
# Security Service v.0.2.0

**for the Planetary Data System**

**NASA Jet Propulsion Laboratory,**
**California Institute of Technology**

**01 November 2010**

# Table of Contents

# 1.1 Overview

## About Security Service

The Security Service provides the authentication and authorization functions for the PDS 2010 system. The intent of this service is to control access to interfaces and services that require authentication and authorization (e.g., Monitor, Report, Registry interfaces, etc.). The functionality for this service is satisfied by the open source software package OpenAM . OpenAM is the follow-on effort by ForgeRock of the formerly named OpenSSO effort, which was initiated by Sun Microsystems.

Please send comments, change requests and bug reports to the PDS Operator at pds_operator@jpl.nasa.gov.

# 1.2 Release Notes

## Release Notes

The purpose of this section is to provide a description of a Security Service release including any impact that the new or modified capabilities will have on the Discipline Nodes or the PDS user community. If viewing the web-based version of this document, a somewhat itemized list of changes for each release can be found on the Release Changes page.

## Release 0.2.0

This release of the Security Service is a component of the integrated release 1.0.0 of the PDS 2010 System. This release is intended as a prototype release in support of the assessment of the PDS4 standards. The new or modified capabilities for this release are as follows:

- Added support for controlling access to HTTP PUT and DELETE methods.
- Added support for controlling access based on group membership.

The liens for this release are as follows:

- Need to resolve an issue defining policy for multiple HTTP methods on the same URL.
- Need to clean up the user list and define a procedure for synching this list with the personnel entries in the Registry Service.

## Release 0.1.0

This release of the Security Service is a component of the integrated release 0.1.0 of the PDS 2010 System. This release is intended as a prototype release in support of the demonstration at the Management Council Face-to-Face meeting in August 2010. This initial release of the service provides the capability to secure specific URLs for the Registry Service and force requests to those secure URLs to require authentication.

# 1.3 Installation

## Installation

This section describes how to install the OpenAM software package and its associated software packages. These packages serve as the Security Service for the PDS 2010 system. The following topics can be found in this section:

- System Requirements
- Software Installation
- Configuration

Note that much of the documentation and examples for OpenAM still make reference to OpenSSO (the former name of the package under Sun Microsystems).

## System Requirements

The software that makes up this project consists of open source packages that are available for download and installation. The packages and their release versions are as follows:

- OpenAM Release 9
- OpenDS 2.2.0
- J2EE Policy Agent 3.0 for Apache Tomcat

The above software packages require the following software to be installed in the target environment:

- Sun Java Standard Edition (J2SE) 1.6.X
- Apache Tomcat 6.0.20

## Software Installation

The standard installation of the Security Service involves at least two machines. The first machine hosts the OpenAM and OpenDS software. The second machine hosts a service that requires access control (e.g., Registry Service). This machine is where the J2EE Policy Agent will be installed and configured. Perform steps 1 through 3 on the first machine and steps 4 and 5 on the second machine. Once the installation of the software is complete, follow the instructions in the Configuration section to configure the software.

### 1. Install Directory Server

Although the installation of OpenAM includes an installation of a directory server ( OpenDS , within the application server), we are choosing to install one separately so that it is accessible from other applications that require a standard LDAP interface.

- Download the package from http://www.opends.org/promoted-builds/2.2.0/ . There are a couple of options to choose from including the QuickSetup Installer or just downloading the ZIP package.
- Install the package so that it operates on the standard LDAP port 389. The ZIP package provides installation documentation. Additional documentation is available at https://docs.opends.org/2.2/page/InstallingTheDs .
- Startup the server.

#### 2. Install Application Server

Although other application servers are supported (e.g., GlassFish), Apache Tomcat is the preferred application server.

- Download the appropriate binary package for your platform from http://tomcat.apache.org/download-60.cgi .
- Install the package so that it operates on port 80. Documentation can be found in the binary distributions and at http://tomcat.apache.org/tomcat-6.0-doc/ .

  Modify the *$CATALINA_HOME/bin/catalina.sh* file as follows:

```
CATALINA_OPTS="-Xms256m -Xmx1024m"
JAVA_OPTS="-Xmx1024m -XX:MaxPermSize=256m"
```

- Startup the server.

#### 3. Install OpenAM

The OpenAM software is packaged as a Web Archive (WAR) file and ready for deployment to an application server.

- Download the package from http://forgerock.com/downloads.html .
- Deploy the downloaded WAR file to the application server. The application should be accessible from */openam*.

#### 4. Install Service Requiring Access Control

On the second machine, either install or verify installation of the service (e.g., Registry Service) requiring access control on that machine's application server.

### 5. Install J2EE Policy Agent

The J2EE Policy Agent software is specific to the application server where it will be installed.

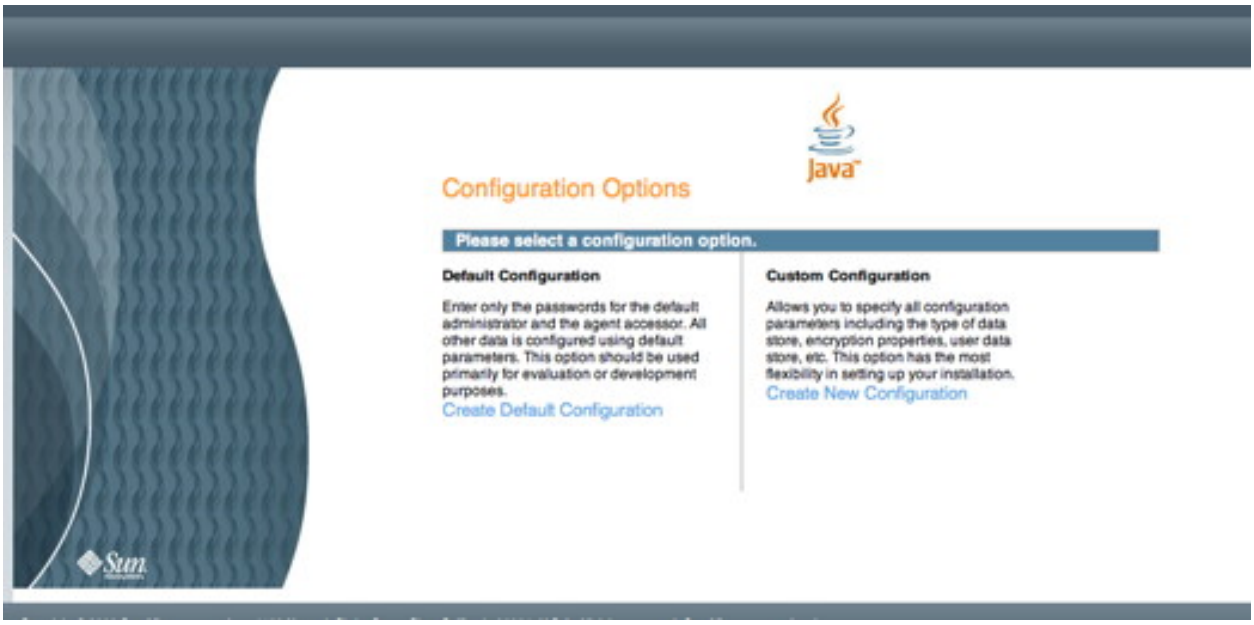
- Shutdown the application server.
- Download the J2EE Policy Agent for your application server from http://forgerock.com/downloads.html .
- Install the J2EE Policy Agent. Documentation (specific to Apache Tomcat 6.0.X) can be found at http://dlc.sun.com/pdf/820-7251/820-7251.pdf . See the Policy Agent Installation section for an example installation. If viewing this document in PDF form, see the appendix for details.
- Startup the application server.

## Configuration

This section details the software and policy configuration of the OpenAM and the J2EE Policy Agent software.

