SSO Plugin

Installation for HP Service Manager

J System Solutions

http://www.javasystemsolutions.com

Version 3.5

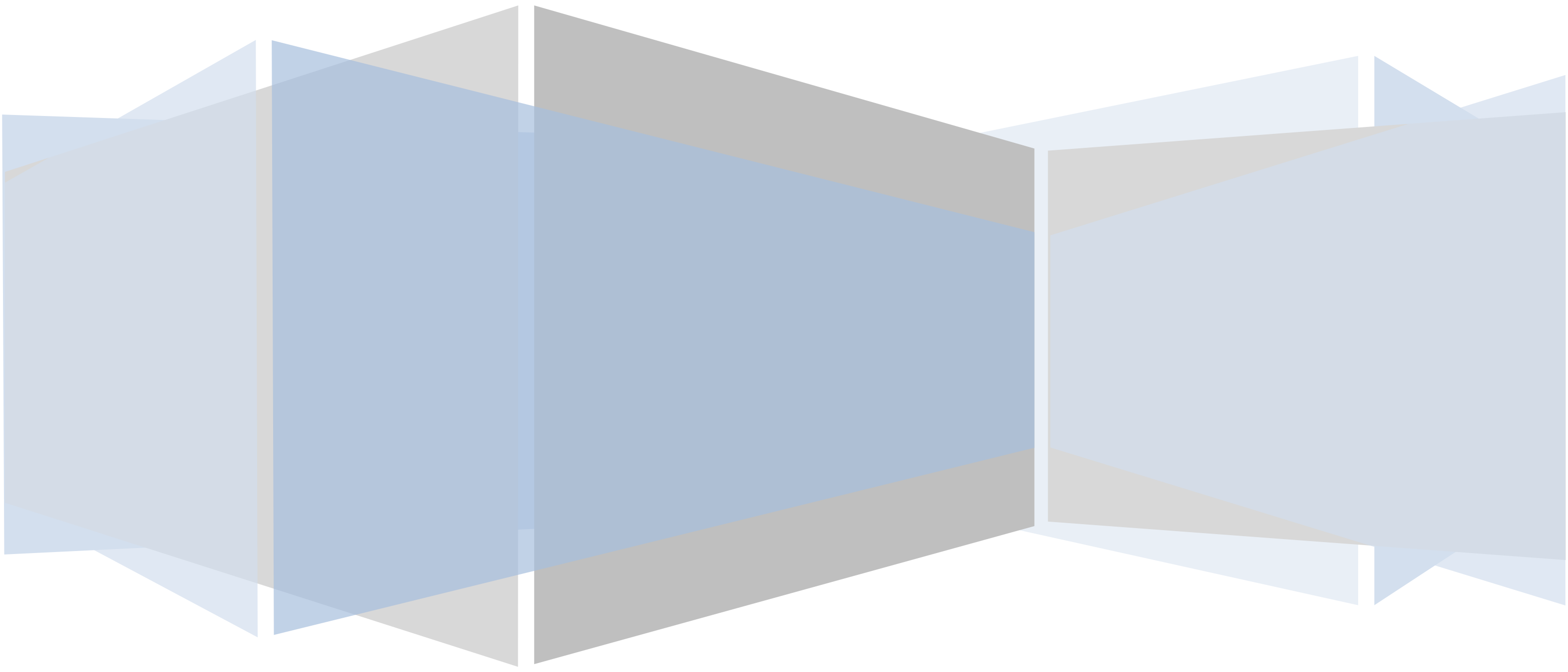


Table of Contents

Introduction

This document covers:

- Compatibility matrix and other introductory material for SSO Plugin.
- Installation and configuration of SSO Plugin for HP Service Manager 9.2+.
- Upgrading from previous versions.

Separate documents are available for other components, ie JasperServer Reports, SAP Business Objects XI, BMC Dashboards, BMC Analytics.

The JSS support website can be found here:

http://www.javasystemsolutions.com/jss/support

Version numbering and new features

The product is marked as version 3.5 because this is the current release of SSO Plugin for other platforms. Whilst the HP Service Manager is a new implementation, the underlying technology is stable, secure and in production use at many global organisations.

