Infor Web User Interface and IBM i WebSphere Application Server

Single Sign On Configuration Guide

Publication Information

Publication date: December 15, 2011

Document code: 20111215164916

Contents

Single Sign On **5**

Prerequisites **6**

Installation Checklist **7**

Confirming WebSphere setup **9**

Configuring WebSphere to use security **10**

Updating WebSphere Application Server Service 14

Installing the identity token application **15**

Installing the Identity Token resource adapter 15

Setting up J2C authentication data 16

Configuring the Identity Token J2C connection factory 17

Installing the identity token test application 19

Installing the identity Token Ear file 20

Installing SPNEGO **23**

Create a virtual host name for WebSphere 23

Step 1 – Generate a user ID for application server 23

Step 2 – Assign the Service Principle Name and create a key file 23

Step 3 – Set up Kerberos Configuration on the application server 24

Step 4 – Enable WebSphere Security 25

Step 5 – Enable SSO 25

Step 6 – Enable trust association 25

Step 7 – Disable Security Pre-Invoke 26

Step 8 – Enable SPNEGO at the JVM level 26

Step 9 – Turn on SPNEGO Logging and Tracing 27

Step 10 – Restart WebSphere 28

Step 11 – Configure Browsers 28

Step 12 – Test the configuration 28
Step 13 – Update HTTP Configuration 29

Single Sign On

This document provides instructions to set up the WebSphere Application Server (WAS) to allow for use of the active directory and to set up EIM to allow WebTop to take advantage of Single Sign On (SSO).

Prior to completing the steps in this document, Enterprise Identity Mapping (EIM) must be implemented on your System i. IBM provides these documents that explain how to configure EIM:

- “Windows-based Single Sign-on and the EIM Framework on the IBM eServer iSeries Server” at http://www.redbooks.ibm.com/abstracts/SG246975.html?Open
- “Scenario: Enable single sign-on” at http://as400bks.rochester.ibm.com/iseries/v5r2/ic2924/index.htm?info/rzakh/rzakhscen2.htm

To confirm that EIM is working properly, change your connection to the System i in iSeries Navigator to use Kerberos. You should no longer be challenged for a password.

To change your iSeries Navigator settings:

1 Start iSeries Navigator and right-click the system that you have configured for Single Sign-On.

2 Choose **Properties**.

3 Select the **Connection** tab and select the **Use Kerberos principal name, no prompting** check box.

4 Click **OK**. If you have already logged into the system, reboot your PC to clear the cached logon credentials.

Prerequisites

The single sign on configuration requires this software:

- IBM i5/OS 5.4.
- EIM installed and running on the System i server.
- WAS 6.1.0.23 or higher. These instructions use WAS 6.1.0.23 Base.
- Microsoft Active Directory for authentication.
- Default WAS Application loaded and running to use the snoop servlet.
- Infor WebTop for IBM System i 4.4 with SP1.

Installation Checklist

Assemble the following information before you begin the installation. You will use this information during the installation and configuration.

Item	Sample value	Your value
WebSphere Server name and port	mywasserver:8011	
Windows domain user name for secure admin of WAS	myco\wasadmin	
Windows domain user name password for secure admin of WAS	waspw1234	
Bind Distinguished Name for the admin user	CN=Service WASAdmin,OU=SSO,OU=Service Accounts,DC=myco,DC=com	
Windows Kerberos Authentication Server name (usually the Domain Controller)	mywdc1	
Windows Kerberos Authentication Server name port (usually the Domain Controller)	Default: 389	
Base Distinguished Name for the domain (from Microsoft Active Directory)	dc=myco,dc=com	
EIM Admin User ID (created during EIM setup)	cn=administrator	
EIM Admin User password (created during EIM setup)		
EIM LDAP Directory Server (created during EIM setup)	mysystemi.myco.com	
EIM Domain Name (created during EIM setup)	EIMMYI	
EIM Source User Registry Name (created during EIM setup)	MYCO.COM	

Item	Sample value	Your value
WAS system virtual name (new name in DNS for WAS system HTTP access) Do not create as an alias.	mywas	
Domain Service Principle User ID for WebSphere Application Server system (for authenticating users)	myco\mywas	
Uppercase Kerberos realm (Upper case)	MYCO.COM	
Keytab file location and name	c:\winnt\mywas.keytab	
Key distribution center name	mywdc1	
Lower case domain name	myco.com	

Confirming WebSphere setup

Follow the instructions in this section to set up WAS to use Active Directory to perform authentication. These instructions were developed using a WAS 6.1 Base Server. Although this process could apply to other WebSphere Servers, the steps may be different.