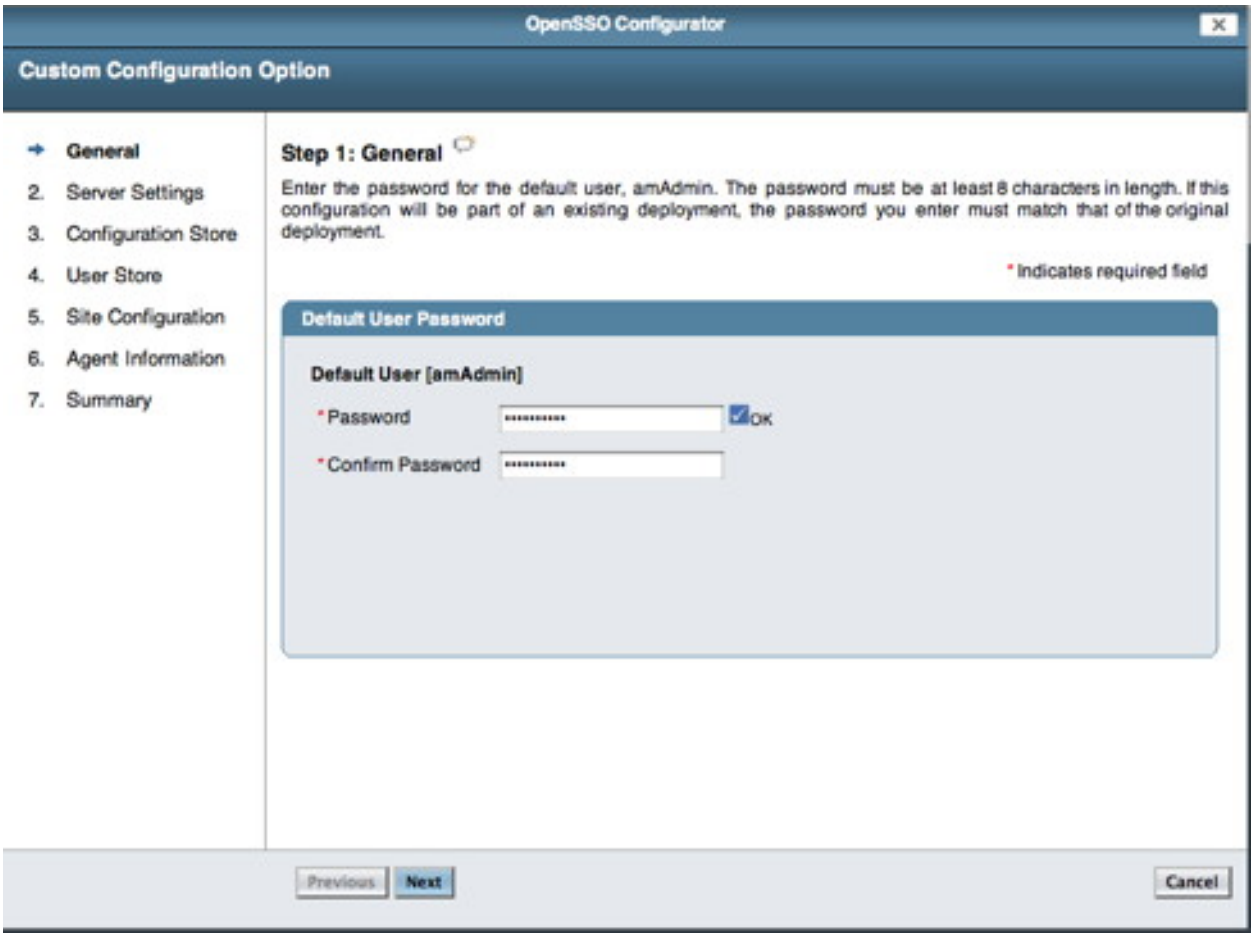
### Software Configuration

Start the configuration by opening your favorite browser (e.g., Firefox, Safari, etc.) and go to the following URL (http://[host[:port]]/openam/), where the *host* and *port* (if other than port 80) values correspond with the application server installation from step 2 above. You should see the following screen in your browser window:



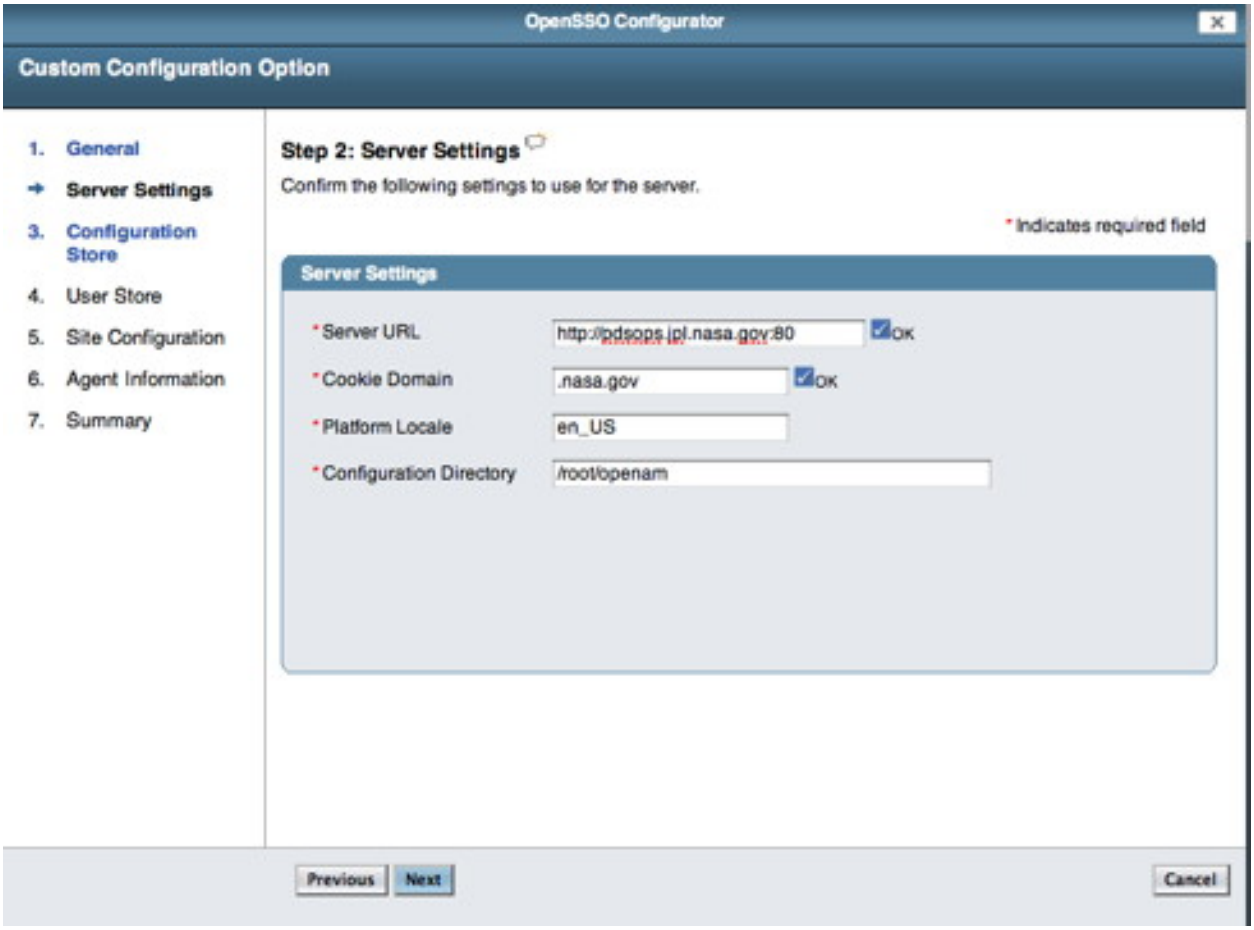

If viewing this document in online form, click the image for a larger version.

Select the *Create New Configuration* link on the screen above. You should see the following screen in your browser window:



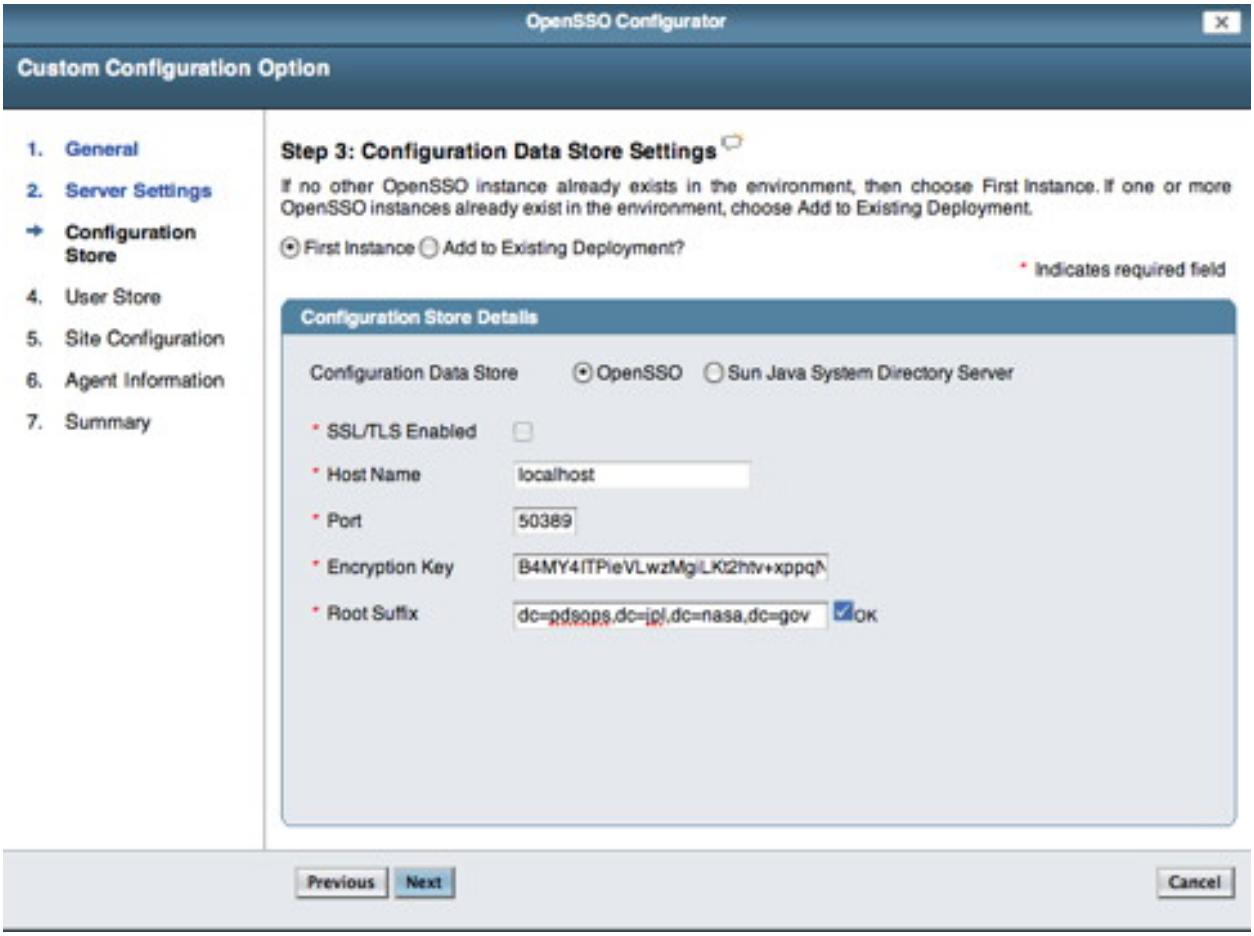

If viewing this document in online form, click the image for a larger version.