It is anticipated that features currently available for BMC AR System, but not included in the HP Service Manager build, will be available in a subsequent release. Whilst only a few features are missing, most notably the functionality to automatically raise an incident when a user has no SSO access to HP Service Manger, if any are of particular importance to an organisation then please contact JSS so we can prioritise development accordingly.

Compatibility

The product has been developed for Service Manager 7.1+ and will run on all platforms.

There are additional installation steps for SM 9.3 due to a change in the way SSO is enabled on the Service Manager server component (discussed in the enabling trusted sign on section).

Please note:

1. We support Tomcat 5.5+, Weblogic 11g+ and Websphere. If you use another Java servlet engine, please contact us to confirm supportability.

The SSO Plugin will support many different URL protection products and methods. Popular products include:

Authentication Systems						
RSA Access Manager (ClearTrust)	CA SiteMinder	Quest QSJ	HTTP Basic	Novell Access Manager	OpenID	X509 client certificates

The SSO Plugin also provides a full Integrated Windows Authentication implementation (ie Kerberos and NTLMv2) out of the box.

Java compatibility

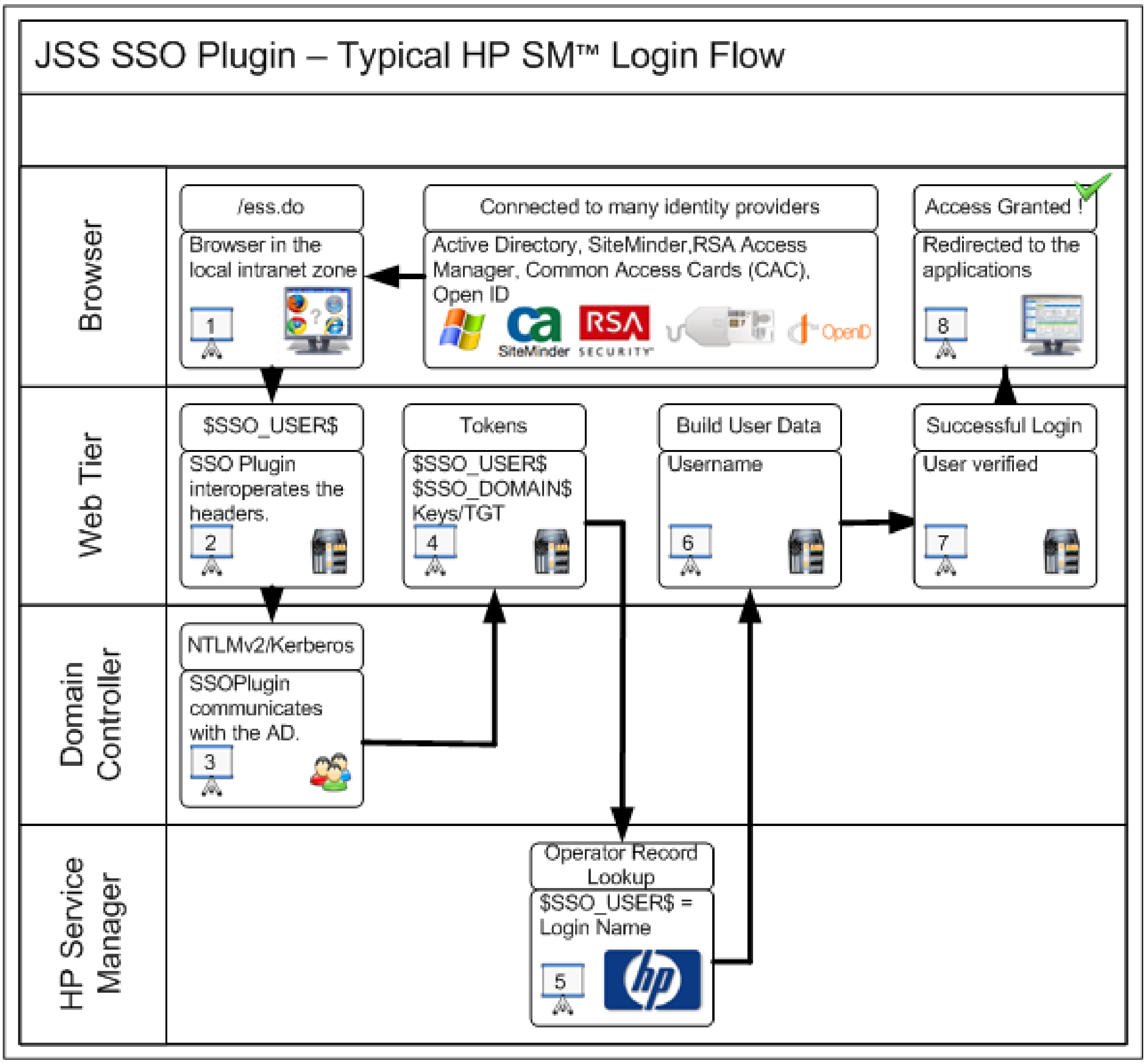
The Web Tier for Service Manager 7.1 requires Java 1.5 and SSO Plugin is supported on version 1.5 update 7 or greater, however we recommend the latest (and final) version of 1.5 which is 1.5 update 22.