Ensure that the default application is loaded so that you can use the snoop servlet to check the steps and your progress.

To confirm the WebSphere setup:

1 From the WAS menu, select **All Programs**/I**BM WebSphere**/**Application Server**/Profiles/**{Profile Name}**/**First Steps**.

2 Run the Installation Verification Option. You must receive this message to proceed:

IVTL0070I: The Installation Verification Tool verification succeeded. IVTL0080I: The installation verification is complete.

3 To make sure that the snoop servlet is working, enter this URI:

http://{hostname}:{port}/snoop Example: http://mywas:9081/snoop

4 Generate the Version report to validate that you are on the correct WAS patch level.

a Run the genVersionReport.bat command and look at the VersionReport.html.

b Make sure the Version Report has the patch level of 6.1.0.23 or higher.

Configuring WebSphere to use security

After you set up security, you will be prompted to open the Admin console. You must enter the user ID and password that you set up below. If the WebSphere server is set up to run as a service, you may not be able to stop it from the service screen, but only from the menu, after you enter the user ID and password.

To configure WebSphere security:

1 From the Start menu, select **All Programs/IBM WebSphere/Application Servers/Profiles/{Profile Name)/Administrative Console**.

2 On the Admin console, expand the **Security** menu node.

3 Select **Secure administration, applications and infrastructure**.

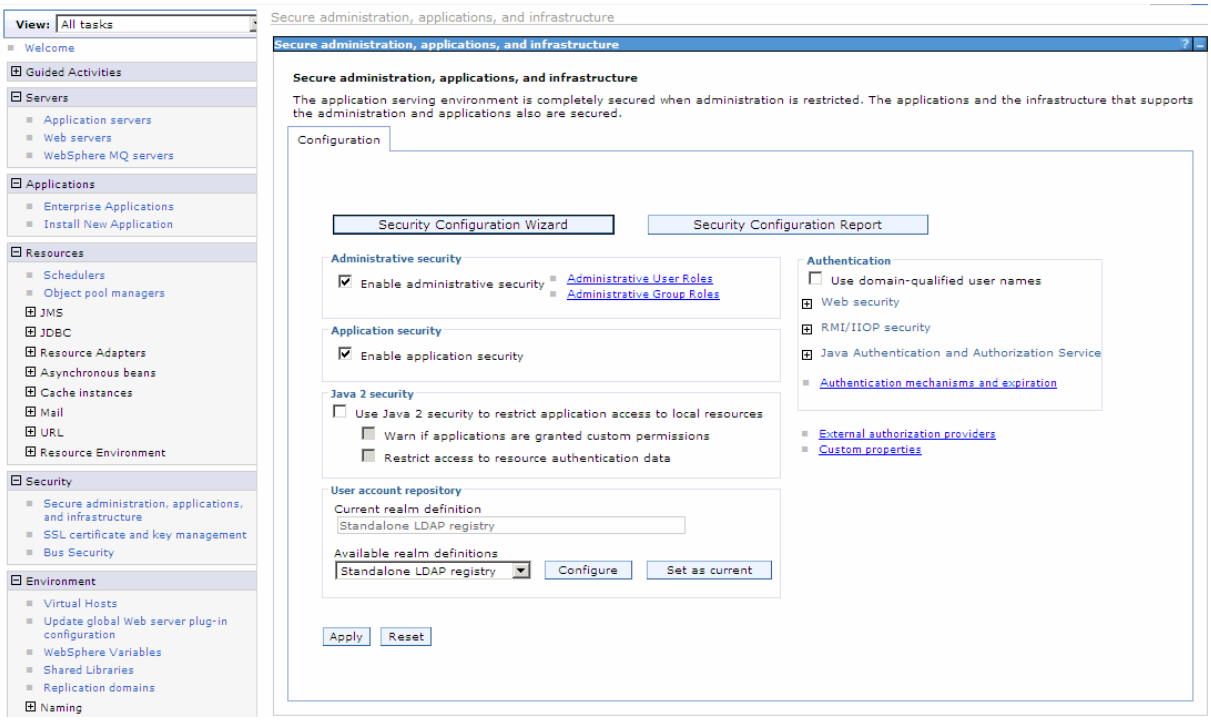

Figure 1: Secure administration, applications, and infrastructure

4 Click **Security Configuration Wizard**.

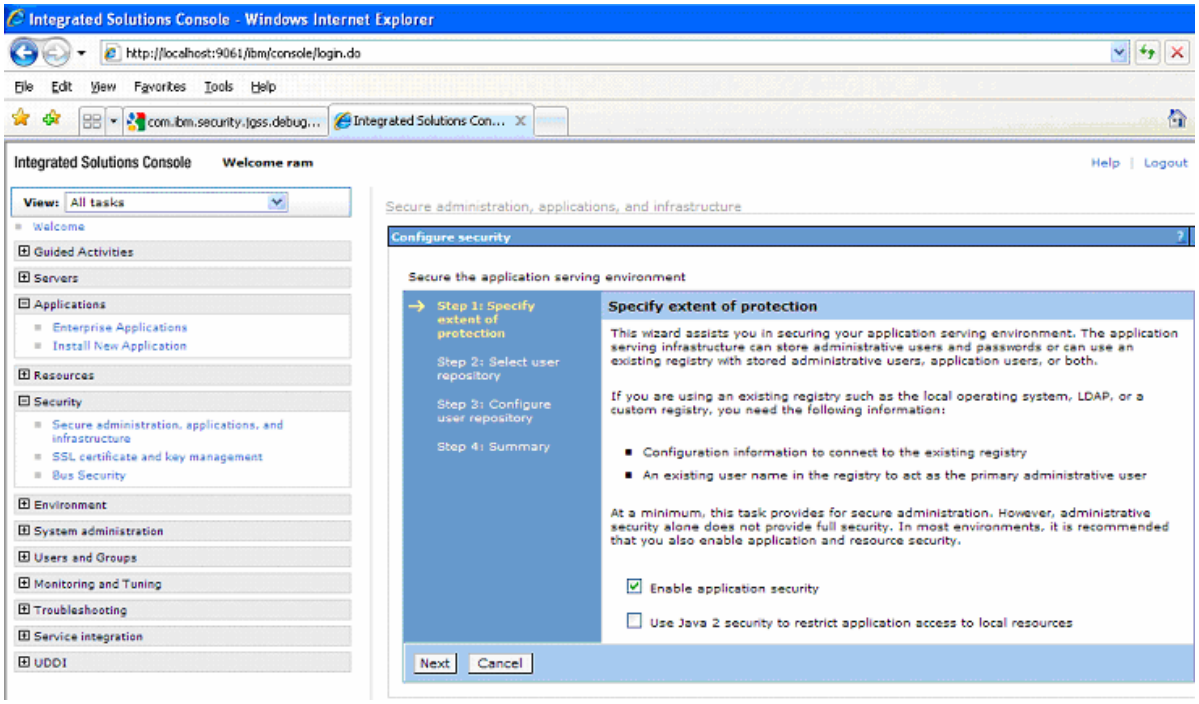

Figure 2: Configure security

5 Select the **Enable application security** check box.