Enter a new password for the *amAdmin* account and then select the *Next* button. You should see the following screen in your browser window:



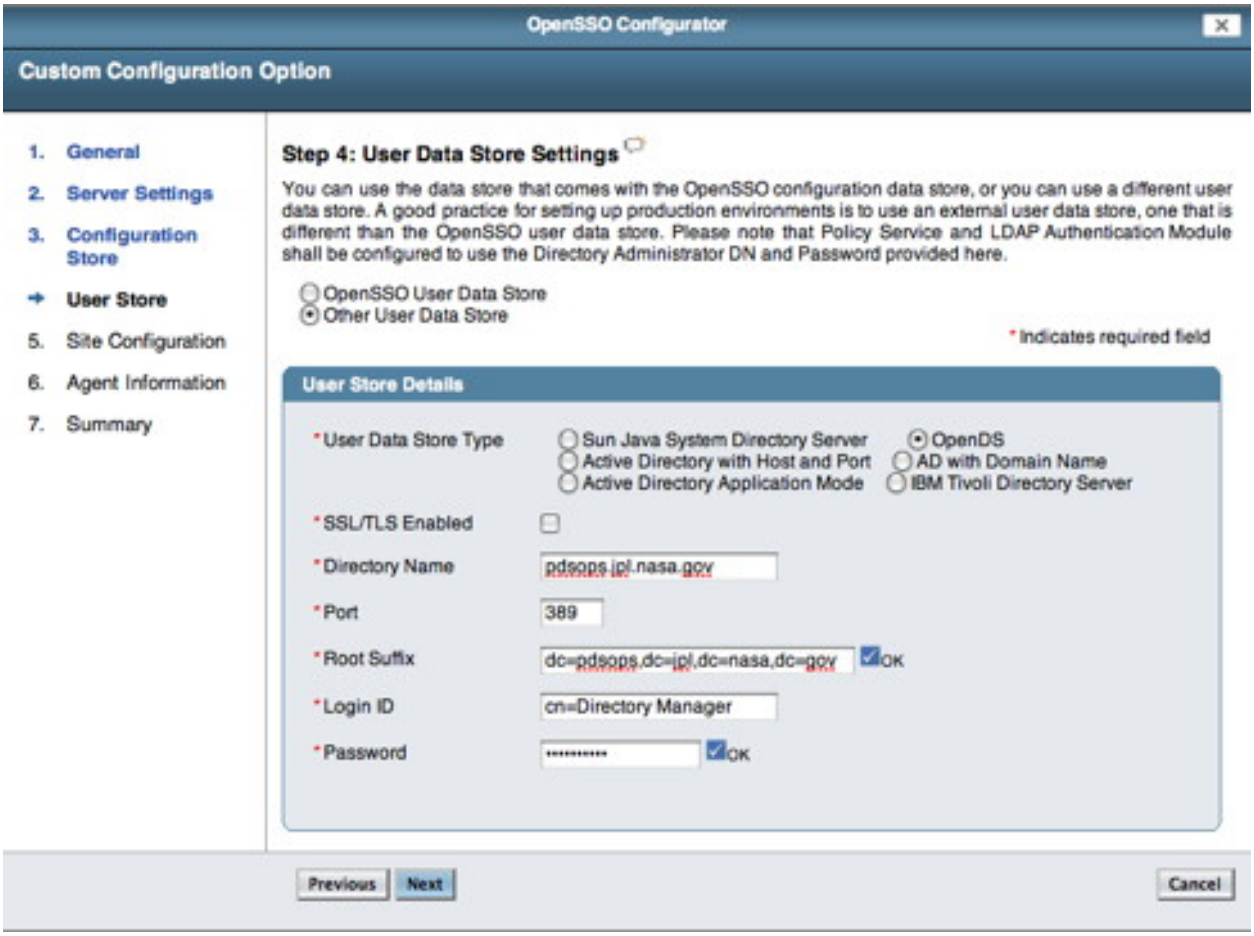

If viewing this document in online form, click the image for a larger version.

Enter the *Server URL* and *Cookie Domain* (e.g., nasa.gov) then select the *Next* button. You should see the following screen in your browser window:



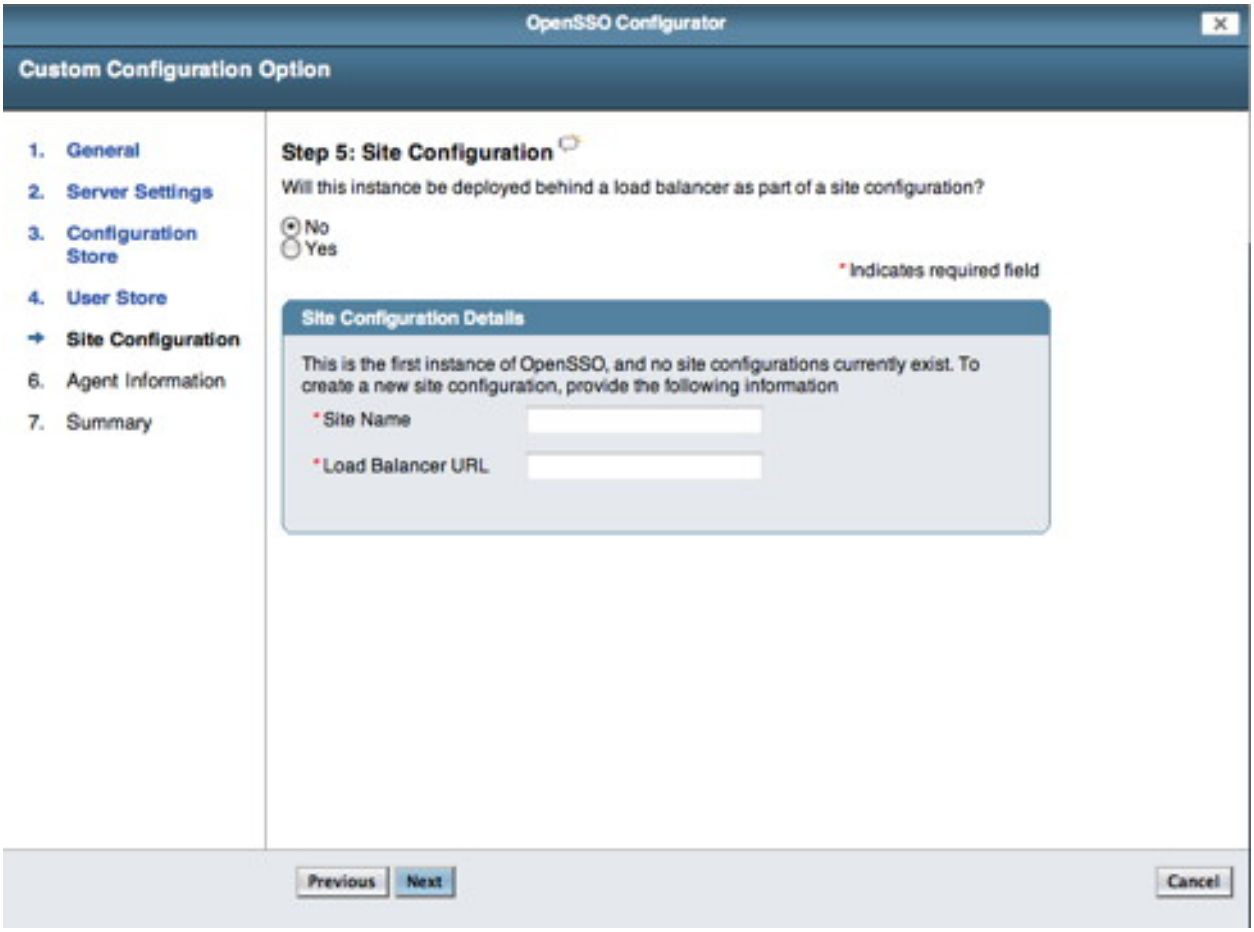

If viewing this document in online form, click the image for a larger version.

