

2013

IBM SINGLE SIGN-ON WITH CA SITEMINDER FOR SAMPLE WEB APPLICATION

Santosh Manakdass & Syed Moinudeen

This article describes how to configure any Web Application for Single Sign-On with SiteMinder. This article assumes that readers have basic knowledge on Single Sign-On and familiar with SiteMinder. This article assumes the required software i.e. WAS, SiteMinder Policy server, SiteMinder Administrative UI, Apache as Proxy server are installed.



Santosh Manakdass



SayedMoinuddin

About the authors: Working as a developer for Atlas team under ECM. Their daily work involves in developing and fixing defects for our product involving areas like Java, JavaScript, JSF, Gwt, Oracle etc. Reach out to them at samanakd@in.ibm.com, syed.moinudeen@in.ibm.com

Introduction

SiteMinder provides policy-based authentication as well as single sign-on for all Web-based applications. SiteMinder configuration is very complex which involves SiteMinder Policy Server, Web Agents, Proxy Server, SiteMinder Administration UI console configurations etc. We can find many resources in web which gives details on SiteMinder configuration but not completely and that those do not work as expected. We are writing complete steps of configuring a sample Web Application i.e., Snoop, which comes deployed with IBM WAS.

Many of the readers who use Single Sign-On using CA SiteMinder can begin with our article as we mention each and every step from scratch. Many times audience may miss out simple configurations and get stuck. Our article will help the beginners with each and every step to know how to configure Single Sign-On with SiteMinder for sample application.

NOTE1: The article was developed using WAS 7.0, SiteMinder Policy server v12, SiteMinder Administrative UI v12, Apache 2.2 as Proxy server.

NOTE2: Apache HTTP server is registered product of The Apache Software Foundation. SiteMinder software are registered product of CA Site Minder.

Overview

SiteMinder Interaction with a Web Application

Below Diagram gives a Sequence Diagram of the interaction of Client with any Web Application involving SiteMinder.

