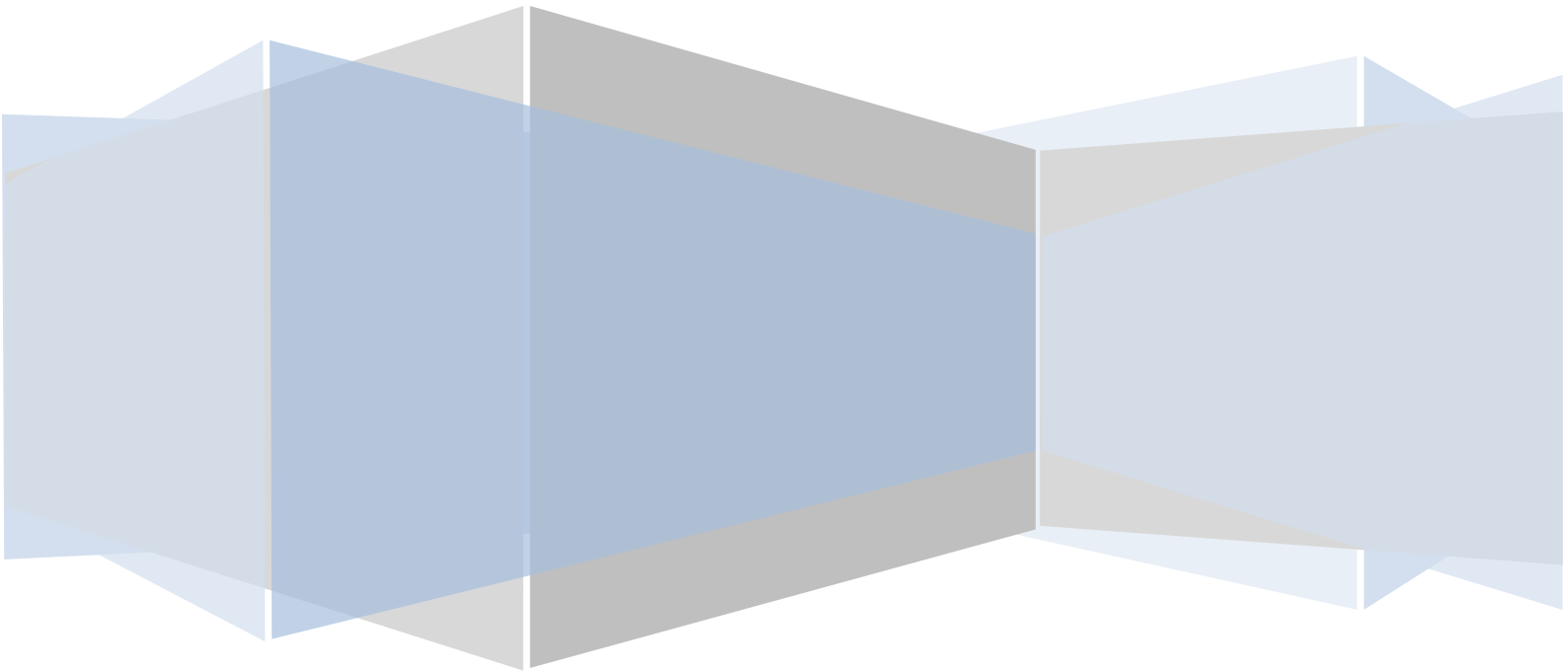
SSO Plugin

HP Service Request Catalog

J System Solutions

http://www.javasystemsolutions.com

Version 4.0



Introduction

SSO Plugin can be deployed to SRC in two ways:

1. An integrated module with no third party dependency,
2. A service connected to an existing SSO Plugin instance deployed to HP Service Manager (Web Tier) or the SSO Plugin Authentication Service using the SSO Plugin "Identity Federation Service".

The reason we provide two models is because of an issue with Adobe Flash and NTLM (discussed below) and also to support SSO Plugin's user aliasing feature.

For option 1, deploying SSO Plugin as an integrated module to SRC, see the SSO Plugin Authentication Service installation guide.

This document explains how to deploy option 2, but some instructions in the SSO Plugin Authentication Service installation guide will be referenced.