Modify the *Root Suffix* with the information from the OpenDS installation (e.g., dc=pdsops,dc=jpl,dc=nasa,dc=gov) then select the *Next* button. You should see the following screen in your browser window:



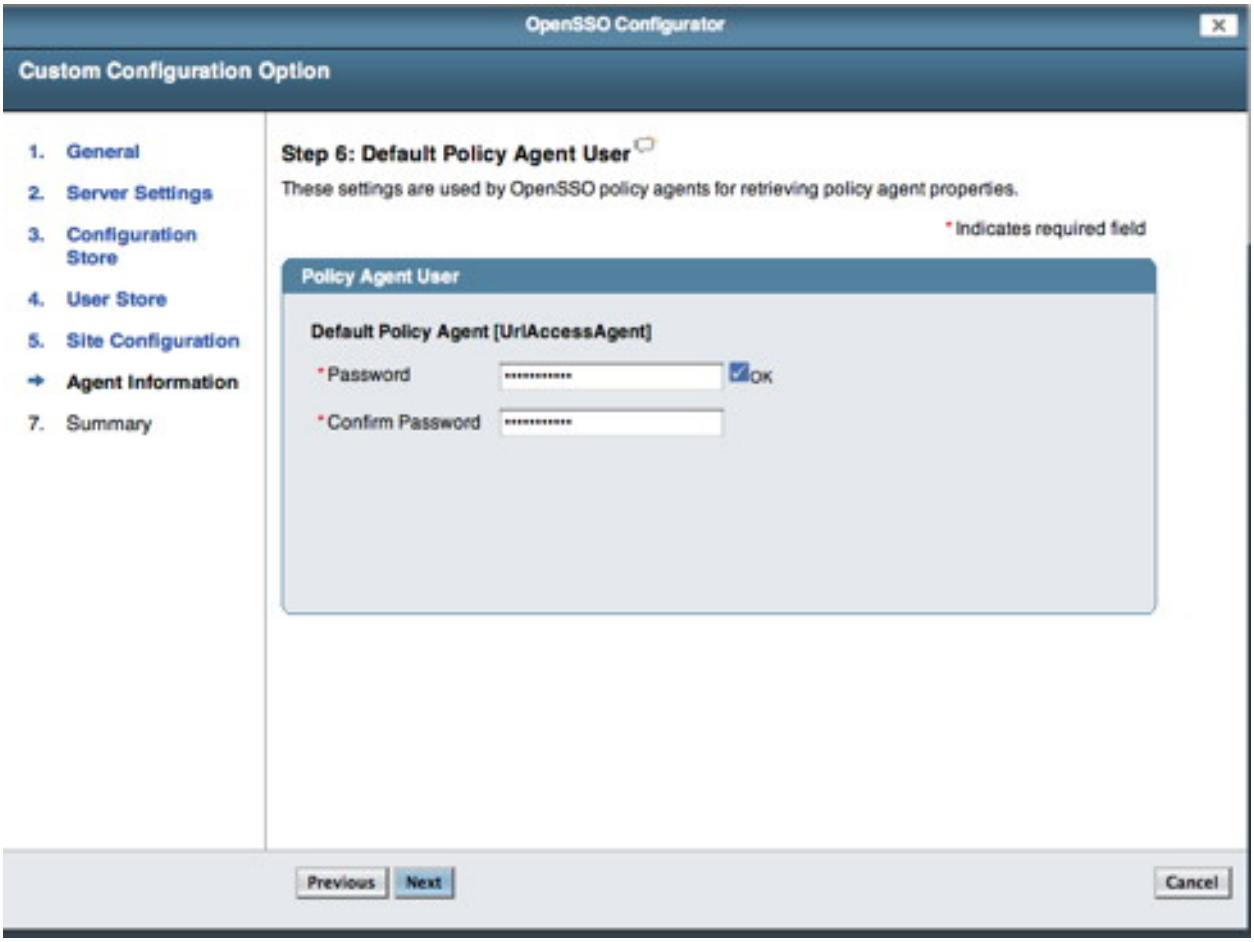

If viewing this document in online form, click the image for a larger version.

Select the *OpenDS* radio button, enter the *Directory Name* (e.g., pdsops.jpl.nasa.gov), *Port* (389), *Root Suffix* (e.g., dc=pdsops,dc=jpl,dc=nasa,dc=gov), *Login ID* (cn=Directory Manager) and *Password* for the OpenDS installation then select the *Next* button. You should see the following screen in your browser window:



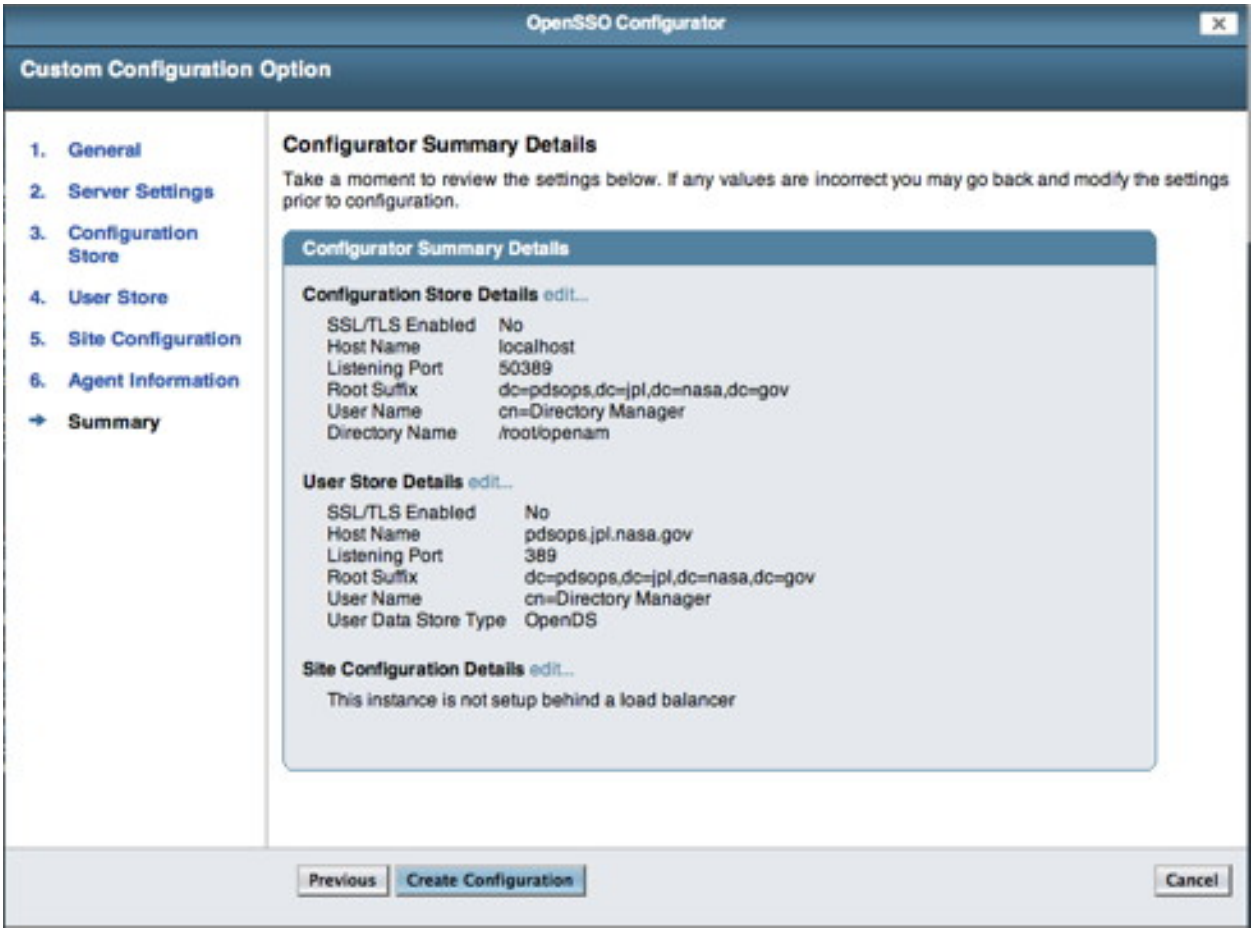

If viewing this document in online form, click the image for a larger version.