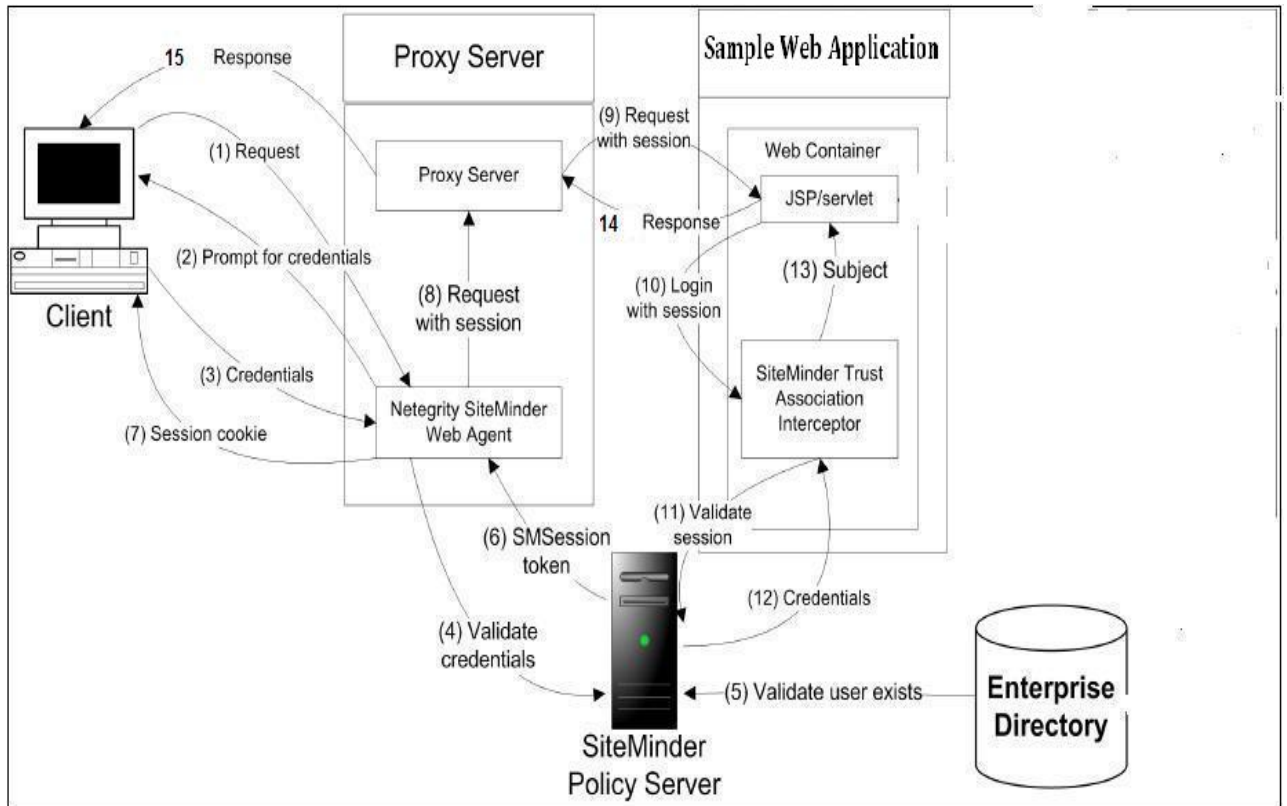


Figure 1: Sequence Diagram of the interaction of Client with any Web Application involving SiteMinder

Configurations required for any Web Application for Single Sign-On with SiteMinder

We will be using the basic sample application i.e., Snoop, which comes deployed with IBM Websphere Application Server to show how to configure any web application for Single Sign-On with SiteMinder.

The following are the configurations needed:

1. SiteMinder Policy Server Configurations
2. Proxy Server Configurations
3. Websphere Application Server Configurations

SiteMinder Policy Server Configurations

Installed the SiteMinder Policy Server software and configured SiteMinder Policy Store using Oracle DB.

The following configurations are needed in SiteMinder Administrative console i.e. Policy server web Interface.

1. Create agent for proxy server. As for example: proxy_agent.
Select *Supports 4.x agents* check box and enter IP address of SiteMinder Policy server under Trust Settings.

The screenshot displays the SiteMinder Administrative console interface. At the top, a blue header bar indicates the user is logged in as 'siteminder' to 'conf2.p8.ibm.com' with a '(Logout)' link. Below this, a navigation bar contains tabs for 'Infrastructure', 'Policies', 'Reports', and 'Administration'. Under the 'Policies' tab, a sub-navigation bar shows 'Agents', 'Authentication', 'Directory', and 'Hosts'. The main content area is titled 'View Agent: proxy_agent'. It is divided into three sections: 'General', 'Agent Type Settings', and 'Trust Settings'. The 'General' section shows 'Name: proxy_agent' and 'Description: Agent for Proxy Server'. The 'Agent Type Settings' section shows 'Agent Type: Web Agent' and a checked checkbox for 'Supports 4.x agents'. The 'Trust Settings' section shows 'IP Address: 9.126.153.226' and 'Shared Secret: *****'.

Logged in as: siteminder to conf2.p8.ibm.com (Logout)			
Infrastructure	Policies	Reports	Administration
▼ Agents	► Authentication	► Directory	► Hosts
View Agent: proxy_agent			
General			
Name: proxy_agent		Description: Agent for Proxy Server	
Agent Type Settings			
Agent Type: Web Agent			
Supports 4.x agents		<input checked="" type="checkbox"/>	
Trust Settings			
IP Address: 9.126.153.226			
Shared Secret: *****			

Figure 2 : Agent created for proxy server

2. Similarly, create an agent for Snoop. For example: snoop_agent.



SiteMinder Administrative UI

Logged in as: **siteminder** to **conf2.p8.ibm.com** (Logout)