The Web Tier for Service Manager 9.2+ runs on Java 1.6.

Overview of the SSO Plugin

The SSO Plugin is invoked by the SM when a user goes to /index.do (support console) or /ess.do (self service console).

If the relevant details were available on the incoming request for the SSO Plugin to operate correctly, then these details are passed back to the SM. SSO Plugin also ensures users have access to SM before proceeding with an SSO login, which includes checking they are not a self service user trying to access the support console.


JSS SSO Plugin – Typical HP SM™ Login Flow
Browser
Web Tier
Domain Controller
HP Service Manager
/ess.do
Browser in the local intranet zone
1
Connected to many identity providers
Active Directory, SiteMinder,RSA Access Manager, Common Access Cards (CAC), Open ID
SiteMinder
RSA SECURITY
OpenID
Access Granted !
Redirected to the applications
8
SSO_USER
SSO Plugin interoperates the headers.
2
Tokens
SSO_USER
SSO_DOMAIN
Keys/TGT
4
Build User Data
Username
6
Successful Login
User verified
7
NTLMv2/Kerberos
SSOPlugin communicates with the AD.
3
Operator Record Lookup
SSO_USER = Login Name
5

Installation

To install the SSO Plugin for Service Manager, there are two steps:

1. Configuring the Service Manager server component.
2. Configuring the Web Tier component.

Configuring the Service Manager server component

There are two steps required to set up the SM server component:

1. Enable trusted sign on.
2. Modify the Operator webservice, to allow SSO Plugin running in Web Tier to interact with the Operator table.

Enabling trusted sign on

While HP provide comprehensive documentation on how this is achieved, there are two ways in which this can be achieved: With and without creating client certs.

Creating client certs involves setting up SSL certificates for each component and is a long process. This is discussed in a document available from HP titled *SM7_Single Sign-On Authentication.pdf.*

The quickest solution is to enable trusted sign-on without client certs, which simply involves opening the sm.ini file (typically found in c:\Program files\HP\Service Manager\Server\RUN) and adding the following line:

```
trustedsignon:1
```

This has been tested in SM 9.2x, however in SM 9.3, HP modified the server component so client certs had to be enabled. The HP SM configuration guide must be followed to enable client certs and JSS are happy to guide you through the process.

We have asked HP to revert this change to give users the option of not using client certs, speeding up proof of concept installations. The enhancement request is QCCR1E68951.

Once this has been set, restart the SM server component.

Disabling Operator LDAP

If you have LDAP enabled with a mapping to the Operator table, delete the mapping from the LDAP mappings. This is because trusted sign on does not appear reliable with the LDAP integration, and SSO Plugin provides the ability for users to authenticate against a Windows domain controller once SSO has been enabled, so the Operator LDAP integration becomes redundant for most deployments.