Select the *No* radio button then select the *Next* button. You should see the following screen in your browser window:



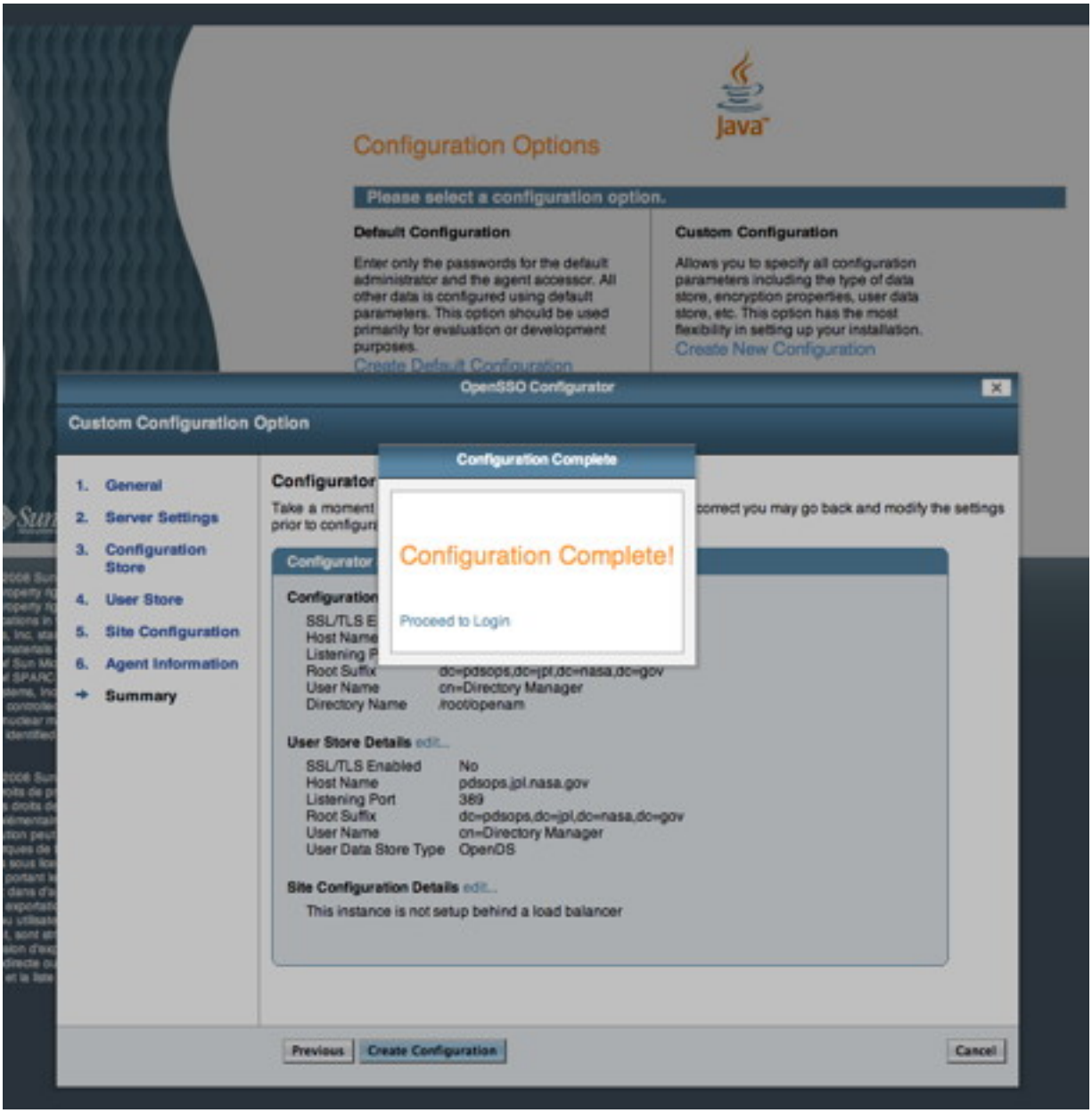

If viewing this document in online form, click the image for a larger version.

Enter a new *Password* for the Policy Agent then select the *Next* button. You should see the following screen in your browser window:




If viewing this document in online form, click the image for a larger version.

Assuming the information is correct, select the *Create Configuration* button. If no error messages are displayed you should see the following screen in your browser window indicating successful completion:



If viewing this document in online form, click the image for a larger version.

### Directory Server Configuration

With the software configuration is complete it is time to add groups and users to the directory server. Execute the commands as follows.

- *% $OPEN_DS/bin/ldapmodify -p 389 -h pdsops.jpl.nasa.gov -D "cn=Directory Manager" -w <password> -c -a -f pdspers_schema.ldif*
- *% $OPEN_DS/bin/ldapmodify -p 389 -h pdsops.jpl.nasa.gov -D "cn=Directory Manager" -w <password> -c -a -f*

*pds_groups.ldif*

- *% $OPEN_DS/bin/ldapmodify -p 389 -h pdsops.jpl.nasa.gov -D "cn=Directory Manager" -w <password> -c -a -f pdsops_pers.ldif*

### Policy Configuration

With the software configuration and the directory server configuration complete it is now time to configure the policy. Select the *Proceed to Login* link from the screen above. You should see the following screen in your browser window:

If viewing this document in online form, click the image for a larger version.
Enter the *User Name* (amAdmin) and *Password* then select the *Login* button.

### *Create a User*

Perform the following steps to create a user:

- Select the *Access Control* tab.
- Select */ (Top Level Realm)*.
- Select the *Subjects* tab.
- Select the *New* button from the *User* section.

You should see the following screen in your browser window:


If viewing this document in online form, click the image for a larger version.
Enter the information for a test user (e.g., pdsadmin) then select the *OK* button.

### *Create a Policy*

Perform the following steps to create a policy:

- Select the *Access Control* tab.
- Select */ (Top Level Realm)*.
- Select the *Policies* tab.
- Select the *New Policy* button.
- Enter a name (e.g., registry_policy).
- Select the *New* button from the *Rules* section.

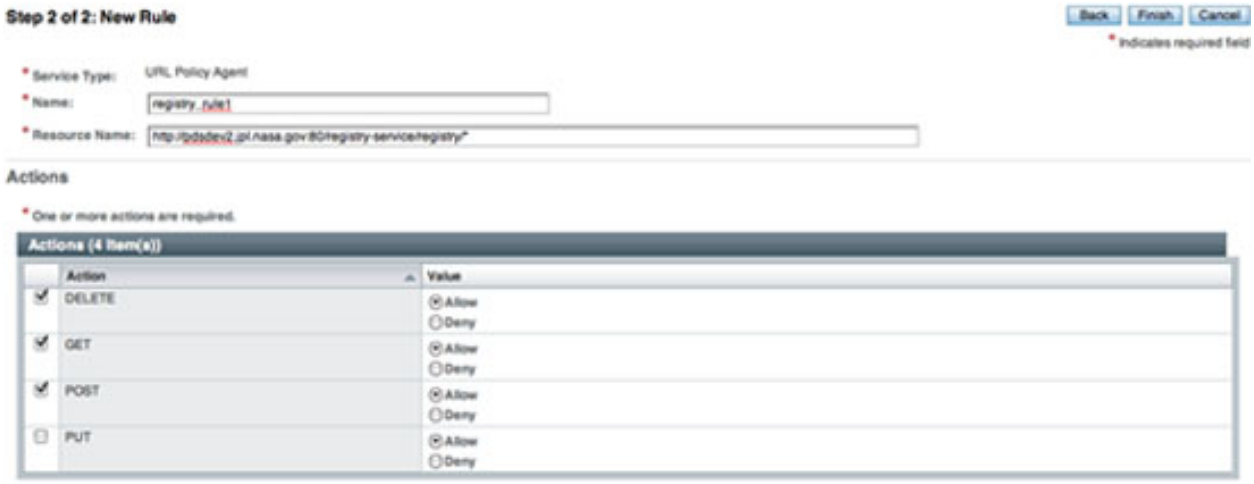
You should see the following screen in your browser window:


If viewing this document in online form, click the image for a larger version.

Continue with the following steps to create a policy:

- Select the *URL Policy Agent (with resource name)* radio button.
- Select the *Next* button.

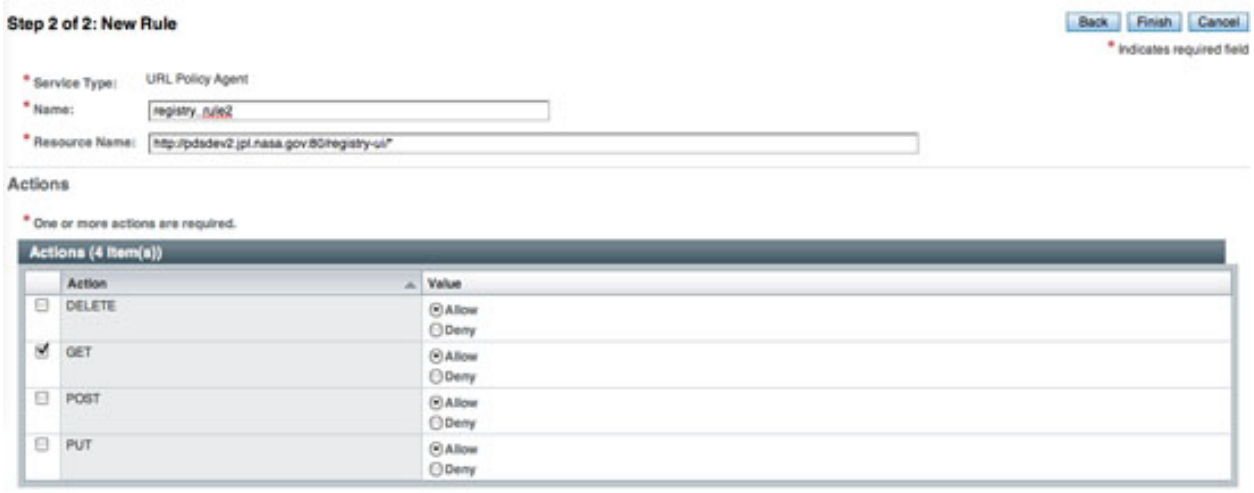
You should see the following screen for entering a rule in your browser window:




If viewing this document in online form, click the image for a larger version.

