more groups can be configured for exclusion from this feature. If a user is in a defined group, their account will not take part in the automatic SSO enable process.

This does not affect the exclusion for administrators that still applies.

Improved login page to HP Service Manager

In previous versions of SSO Plugin, the Service Manager login page for Integrated Windows Authentication and LDAP was separate to the SM native login page (ie the one supplied by HP). Whilst, BMC AR System users enjoyed a combined login page, with a radio button allowing them to switch between an AR System and IWA/LDAP login.

The combined login page is now supported for Service Manager.

Integration with BMC Analytics, BMC Dashboards and SAP Business Objects

The integration with these products includes automatic management of the user repository by replicating both the BMC and HP user and group configuration.

This feature is a big differentiator between SSO Plugin and rival solutions, however the method of configuring the group mappings between ITSM and the third party product was not ideal.

This release of SSO Plugin includes an easy to edit configuration file to define group mappings.

The file is called jss-ssoplugin-groupmapping.properties and is located on the classpath of the third party application, ie for SAP Business Objects and BMC Analytics, tomcat/webapps/InfoViewApp/WEB-INF/classes.

The file is a list of mappings in the format ITSM group = BOXI group(s), ie.

```
Administrator=Administrators
Asset Config=Administrators
Asset Master=Supervisor, Service Delivery Manager, Service Support Manager
Business Manager=Supervisor, Service Request Manager, Service Support
Manager
```

This functionality is available to all applications integrated with SSO Plugin using the Identity Federation Service.

Native RSA SecurID support

This version of SSO Plugin includes a new integration to the RSA SecurID service. The SecurID 'change token value' is also supported, including policy server settings such as min/max/force alphanumeric PIN, etc.

This feature is easily configurable via the SSO Plugin configuration interface, where the path to the SecurID 'SD configuration file' is provided. The RSA SecurID agent jar file and other appropriate files need to be installed within the webserver too.

Given this feature is new and each SecurID deployment is different in some way, JSS will provide testing/installation support for customers interested in such a deployment.

Central Authentication Service (CAS)

This version of SSO Plugin includes a new integration to the Central Authentication Service (CAS) system, popular on University campuses.

This feature is easily configurable via the SSO Plugin configuration interface, with just the URL of the CAS service required.

LDAP authentication

The LDAP module has been improved to set the SSO username to the value of any attribute from the matched LDAP record.

For example, if using Active Directory, this allows users to login with their Active Directory credentials, and the 'mail' attribute containing their email address to be set as the SSO username.

Alias username by LDAP

This new feature allows SSO Plugin to look up an alternative identifier given the SSO username from a third party LDAP.

For example, this allows an Integrated Windows Authentication implementation, which returns a Windows username, to be mapped to a user's email address held in the Active Directory.

Other use cases include looking up a US Department of Defence EDIPI number from an LDAP when a user authenticates using a Common Access Card.

Upgrades for existing customers

The release is available at no cost to customers that are enjoying our support service. Simply download the product and consult the installation manual for upgrade steps, or contact JSS support for assistance.

Please note that new licenses are required with this release and they can be generated using the JSS licensing tool.