Infrastructure Policies Reports Administration

Agents Authentication Directory Hosts

View Agent: *snoop_agent*

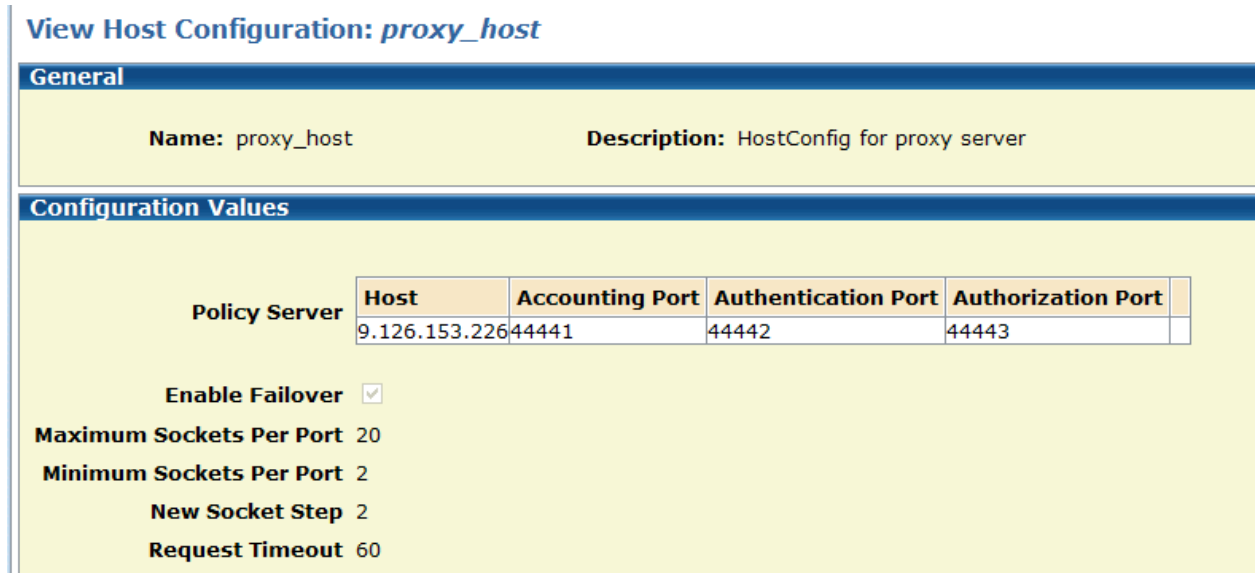
General	
Name: snoop_agent	Description: Agent for snoop

Agent Type Settings	
Agent Type	Web Agent
Supports 4.x agents	<input checked="" type="checkbox"/>

Trust Settings	
IP Address	9.126.153.226
Shared Secret	*****

Figure 3 : Agent for Snoop server

3. Create Host configuration object for proxy server say proxy_host.
For PolicyServer parameter, enter IP Address of SiteMinder PolicyServer as value.



View Host Configuration: *proxy_host*

General	
Name: proxy_host	Description: HostConfig for proxy server

Configuration Values				
Policy Server	Host	Accounting Port	Authentication Port	Authorization Port
	9.126.153.226	44441	44442	44443
Enable Failover	<input checked="" type="checkbox"/>			
Maximum Sockets Per Port	20			
Minimum Sockets Per Port	2			
New Socket Step	2			
Request Timeout	60			

Figure 4 : Host Configuration object for proxy server

4. Similarly, Create Host configuration object for snoop server say snoop_host.

The screenshot shows the 'View Host Configuration: snoop_host' page. The navigation bar includes 'Infrastructure', 'Policies', 'Reports', and 'Administration'. Below it, a breadcrumb trail shows 'Agents' > 'Authentication' > 'Directory' > 'Hosts'. The main content area has a 'General' tab selected, showing the 'Name: snoop_host' and 'Description: Host Configuration object for Sno'. Below this is a 'Configuration Values' section with a table for 'Policy Server' settings.

Host	Accounting Port	Authentication Port	Authorization Port
9.126.153.226	44441	44442	44443

Below the table, there is a checkbox for 'Enable Failover' which is checked.

Figure 5: Host Configuration object for snoop server

5. Create Agent configuration objects for reverse proxy say proxy_agentconfig. Add or edit the following parameter values:

- ❖ CookieDomain: Enter the Active Directory domain in which you are running, including a leading period (for example, p8.ibm.com).
- ❖ CookieProvider: Edit the #CookieProvider entry, delete the leading # character, and add the URL for the proxy server (for example, http:// <IP Address of proxyserver >:80/SmMakeCookie.ccc).