- Enter a *Name* (e.g., registry_rule1).
- Enter a *Resource Name* (e.g., http://pdsops2.jpl.nasa.gov:80/registry-service/registry/*).
- Select the *DELETE*, *GET* and *POST* check boxes.
- Select the *Finish* button.

Enter a second rule as detailed in the following screen:




If viewing this document in online form, click the image for a larger version.

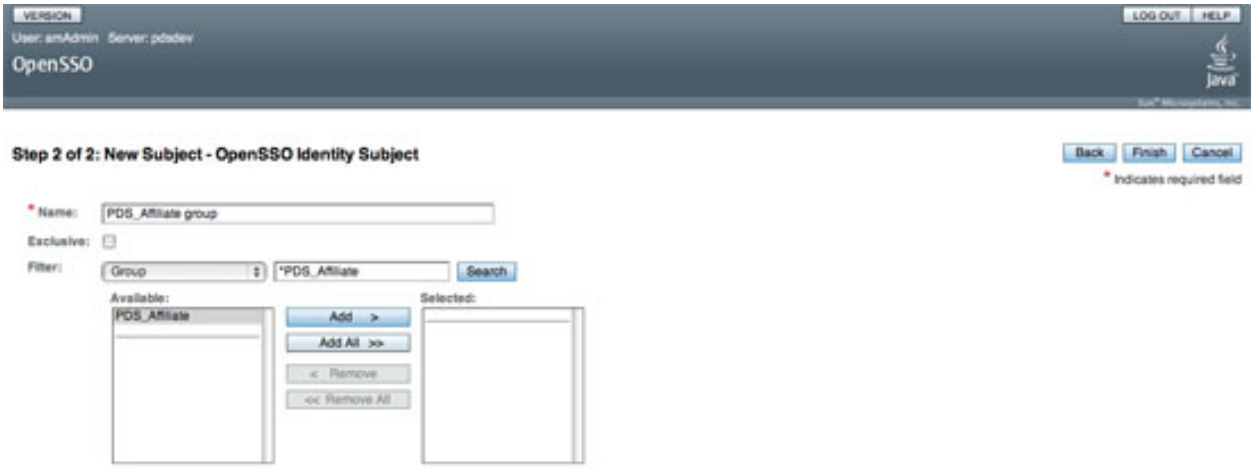
- Enter a *Name* (e.g., registry_rule2).
- Enter a *Resource Name* (e.g., http://pdsops2.jpl.nasa.gov:80/registry-ui/*).
- Select the *GET* check box.
- Select the *Finish* button.

Once the rules are defined, the subject must be defined. Select the *New* button from the *Subjects* section. You should see the following screen in your browser window:


If viewing this document in online form, click the image for a larger version.

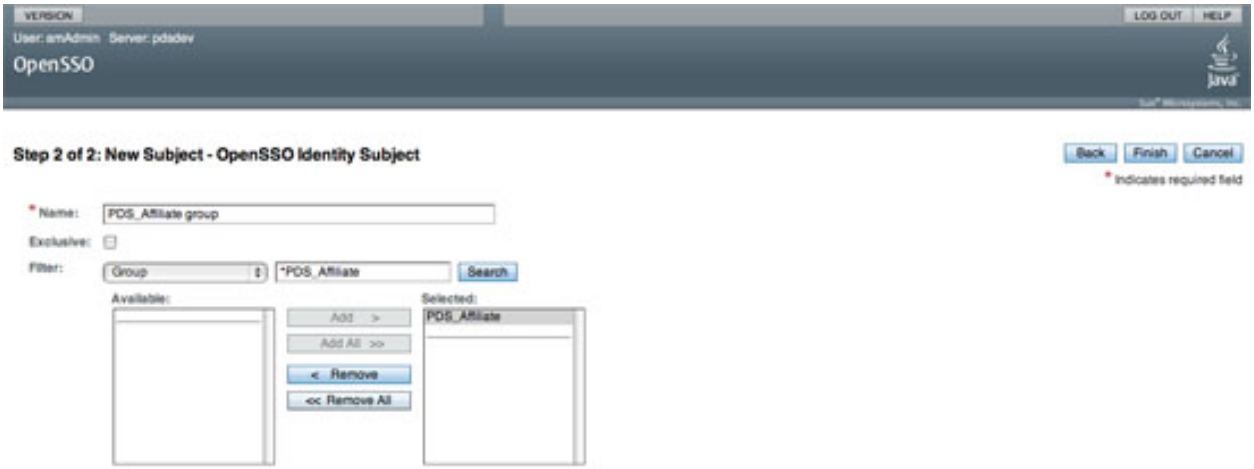
- Select the *OpenSSO Identity Subject* radio button.
- Select the *Next* button.

You should see the following screen in your browser window:




If viewing this document in online form, click the image for a larger version.

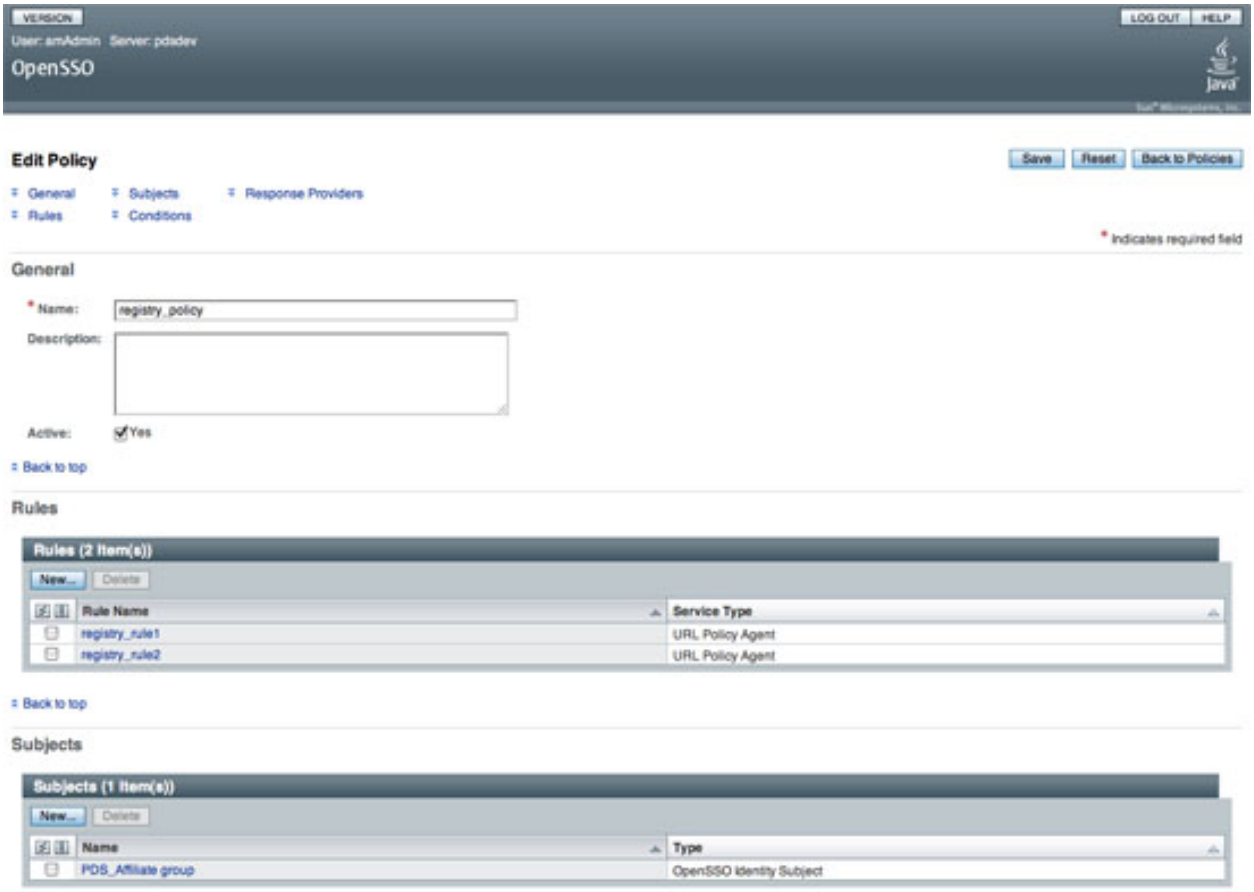
- Enter a *Name* (e.g., PDS_Affiliate group).
- Choose *Group* from the *Filter* list.
- Enter a group name to search on the * text box (e.g., *PDS_Affiliate).
- Select the *Search* button. Then, you will see the group name in the *Available* list box.
- Select the group name from the *Available* list box.
- Select the *Add* > button.




If viewing this document in online form, click the image for a larger version.