6 Click **Next**.

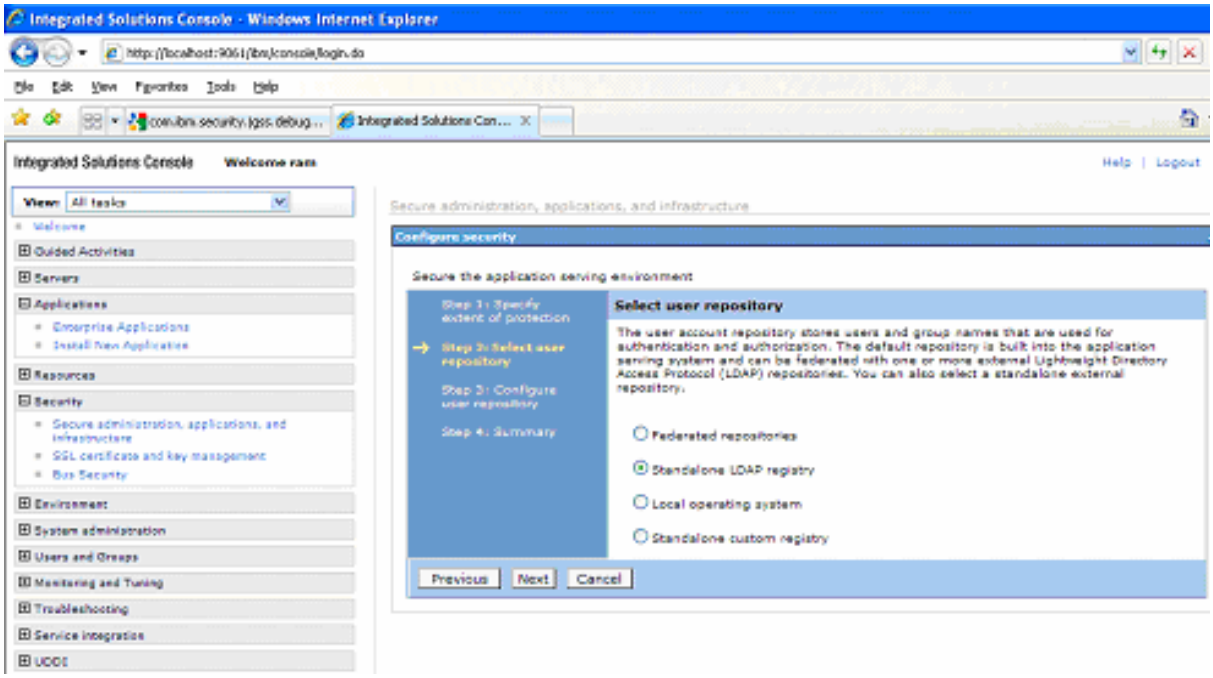

Figure 3: Select user repository

7 Select **Standalone LDAP registry**.

8 Click **Next**.

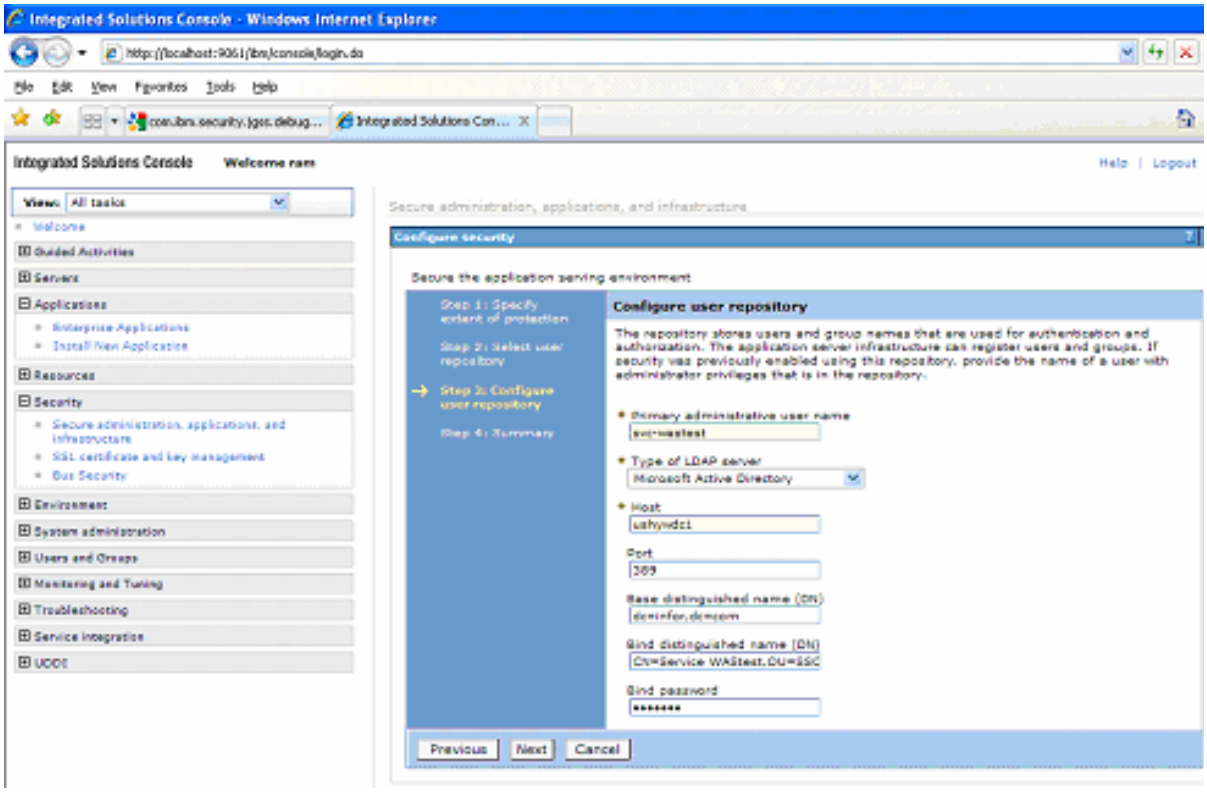

Figure 4: Configure user repository

9 On the Configure user repository screen, specify this information:

Primary Administrative User Name

Specify your Active Directory user name, for example, **wasadmin**. This user profile name is used to authenticate against Active Directory.

Type of LDAP server

Select **Microsoft Active Directory**.

Host

Specify the Host name for Active Directory, for example, **mywdc1**. This is the Active Directory server.

Port

Specify the port.

Base distinguished name

Example: **dc=myco,dc=com**

Bind distinguished name

Example: **CN=Service WASAdmin,OU=SSO,OU=Service Accounts,DC=myco,DC=com)**

Bind password