CookieDomainScope	
CookieProvider	http://9.126.153.227:80/SmMakeCookie.ccc

- ❖ DefaultAgentName: Edit the #DefaultAgentName entry, delete the leading # character, and add the name of the Web agent on the proxy server created above (for example, proxy_agent).

DefaultAgentName	proxy_agent
------------------	-------------

- ❖ LogAppend: Set value to yes.
- ❖ LogFileName: Enter the name of the log file on the proxy server (for example, C:\Program Files\Apache Group\Apache2\logs\WebAgent.log).
- ❖ LogFileSize: Set value to 10.
- ❖ LogLevel: Set value to 15.
- ❖ Logfile: Set value to yes.
- ❖ PreservePostData: Set value to no.
- ❖ ProxyAgent: Set value to yes.
- ❖ ProxyTrust: Set value to no.
- ❖ SecureApps: Edit the #SecureApps entry, delete the leading # character, and set the value to no.
- ❖ TraceConfigFile: Enter the name of the trace configuration file (for example, C:\Program Files\CA\webagent\config\WebAgentTrace.conf).
- ❖ TraceFile: Set value to yes.

- ❖ TraceFileName: Enter the name of the trace output file (for example, C:\Program Files\Apache Group\Apache2\logs\WebAgentTrace.log).
- ❖ TranscientIPCheck: Set value to yes.
- ❖ PersistentIPCheck : Set value to yes.

6. Similarly, Create Agent configuration objects for snoop say snoop_agentconfig. Add or edit the following parameter values:

- ❖ DefaultAgentName: Edit the #DefaultAgentName entry, delete the leading # character, and enter the name of the ASA Agent on the snoop server created above (for example, snoop_agent).
- ❖ LogAppend: Set value to yes.
- ❖ LogFileName: Enter the name of the log file on the snoop server (for example, C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\AppServerAgent.log).
- ❖ LogFileSize: Set value to 10.
- ❖ LogLevel: Set value to 15.
- ❖ Logfile: Set value to yes.
- ❖ ProxyTrust: Set value to no.
- ❖ ChallengeForCredentials: Set value to yes.
- ❖ AssertionAuthResource: Set value to /siteminderassertion
- ❖ RmiAuthResource: Set value to /sitemindermirealm
- ❖ SystemAuthResource: Set value to /sitemindersystemrealm
- ❖ BadUrlChars: leave default value.

BadUrlChars	/.,./,./,./,* ,* ,~ ,\,%00-%1f,%7f-%ff,%25
-------------	--

7. Configure the User Directory. Say user_dir
Here, specify the details on the LDAP User directory whose members will be allowed to access the Application.

View User Directory: *user_dir*

General	
Name: user_dir	Description: User Active Directory Interface

Directory Setup	
Namespace: AD:	Server: windevintWAS.p8.ibm.com
Use authenticated user's security context: <input type="checkbox"/>	Secure Connection: <input type="checkbox"/>

Administrator Credentials	
Require Credentials <input checked="" type="checkbox"/>	
Username	cn=Administrator,cn=Users,dc=p8,dc=ibm,dc=com
Password	*****
Confirm Password	*****

LDAP Settings	
LDAP Search Root cn=Users,dc=p8,dc=ibm,dc=com Scope <input type="radio"/> One Level <input checked="" type="radio"/> Sub-Tree Max Time 30 Max Results 0	LDAP User DN Lookup Start (&(objectClass=user)(cn= End)) Effective Lookup (&(objectClass=user)(cn= ID-From-Login))

Figure 6: Creation of user Directory

8. Create the SiteMinder domain say ssosm_domain.
In the Users Directories tab, select the name of the user directory created above (for example, user_dir).