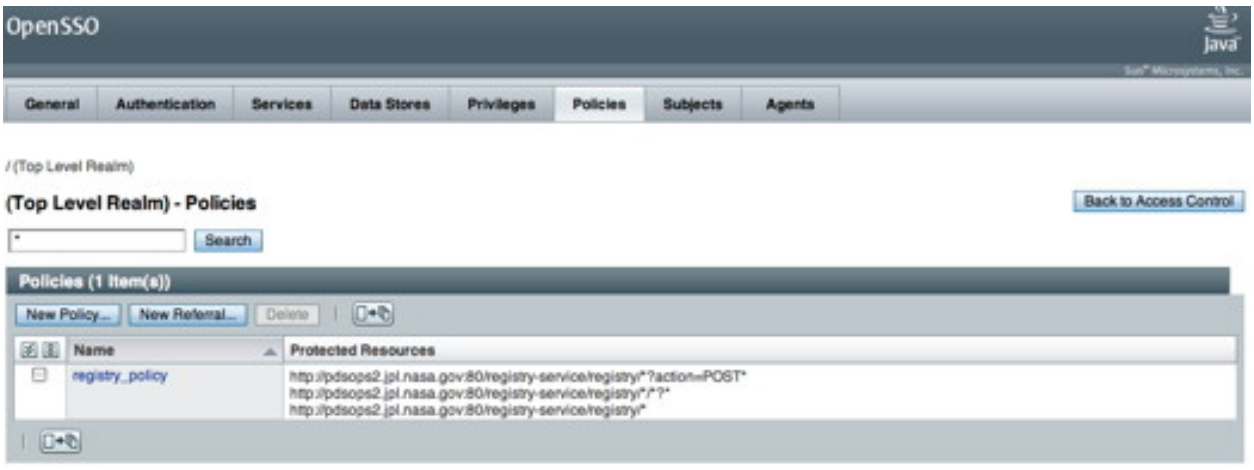
- Select the *Finish* button.
- Select the *Save* button on the subsequent screen.

You should see the following screen in your browser window:




If viewing this document in online form, click the image for a larger version.

Select the *OK* button and you should see the following screen in your browser window:



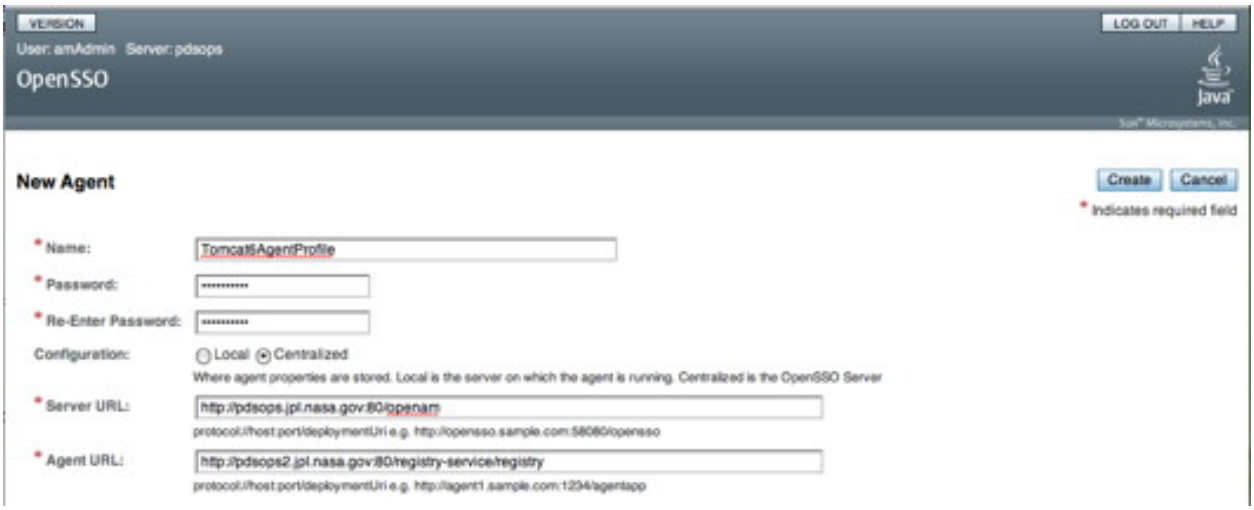

If viewing this document in online form, click the image for a larger version.

***Configure a Policy Agent***

Perform the following steps to configure a policy agent:

- Select the *Access Control* tab.
- Select */(Top Level Realm)* realm.
- Select the *Agent* tab.
- Select the *J2EE* tab.
- Select *New* on the *Agent* section.

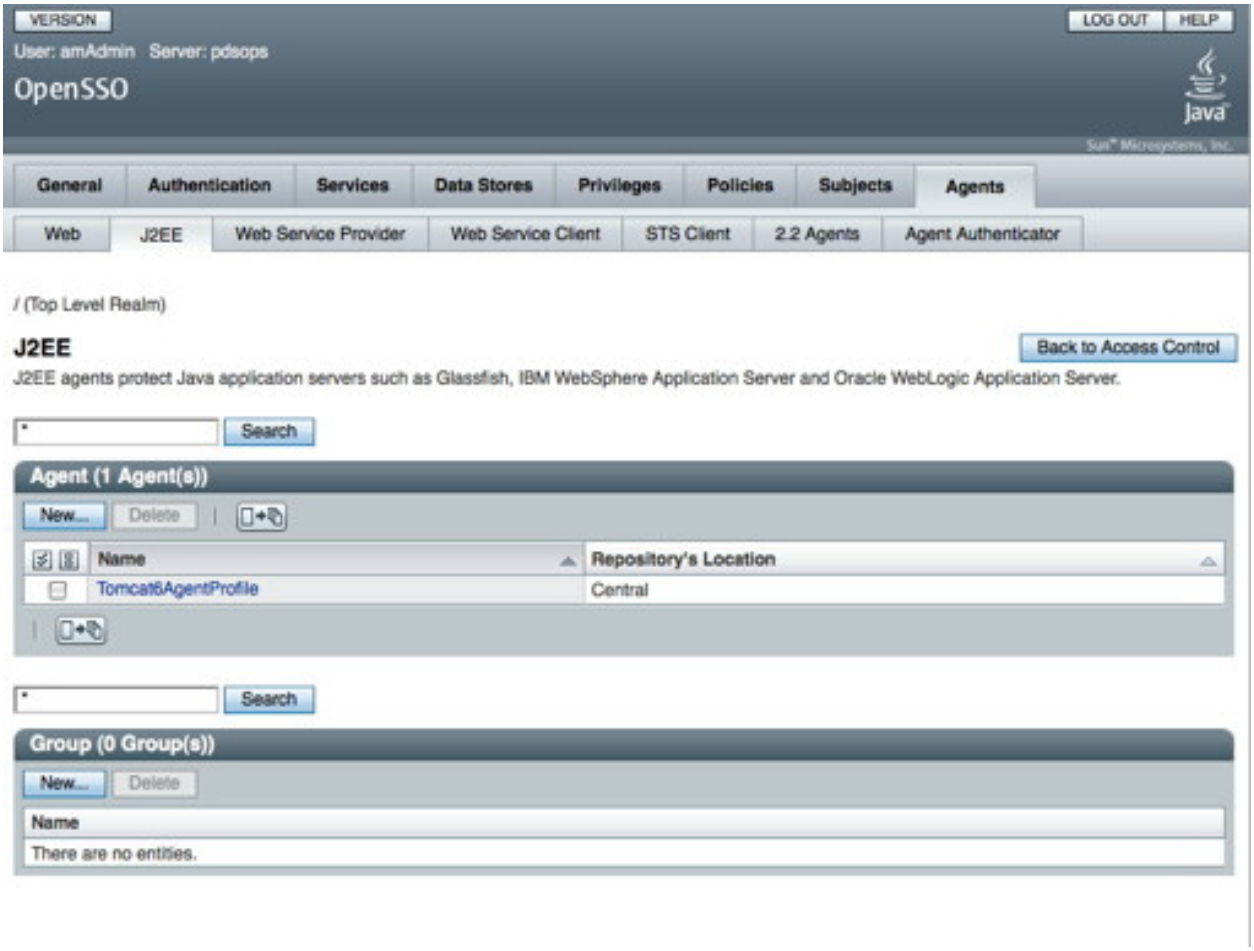
You should see the following screen in your browser window:




If viewing this document in online form, click the image for a larger version.

- Enter a *Name* (same as a profile name when you install a policy agent e.g., Tomcat6AgentProfile).
- Enter a new *Password* (same password that is in $HOME/tomcat6agentpw when you install a policy agent)
- Enter a *Server URL* (e.g., http://pdsops.jpl.nasa.gov:80/openam). Note that the port number should be specified, otherwise it is defaulted to port 80.
- Enter the *Agent URL* with the target service URL (e.g., http://pdsops2.jpl.nasa.gov:80/registry-service/registry).
- Select the *Create* button.

You should see the following screen in your browser window:




If viewing this document in online form, click the image for a larger version.