Specify the password for the Active Directory user profile.

10 Click **Next**.

11 Click **Finish**.

12 Select **Save**.

13 Expand the **Web Security** node.

14 Select **General Settings**.

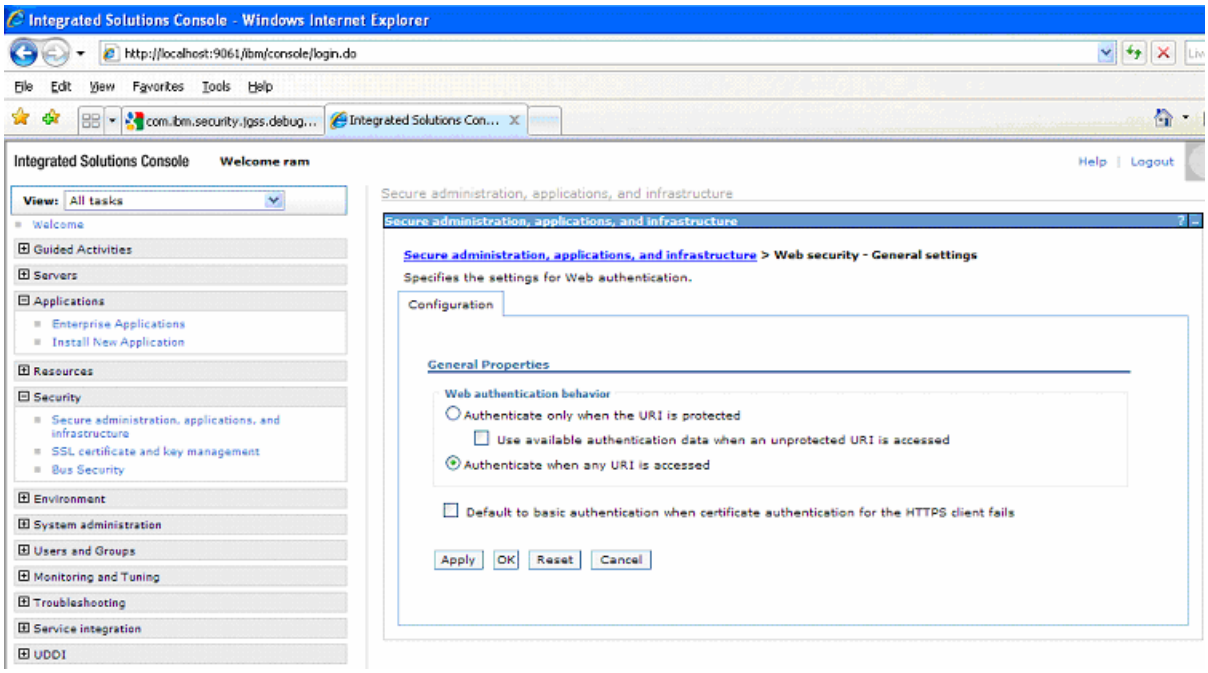

Figure 5: General Properties

15 Select **Authenticate when any URI is accessed**.

16 Click **Apply**.

17 Select **Save**.

18 Close the Admin Console.

19 Stop the WAS Server.

20 Run snoop servlet again to ensure that the server is stopped.

Updating WebSphere Application Server Service

After security has been applied to a given WebSphere Application Server profile, a user ID and password are required to stop the service. To update the service so that the proper user ID and password are used to stop the service, run the WASService.exe. After WASService.exe is successfully run, a user profile and password popup is no longer presented when you stop the profile.