View Domain: *ssosm_domain*

General	Realms	Policies	Responses	Rule Groups	Variables				
General Name: ssosm_domain Description: SSO Siteminder Domain Global Policies Apply: <input checked="" type="checkbox"/>									
User Directories <table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> user_dir</td> <td>User Active Directory Interface</td> </tr> </tbody> </table>						Name	Description	<input checked="" type="radio"/> user_dir	User Active Directory Interface
Name	Description								
<input checked="" type="radio"/> user_dir	User Active Directory Interface								

Figure 7 : Creation of SiteMinder Domain

9. Create the primary realm for the reverse proxy under the Domain i.e. ssosm_domain created above say proxy_realm.

The screenshot displays the IBM Security Manager console interface. At the top, there are tabs for 'Infrastructure', 'Policies', 'Reports', and 'Administration'. Below these, a navigation bar shows 'Applications', 'Domains', 'Expressions', 'Global', and 'Password'. The main content area is titled 'View Realm: proxy_realm'. It is divided into three sections: 'General', 'Resource', and 'Rules'. The 'General' section shows 'Name: proxy_realm', 'Domain: ssosm_domain', and 'Description: Realm for Proxy server'. The 'Resource' section shows 'Agent: proxy_agent', 'Resource Filter: /snoop', 'Effective Resource: proxy_agent(9.126.153.226)/snoop', 'Default Resource Protection: Protected (selected)', and 'Authentication Scheme: Basic'. The 'Rules' section contains a table with one rule named 'Get'.

Name	Description
Get	Get Rule for Proxy Realm

Figure 8: Creation of Realm for proxy server

10. Create a rule say Get as shown below under the reverse proxy server realm i.e. proxy_realm.

View Rule: Get

[View Realm: proxy_realm](#) > View Rule: Get

General	
Name: Get	Description: Get Rule for Proxy Realm
Domain: ssosm_domain	Realm: proxy_realm

Attributes	
Realm and Resource	
Resource /*	
Effective Resource: proxy_agent/snoop/*	
Regular Expression <input type="checkbox"/>	
Allow/Deny and Enable/Disable	
<input checked="" type="radio"/> Allow Access	
<input type="radio"/> Deny Access	
Enabled <input checked="" type="checkbox"/>	
Action	
<input checked="" type="radio"/> Web Agent actions	
<input type="radio"/> Authentication events	
<input type="radio"/> Authorization events	
Action <ul style="list-style-type: none">• Get• Post	

Figure 9 : Rule for proxy realm

11. Create the snoop realm for the snoop server, say snoop_realm under Domain created above as shown below.

▸ Applications ▾ Domains ▸ Expressions ▸ Global ▸ Password

View Realm: *snoop_Realm*

General

Name: snoop_Realm **Description:** Realm for snoop
Domain: ssosm_domain

Resource

Agent ...

Resource Filter /snoop

Effective Resource snoop_agent(9.126.153.226)/snoop

Default Resource Protection ☒ Protected ☐ Unprotected

Authentication Scheme Basic

Rules

	Name	Description
▶	snoop_rule	Rule for snoop

Figure 10: Creation of Realm for snoop server

12. Create a rule for the snoop_realm Realm created above say snoop Get.

Applications ▾ **Domains** ▸ **Expressions** ▸ **Global** ▸ **Password**

View Rule: *snoop_rule*

[View Realm: *snoop_Realm*](#) > View Rule: *snoop_rule*

General	
Name: snoop_rule	Description: Rule for snoop
Domain: ssosm_domain	Realm: snoop_Realm

Attributes
Realm and Resource <p>Resource /*</p> <p>Effective Resource: snoop_agent/snoop/*</p> <p>Regular Expression <input type="checkbox"/></p>
Allow/Deny and Enable/Disable <p><input checked="" type="radio"/> Allow Access</p> <p><input type="radio"/> Deny Access</p> <p>Enabled <input checked="" type="checkbox"/></p>
Action <p><input checked="" type="radio"/> Web Agent actions</p> <p><input type="radio"/> Authentication events</p> <p><input type="radio"/> Authorization events</p> <p>Action • Get • Post</p>

Figure 11: Rule for snoop realm

13. Create a Policy for the reverse proxy server say proxy_policy under Domain created above. Add the Available Members list for the group name shown below:

View Policy: proxy_policy

General	Users	Rules	Expression
---------	--------------	-------	------------

User Directories

user_dir

AND Users/Groups ☐

	▲ Name	User Class	Exclude
▶	CN=Domain Admins,CN=Users,DC=p8,DC=ibm,DC=com	group	
▶	CN=smgroup,CN=Users,DC=p8,DC=ibm,DC=com	group	

Figure 12a: Creation of Policy for proxy server

Add the Get rule created above under Rules tab as shown below.