***Configure Not Enforced URI Processing***

Perform the following steps to configure "Not Enforced URI Processing":

- Select the *Access Control* tab.
- Select */(Top Level Realm)* realm.
- Select the *Agent* tab.
- Select the *J2EE* tab.
- Select the *Tomcat6AgentProfile* link.
- Select the *Application* tab.
- Select the *Not Enforced URI Processing* link.

You should see the following screen in your browser window:


If viewing this document in online form, click the image for a larger version.

Enter each of the following values in the *New Value* text box and select the *Add* button:

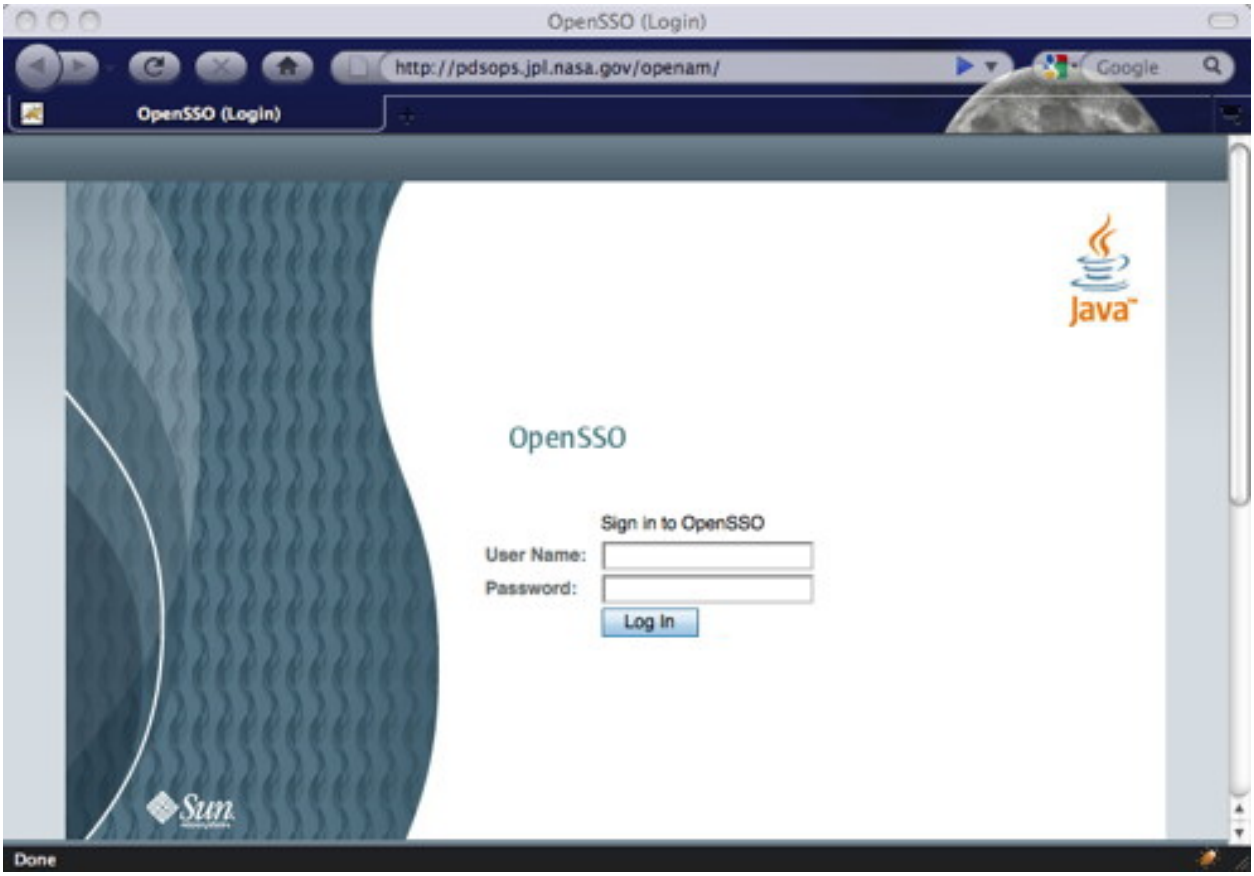
- /registry-ui/
- /registry-service/registry/events/*
- /registry-service/registry/schmes/*
- /registry-service/registry/services/*

Select the *Enabled* check box from the *Invert Not Enfored URIs*.

# 1.4 Operation

## Operation

When Graphical User Interface (GUI) applications have been configured for access control, the user is redirected to the following OpenAM login screen to provide their identification credentials:




If viewing this document in online form, click the image for a larger version.

Once the user enters their identification credentials (user name and password) correctly, they are redirected back to the original application. If the user is accessing an access controlled application via its REST-based interface, they can utilize the *curl* application to obtain an authentication cookie as follows:

```
% curl -d "&username=<username>&password=<password>" \
http://pdsops.jpl.nasa.gov/openam/identity/authenticate
```

```
token.id=AQIC5wM2LY4SfcyFAElnVTJ4ywAONCJRVy74LMgzFYbRmdI=@AAJTSQACMDE=#
```

This cookie can then be passed as follows in a *POST* request:

```
% curl -X POST ... --cookie 'iPlanetDirectoryPro="<token.id>"'
```

The example above also applies to a *DELETE* request.

# 1.5 Appendix - Policy Agent Installation

## Policy Agent Installation

This section details an example installation of the J2EE Policy Agent for Apache Tomcat. The following properties pertain to this example installation:

- OpenAM URL: http://pdsops.jpl.nasa.gov:80/openam
- Agent URL: http://pdsops2.jpl.nasa.gov:80/registry-service/registry
- Agent Profile name: Tomcat6AgentProfile
- Agent Profile password filename: /usr/local/j2ee_agents/tomcat6agentpw

```
% ./agentadmin --install
Do you completely agree with all the terms and conditions of this License
Agreement (yes/no): [no]: yes


***************************************************************************
Welcome to the OpenSSO Policy Agent for Apache Tomcat 6.0 Servlet/JSP
Container

***************************************************************************


Enter the complete path to the directory which is used by Tomcat Server to
store its configuration Files. This directory uniquely identifies the
Tomcat Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Tomcat Server Config Directory Path
[/opt/apache-tomcat-6.0.14/conf]: /usr/local/tomcat6/conf


Enter the URL where the OpenSSO server is running. Please include the
deployment URI also as shown below:
(http://opensso.sample.com:58080/opensso)
[ ? : Help, < : Back, ! : Exit ]
OpenSSO server URL: http://pdsops.jpl.nasa.gov:80/openam


$CATALINA_HOME environment variable is the root of the tomcat
installation.
[ ? : Help, < : Back, ! : Exit ]
Enter the $CATALINA_HOME environment variable: /usr/local/tomcat6
```

```
Choose yes to deploy the policy agent in the global web.xml file.
[ ? : Help, < : Back, ! : Exit ]
Install agent filter in global web.xml ? [true]:


Enter the Agent URL. Please include the deployment URI also as shown below:
(http://agent1.sample.com:1234/agentapp)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: http://pdsops2.jpl.nasa.gov:80/registry-service/registry


Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: Tomcat6AgentProfile


Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /usr/local/j2ee_agents/tomcat6agentpw


---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
Tomcat Server Config Directory : /usr/local/tomcat6/conf
OpenSSO server URL : http://pdsops.jpl.nasa.gov:80/openam
$CATALINA_HOME environment variable : /usr/local/tomcat6
Tomcat global web.xml filter install : true
Agent URL :
http://pdsops2.jpl.nasa.gov:80/registry-service/registry
Agent Profile name : Tomcat6AgentProfile
Agent Profile Password file name :
/usr/local/j2ee_agents/tomcat6agentpw

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:

Updating the /apps/apache-tomcat-6.0.26/bin/setclasspath.sh script
with the Agent classpath ...DONE.

Creating directory layout and configuring Agent file for Agent_001
instance ...DONE.

Reading data from file /apps/j2ee_agents/tomcat6agentpw and encrypting
it ...DONE.

Generating audit log file name ...DONE.

Creating tag swapped OpenSSOAgentBootstrap.properties file for instance
Agent_001 ...DONE.

Creating a backup for file /usr/local/tomcat6/conf/server.xml ...DONE.
```

```
Creating a backup for file /usr/local/tomcat6/conf/web.xml ...DONE.

Adding OpenSSO Tomcat Agent Realm to Server XML file :
/usr/local/tomcat6/conf/server.xml ...DONE.

Adding filter to Global deployment descriptor file :
/usr/local/tomcat6/conf/web.xml ...DONE.

Adding OpenSSO Tomcat Agent Filter and Form login authentication to
selected Web applications ...DONE.


SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/apps/j2ee_agents/tomcat_v6_agent/Agent_001/config \
/OpenSSOAgentBootstrap.properties
Agent Configuration file location
/apps/j2ee_agents/tomcat_v6_agent/Agent_001/config \
/OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/apps/j2ee_agents/tomcat_v6_agent/Agent_001/logs/audit
Agent Debug directory location:
/apps/j2ee_agents/tomcat_v6_agent/Agent_001/logs/debug


Install log file location:
/apps/j2ee_agents/tomcat_v6_agent/installer-logs/audit/install.log

Thank you for using OpenSSO Policy Agent

[root@pdsops2 j2ee_agents]#
```