Please ensure the following is present in sm.ini:

```
ldapdisable:1
```

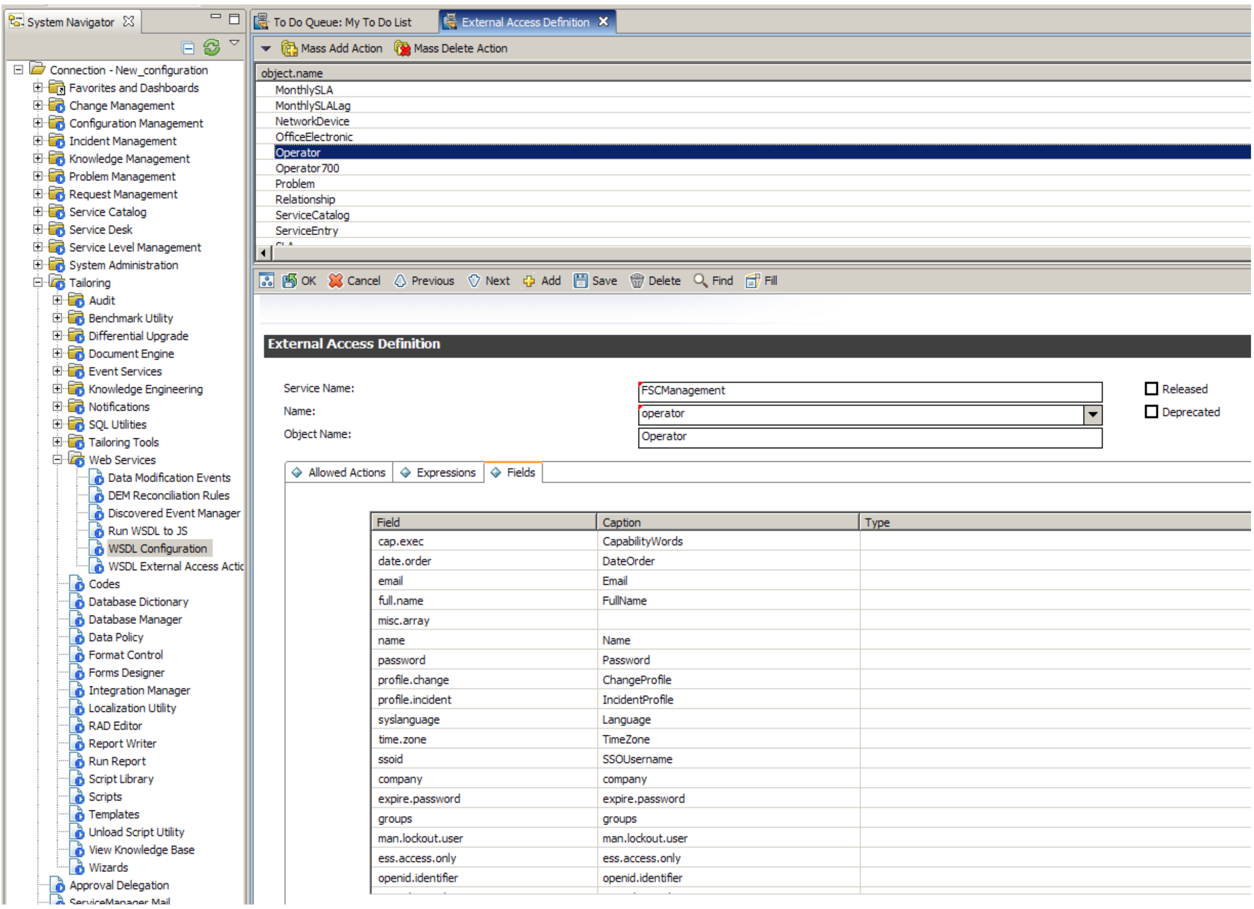
Modifying the Operator webservice

SSO Plugin uses the webservice interface to perform queries against the Operator table, however the default webservice definition does not expose all the required fields.