View Policy: proxy_policy

General	Users	Rules	Expression
---------	-------	--------------	------------

Rules

Realm	Rule	Response	Response Group
proxy_realm	Get		

Figure 12b: Creation of Policy for proxy server

14. Create a Policy for the snoop server say snoop_policy under Domain created above. Add the Available Members list for the group name as shown below:

View Policy: *snoop_policy*

General	Users	Rules	Expression
---------	--------------	-------	------------

User Directories

user_dir

AND Users/Groups ☐

	Name	User Class	Exclude
▶	CN=Domain Admins,CN=Users,DC=p8,DC=ibm,DC=com	group	
▶	CN=smgroup,CN=Users,DC=p8,DC=ibm,DC=com	group	

Figure 13a: Creation of Policy for snoop server

Add the snoop rule created above under Rules tab as shown below.

View Policy: *snoop_policy*

General	Users	Rules	Expression
---------	-------	--------------	------------

Rules

Realm	Rule	Response	Response Group
snoop_Realm	snoop_rule		

*Figure 13b: Creation of Policy for proxy server***Proxy Server Configurations**

The following configurations are needed in Reverse Proxy Server:

1. Install Apache HTTP server.
2. Configure the Apache HTTP server for reverse proxy mode.
 - Open the file httpd.conf located in
C:\Program Files\Apache Group\Apache2\conf
 - Uncomment the following lines in the LoadModule section:
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so

```
LoadModule proxy_http_module modules/mod_proxy_http.so
```

- Add the following lines at the end of the file:

```
### Proxy configuration
```

```
ProxyRequests Off
```

```
<Proxy http://<proxy server name>/snoop*>
```

```
Order deny, allow
```

```
Allow from all
```

```
</Proxy>
```

```
<Location /snoop>
```

```
ProxyPass          http://<snoop server name>:port/snoop
```

```
ProxyPassReverse  http://<snoop server name>:port/snoop
```

```
</Location>
```

- Restart the Apache HTTP service.
3. Install the SiteMinder web agent.
 4. Configure the SiteMinder web agent as given in SiteMinder documentation.
 5. Enable the Web Agent.
 - Open the file WebAgent.conf located at;
C:\Program Files\Apache Group\Apache2\conf
 - Change the value of the AgentConfigObject="proxy_agentconfig" i.e. the agent configuration object created for proxy server above.
 - Change the value of the EnableWebAgent property to YES.
 - Save and close the file.
 - Restart Apache HTTP Server service.

WebSphere Application Server Configurations

In this section, we configure WebSphere Application Server (version 7.0 is used in this article) to work with the SiteMinder Application Server Agent.

NOTE: Snoop server refers to the server where the Web Application is deployed.
The following configurations are needed in snoop Server:

1. Patch WebSphere JCE Security Policy files.
2. Set PATH and JAVA_HOME to Websphere JRE.
3. Define JVM™ system variables in Websphere as shown below.
Restart Websphere.