To run the WASService.exe program:

1 Open a command window.

2 Change to the [WAS install dir]\bin directory.

3 Enter the following command, replacing the parameters, including the brackets, as shown in the table below.

C:\IBM\6.1\WebSphere\AppServer\bin>WASService.exe -add [Service Name] -serverName [server name] –profilePath [path to profile] -stopArgs "-username [userID] -password [password]"

Parameter	Description
[Service Name]	Name of the given service. Example: **mymachineNode01**
[server name]	Name of the server. Example: **server1**
[path to profile]	DOS path down to and including the profile name. Example: **c:\ibm\websphere\appserver\profiles\default**
[userID]	User ID that you entered in Step 9 of "Configuring WebSphere to use security."
[password]	Password that you entered in Step 9 of "Configuring WebSphere to use security."

4 Start the WAS Server.

5 Run snoop servlet again.

6 When prompted, enter an Active Directory user ID and password.

7 Press **Enter** to display the snoop servlet page.

Installing the identity token application

The identity token installation consists of two parts. The first part is the installation of the identity Token resource adapter. The second part is the installation of the identity token test application. Installing the identity token test application validates that the identity token resource adapter is set up and verifies the EIM configuration.

Installing the Identity Token resource adapter

To install the Identity Token resource adapter:

1. From the Start menu, select **All Programs/IBM WebSphere/Application Servers/Profiles/{Profile Name}/Administrative Console**. Because you have enabled security, you must enter the user ID and password that you used during the security setup.
2. Specify the user ID, for example, **wasadmin**.
3. Specify the password.
4. Press **Enter**.
5. If you get the message **There is a problem with this website's security certificate**, select **Continue to the website (not recommended)**.
6. You have the option to add the certificate as a trusted certificate.
7. If the browser displays a single graphic, click **Back** and log on again.
8. After you are successfully logged on, expand the **Resources** menu topic.
9. Expand the **Resource adapters** drop down.
10. Select the **Resource adapters** link.