1. Locate the Operator web service in the WSDL configuration (Tailoring → Webservices → WSDL Configuration), select operator in the name drop down field and press search.
2. Select the Operator (not Operator.700) object and expose the following fields:

1. company
2. expire.password
3. groups
4. man.lockout.user
5. ess.access.only
6. login.revoked

The following screenshot shows the operator webservice configuration. Adding extra fields is performed through Tailoring → Forms designer → operator.g form.



object.name
MonthlySLA
MonthlySLALag
NetworkDevice
OfficeElectronic
Operator
Operator700
Problem
Relationship
ServiceCatalog
ServiceEntry

External Access Definition

Service Name: FSCManagement

Name: operator

Object Name: Operator

□ Released

□ Deprecated

Field	Caption	Type
cap.exec	CapabilityWords	
date.order	DateOrder	
email	Email	
full.name	FullName	
misc.array		
name	Name	
password	Password	
profile.change	ChangeProfile	
profile.incident	IncidentProfile	
syslanguage	Language	
time.zone	TimeZone	
ssoid	SSOUsername	
company	company	
expire.password	expire.password	
groups	groups	
man.lockout.user	man.lockout.user	
ess.access.only	ess.access.only	
openid.identifier	openid.identifier	

Please note, there are three extra fields that can be added to the Operator form that may also be added for additional SSO Plugin functionality:

- ssoid: For supporting user aliasing.
- openid.provider and openid.identifier: For integrating with an OpenID provider such as Google Mail).

These fields are not required for SSO Plugin to perform a standard set of operations that are required by most users. The extra fields are only required for advanced configurations, the most common being user aliasing: mapping an SSO ID to a different Operator login name.

Installing the Web Tier component

A separate highly detailed JSS document (“Configuring Mid Tier and Web Tier”) explains how to configure SSO Plugin for Web Tier, with details on the integration process between SSO Plugin and third party SSO providers (such as Active Directory). This section only covers the installation process.

To install the SSO Plugin on the Web Tier, please follow these steps:

1. Copy the contents of the webtier directory from the installation files into the root Web Tier directory. i.e. the contents of webtier into the Web Tier directory that *contains* the WEB-INF directory. If asked to confirm overwriting of files, click yes: SSO Plugin only adds to the files.
2. For Service Manager version 9.21 or greater, a manual change must be made to the Web Tier configuration file to enable third party files to be run.
    1. Locate the Web Tier application-context.xml file in the WEB-INF/classes directory.
    2. Add the text in bold to the file, the non-bold area can be found at approximately line 30:

```
/loginpreload.jsp=#NONE#
/jss-sso/**/*.jsp=#NONE#
/**/*.jsp=resourceFilter
/*.jsp=resourceFilter
/**=httpSessionContextIntegrationFilter,anonymousProcessingFilter
```

3. Restart Web Tier.
4. If you are using IBM Websphere 7, use WAS to ensure the com.ibm.ws.jsp.jdkSourceLevel custom property is set to 16 on the web extension file or the custom WebContainer. This tells Websphere that the application was compiled for Java 1.6+.
5. Go to the SSO Plugin status page by pointing your browser at http://host/webtier/jss-sso/index.jsp. You will be presented with a status page.
6. Locate the document titled Configuring Web Tier to configure the SSO Plugin.
7. If SSO fails then review the troubleshooting document or contact JSS support.

Licensing

The product is supplied with a two month evaluation license, applied during the web based configuration process. If you choose to purchase SSO Plugin, a permanent license can be generated through the JSS website. If your trial license expires, please contact JSS for a new one.

Upgrades

Assuming SSO Plugin is installed and working, or at least configurable, the steps are as follows:

1. Stop Tomcat.
2. Replace the Web Tier files, ie copy the contents of the webtier directory into the Web Tier directory in the Tomcat webapps directory.
3. Delete the Tomcat 'work' directory, which is a temporary cache directory re-created when Tomcat starts.
4. Start Tomcat.
5. Go to the Web Tier SSO configuration, check it is still correct and press 'set configuration'.

Upgrading integrations to SAP Business Objects and Jasper Reports.

The deployment mechanism of these applications rarely change but we recommend copying the relevant jar files from the installation files to the third party application.

For example, copy the jar files in businessobjects/WEB-INF/lib (from the installation files) to the relevant location in the Business Objects installation, as per the original deployment.