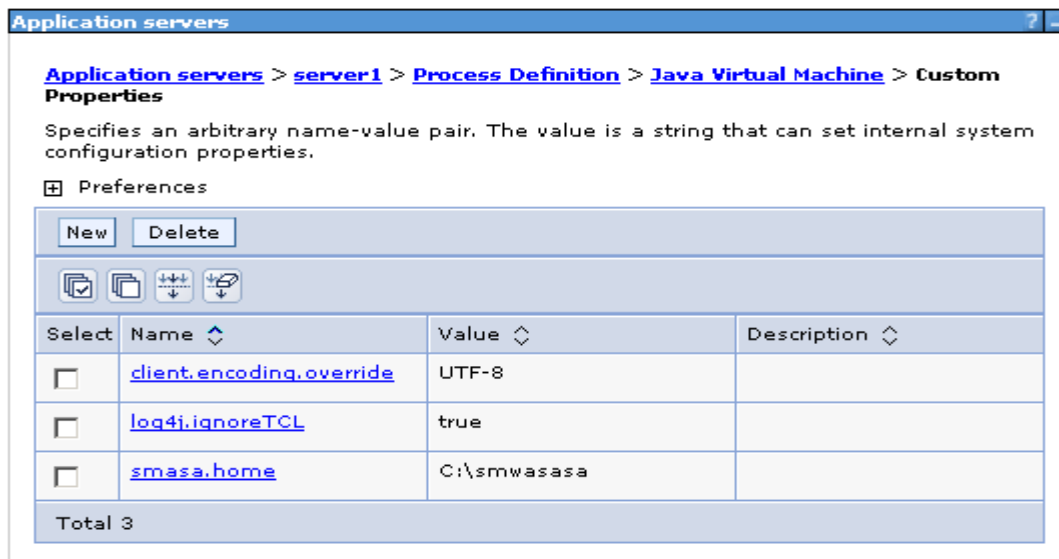


Figure 14: Configure JVM system variables

4. Install Siteminder Application server agent for Websphere at Installation Directory, C:\smwasasa.
 Note: While installing above Siteminder Application server agent for Websphere Enter host configuration object as snoop_host and agent configuration object as snoop_agentconfig created above.
5. Stop Websphere. Configure the SiteMinder logging class loader.
 Move the files smlogger.jar and log4j.jar from:
 C:\Program Files\IBM\WebSphere\AppServer\lib\ext to:
 C:\smwasasa\lib (Create the directory if does not exist.)
6. Copy the SiteMinder Agent properties file.
 Copy the smagent.properties file from: C:\smwasasa\conf to:
 C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\properties
 Start WebSphere.
7. Set required LDAP Configuration.

