

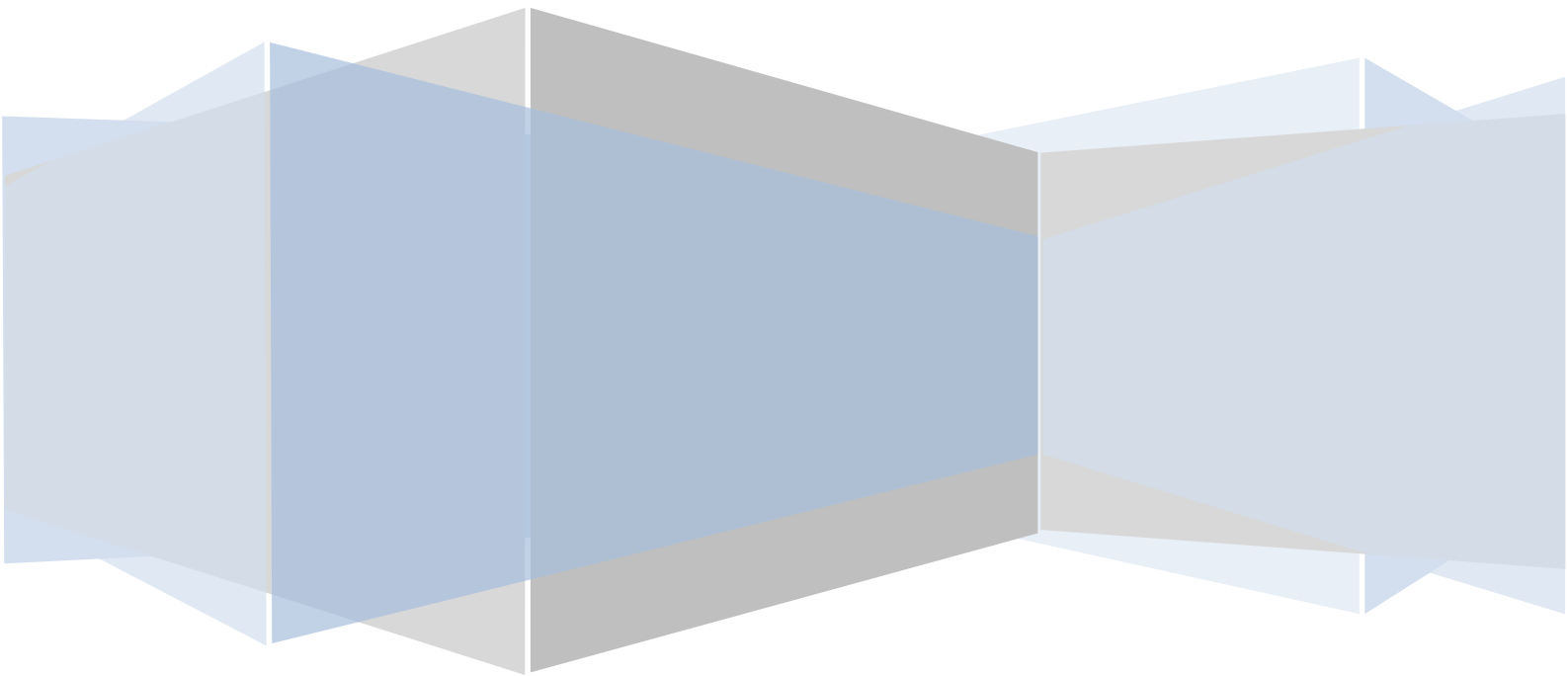
SSO Plug-in

HP Service Manager installation commentary

J System Solutions

<http://www.javasystemsolutions.com>

Version 3.5



Introduction

Welcome to the JSS SSO Plugin for HP Service Manager installation video. Before commencing with the installation, there are a couple of pre-requisite steps.

The first pre-requisite is to ensure that trusted sign on is enabled. This is the SM feature that enables SSO to be installed on the web tier and Service Request Catalog. As you can see, it is enabled and the trusted client certs are also enabled because they are mandatory on SM 9.3. For information on enabling client certs, contact HP or JSS support.

The second pre-requisite is modifying the Operator webservice. This can only be performed by an SM admin user and is documented in the installation guide.

Now we can start the installation process and we will show you how to configure built-in Active Directory authentication, which allows you to sign in using SSO with IE, Firefox and other browsers.

SSO Plugin supports other types of integration too so this installation overview is pertinent to all type so SSO integration.

For built-in Active Directory, we need to create a computer - not user - account in the Active Directory. This is as per Microsoft design. We supply a script to do this called set-service-account and when we run it, we're prompted for the relevant details.

Once complete, locate the Tomcat running Web Tier and the installation files. Copy the contents of the Web Tier directory from the installation files, to the Web Tier directory within Tomcat.

Restart Tomcat and navigate to the SSO Plugin status page - bookmark it now as you will be visiting it regularly.

Login using the default password, jss, and navigate to the setup interface.

Select built-in AD integration and you are presented with four fields: The hostname of an Active Directory, which your AD administrators can tell you, the Windows DNS name and the computer name and password.

To lookup the Windows DNS name, open the command prompt, type 'net config workstation' and use the Windows DNS name.

SSO Plugin requires an SM admin user to perform queries and modifications to the Operator table. The default is falcon with no password.

For the purposes of simplicity, we assume the Operator usernames are the same as the Windows login names. If they are not, a range of options are available to resolve this issue and these are well documented.

To complete the setup, press set configuration.

Navigate to the status page and it will now inform you that SSO is enabled. SSO can now be tested using the Test SSO facility, which causes the browser to perform SSO and reports useful information such as the protocol selected, whether SM can accept an SSO connection for the user (ie does the SSO user exist in SM), etc.

Finally, test SSO by clicking on the Service Manager link. We are signed in without logging in.

If you click logout, you will note the logout page has been replaced and improved to include a range of options for re-accessing Service Manager.

You may also navigate back to the status page and click on Windows Login, which enables you to login using any Active Directory login. This enables the removal of the SM LDAP integration module, further simplifying your SM deployment.