Adobe Flash and NTLM

There is a bug in the Adobe Flash plugin that can cause uploads to fail in some circumstances. This has been reported to Adobe through one of their forum, and a bug report does exist, but there does not appear to be any movement in resolving the issue.

To work around this problem, option 2 above is deployed with the HP Web Tier must be configured against a different hostname to the SRC component. For example, you may wish to configure:

1. http://servicemanager.mycompany.com -> Web Tier
2. http://src.mycompany.com -> SRC

It does not matter what hostnames you configure but they must be different.

Enabling the identity federation service

This service is used to allow an SSO Plugin enabled Web Tier or Authentication Service to authenticate other products that have been SSO enabled with SSO Plugin. In this case, SRC is the product that will be sending requests to Web Tier or the Authentication Service for authentication.

The identity federation service isn't enabled by default. To enable it, go to the SSO Plugin configuration page and click "Enable identity federation service". The following fields must also be set.

Federation key

This is known only to the SSO Plugin and the third party applications that are integrating with the SSO Plugin. It is used as a seed to a hashing function that allows the identity federation service and acceptor to trust each other.

Token lifetime

When a user has been authenticated, the JSS identity federation acceptor sets a cookie (with the name jss-ssoplugin). The cookie contains an encoded token that includes the logged in user. The cookie is set to expire after a period of time that is calculated to be the time at which the user was authenticated with SSO Plugin, plus the value defined in this field.

Typically, a value of one day will ensure every client has to re-authenticate with SSO Plugin once a day.

Enabling Service Request Catalog

There are two parts to this process: Copying a jar file to SRC and updating a number of files within the SRC installation.

Prior to performing the steps, stop the Java web server (ie Tomcat) instance running Service Request Catalog. When the steps have been completed, start it again.

Copying files to SRC

Locate the jss-sso-thirdparty.jar file in the src directory within the SSO Plugin installation set. Copy it to the SRC WEB-INF/lib directory, found in the SRC program directory (ie tomcat/webapps/src/WEB-INF/lib).

Updating the web.xml file

Locate the SRC web.xml file, found in the SRC program directory (ie tomcat/webapps/src/WEB-INF/web.xml). Make a backup of this file.

Open the file and locate the following:

```
<context-param>
  <param-name>contextClass</param-name>
  <param-value>
com.hp.service.catalog.server.web.context.CustomXmlWebApplicationContext
  </param-value>
</context-param>
```

Locate the web.xml.src.patch file within the installation set src directory. Open it in a text editor, copy it all and paste into the web.xml file placing below the </context-param> specified above in bold.

In the patch you have just applied, locate the following two parameters and set appropriately:

1. **identityFederationServiceURL:** This points to the identity federation service running on the SSO Plugin installation deployed to Web Tier or the Authentication Service.

   The identity federation service URL is /jss-sso/identityfederationservice, relative to the SSO Plugin deployed.

   Therefore, if SSO Plugin is installed on the Web Tier at this URL:

```
http://host:8080/webtier
```

   then the identityFederationServiceURL is:

```
http://host:8080/webtier/jss-sso/identityfederationservice
```

   And an example URL for the SSO Plugin Authentication Service, if you deployed that instead of using a Web Tier, is as follows:

```
http://host:8080/authentication-service/jss-sso/identityfederationservice
```

2. **key:** This must be set to the federated identity key set in the SSO Plugin interface.

The logLevel parameter is optional and controls the amount of logging generated by the identity federation acceptor, the valid values are INFO, DEBUG and TRACE. You are advised to set this to INFO in production.

Configuring SRC to use SSO Plugin

Please refer to the SSO Plugin Authentication Service installation guide. Locate the Configuration for Service Request Catalog and implement the sections Patching application files and enabling manual (no SSO) login.

Testing the integration

When installation is complete, ensure SSO is functioning by visiting the SSO Plugin Test SSO page running on Web Tier or the Authentication Service, ie. http://host/webtier/jss-sso/testsso.jsp or http://host/authentication-service/jss-sso/testsso.jsp.

If the browser can authenticate with the SSO system and a username is deployed, the browser should log into SRC as this username (assuming an account exists in Service Manager).