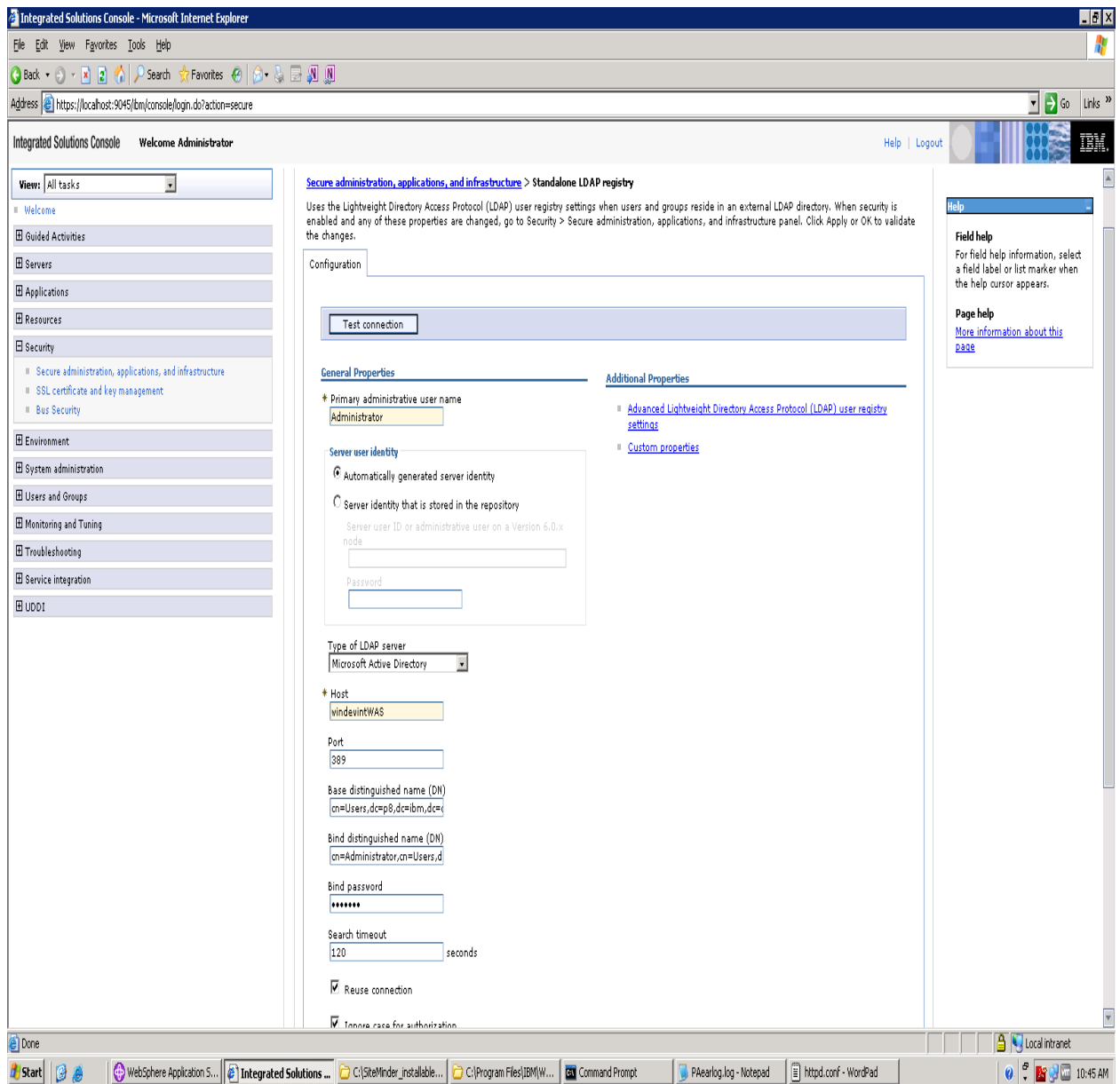


Figure 15: Configure Global security

windevintWAS is the hostname of the Domain Controller.

8. Enable single sign-on option.
 Select **Security** → **Secure administration, applications, and infrastructure**.
 Select **Web Security** → **single sign-on (SSO)**. Check **Enabled** check box.
9. Enable the Trust Association option.
 - Select **Security** → **Secure administration, applications, and infrastructure**.
 - Select the **Web Security** → **Trust association** link.
 - Check the **Enable trust association** check box.
 - Click **Interceptors**. Click **New**

- Enter com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor in the Interceptor class name field. Click Apply. Click Save.

Test the Application after configuring Single Sing-on using SiteMinder

1. Enter the following url in your browser.

http://<proxy server name>/snoop/

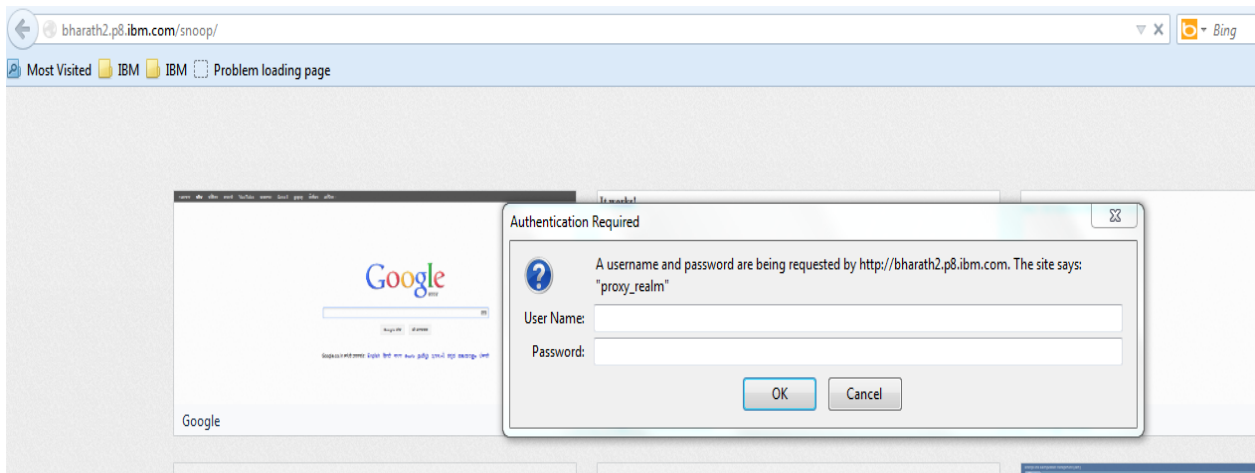


Figure 16: Testing the Application

2. Enter the logon credentials of the user who belongs to the group added above under the policy i.e proxy_policy above in the Siteminder Policy Server Administrative console.

Resources

- Further configuration on filtering the resources and controlled security access on the Application refer to the SiteMinder documentation here <https://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%20SP3-ENU/Bookshelf.html>