

OpenAM Setup SSO v0.2

Add Users

Click **Access Control**.

Click the **Top Level Realm** link.

Click **Subjects**.

Click the **New...** button and fill in the following,

```
ID = clarkkent@thedailyplanet.com
First Name = Clark
Last Name = Kent
Full Name = Clark Kent
Password = Adam's password + more
User Status = Active
```

Java EE Policy Agent Setup

DNS

The only thing you have to worry about is that the system that has the agent on it can use the supplied DNS to get to the OpenAM server.

Profile

The [instructions](#) have some details missing.

Click **Access Control**.

You will see the default Top Level Realm. You can read more from [Oracle on what a realm means](#).

A server usually is with an organization, but if you are a service provider you should create a realm per company you work with for example, dailyplanet and lexcrop. After that, within those realms you might have subrealms, like humanresources where you grant more access. If you go this route, you will need to spend a lot of time becoming well versed with realms.

Click the **Top Level Realm** link.

Click **Agents**.

Under the **Web** heading click the **New...** button and fill in the following,

```
Name = jee
password = Adam's password + more
Configuration = Centralized
Server URL = http://openam.krypton.com:8080/openam = your instance of openam
Agent URL = http://krypton.com:8280/examples = the application you are protecting
```

Setup Agent Filter Mode

The filter would not work until I followed the [Protecting Java EE Applications With OpenSSO Policy Agents](#) article to change the Filter Mode.

Edit the jee Profile. Click the **General** link at the top of the page.

Remove the ALL filter.

For New Value,

Map Key = leave empty

Corresponding Map Value = SSO_ONLY

Setup Agent on Server

Unless otherwise indicated use the serveradmin user account.

Set JAVA_HOME

Edit the .profile file for serveradmin to include JAVA_HOME,

```
# Required by Tomcat6 OpenAM Agent
export JAVA_HOME=/opt/java-forgerock
```

For the .profile change to take effect log out then back into serveradmin.

Download Agent

Check out the [main download page](#) for a list of policy agents. In this example we will be using the Tomcat 6 policy agent,

```
wget
http://download.forgerock.org/downloads/openam/j2eeagents/stable/3.0.3/tom
cat_v6_agent_303.zip
unzip tomcat_v6_agent_303.zip
cd j2ee_agents
mv tomcat_v6_agent /opt/openam.0/agents
```

We will add some basic hardening as a sudo enabled account,

```
sudo chown -R serveradmin:staff tomcat_v6_agent/
sudo chmod -R 750 tomcat_v6_agent/
```

Setup Password File

Create your password file using an editor. Do not use a command line because it may be logged into some kind of history file for example,

```
cd /opt/openam.0/agents
vi tomcat.2.password.txt
```

Afterwards protect the file so only serveradmin has access,

```
chmod 600 ./tomcat.2.password.txt
```

Run Setup

Before installing the policy agent, make sure OpenDJ and OpenAM are running. Also make sure the target tomcat server is currently off. Using serveradmin,

```
cd /opt/openam.0/agents/tomcat_v6_agent
./agentadmin --install
```

Here is the output of our sample install,

```
-----
SUMMARY OF YOUR RESPONSES
-----
Tomcat Server Config Directory : /opt/tomcat.2/conf
OpenSSO server URL : http://openam.krypton.com:8080/openam
$CATALINA_HOME environment variable : /opt/tomcat.2
Tomcat global web.xml filter install : true
Agent URL : http://krypton.com:8280/examples
Agent Profile name : jee
Agent Profile Password file name :
/opt/openam.0/agents/tomcat.2.password.txt
```

A successful install will look like the following,

▼ [Click here to expand...](#)

Updating the /opt/tomcat.2/bin/setenv.sh script with the Agent configuration JVM option ...DONE.
DONE.

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

Reading data from file /opt/openam.0/agents/tomcat.2.password.txt 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 /opt/tomcat.2/conf/server.xml ...DONE.

Creating a backup for file /opt/tomcat.2/conf/web.xml ...DONE.

Adding OpenSSO Tomcat Agent Realm to Server XML file :
/opt/tomcat.2/conf/server.xml ...DONE.

Adding filter to Global deployment descriptor file :
/opt/tomcat.2/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:
/opt/openam.0/agents/tomcat_v6_agent/Agent_001/config/OpenSSOAgentBootstrap.properties
Agent Configuration file location
/opt/openam.0/agents/tomcat_v6_agent/Agent_001/config/OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/opt/openam.0/agents/tomcat_v6_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/openam.0/agents/tomcat_v6_agent/Agent_001/logs/debug
```

Install log file location:
/opt/openam.0/agents/tomcat_v6_agent/installer-logs/audit/install.log

Thank you for using OpenSSO Policy Agent

Test

Before testing make sure you log out of your current OpenAM login used to access the OpenAM console.

Go to the url of the protected application, <http://krypton.com:8280/examples>.

You should be redirect to the OpenAM login page. Enter in the credentials of a the created user.

References

<http://openam.forgerock.org/doc/agent-install-guide/OpenAM-Agent-Install-Guide.html>

<https://wikis.forgerock.org/confluence/display/openam/Add+Authentication+to+a+Website+using+OpenAM>