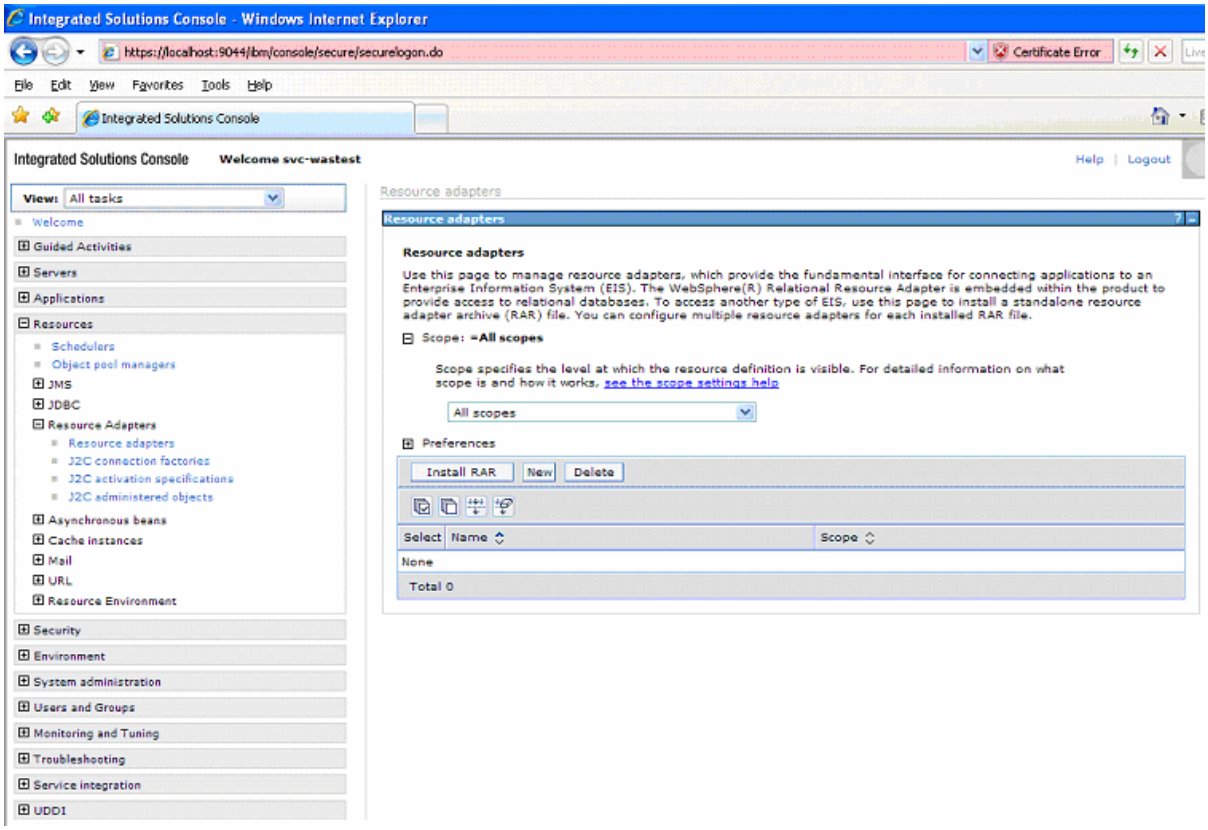

Figure 6: Resource adapters

11 Select **Node only** in the Scope drop down.

12 Click **Install RAR**.

13 Click the browse button.

14 Using a mapped drive to the System i, go to /QIBM/Proddata/os400/security/eim, and select the **idTokenRA.rar**.

15 Click **Next**.

16 Click **OK**.

17 Select **Save**.

Setting up J2C authentication data

In this section, enter the user ID and password that are used by the adapter to connect to the EIM Active Directory server.

To set up the user ID and password:

1 Expand the **Security** topic.

2 Select **Secure administration, applications, and infrastructure**.

3 Expand **Java Authentication and Authorization Service**.

4 Select **J2C authentication data**.

5 Click **New**.

6 Enter **idTokenAlias** in the **Alias** field.

7 Enter **cn=Administrator** in the **User ID** field.

8 Enter the password for the EIM active directory.

9 Click **OK**.

10 Select **Save**.

Configuring the Identity Token J2C connection factory

To configure the connection:

1 Expand the **Resources** topic.

2 Expand the **Resource Adapters** topic.

3 Select **J2C connection factories**.

4 Select **Node only** in the **Scope** drop down.

5 Click **New**.

6 Enter **idtokenconnection** in the **Name** field

7 Enter **eis/IdentityToken** in the **JNDI name** field

8 Select the idTokenAlias from the **Component managed authentication alias** drop down.

9 Select the idTokenAlias from the **Container Managed authentication** drop down.

10 Select **None** from the authentication **Preference** drop down.

11 Select **DefaultPrincipleMapping** from the **Mapping configuration Alias** drop down.

12 Click **OK**.

13 Select **Save**.

14 Select the newly created idtokenconnection connection factory link.

15 Select **custom properties** from **Additional Properties**.

16 Select **LdapHostName**.

17 In value field, specify the EIM LDAP directory Server. Example: **MYSYSTEMI.myco.com**. Enter this value exactly as it appears in the properties value of the EIM domain under the domain controller field. Case of this entry is very important.

18 Click **OK**.

19 Select **Save**.

20 Select the **EimDomainName**.

21 Enter the EIM domain name in the value field (example: **EIMMYSYSTEMI**). This value can be found in the properties value of the domain under the domain field.

22 Click **OK**.

23 Select **Save**.

24 Select the **SourceRegistryName**.

25 Enter the source user registry name that was setup in EIM. This name is used to validate the user and to get the target user ID in the value field. Example: **MYCO.COM**.

26 Click **OK**.

27 Select **Save**.

28 Select the **KeyTimeoutSeconds**.

29 Enter **43200** in the value field.

30 Click **OK**.

31 Select **Save**.

32 Select **UseSSL**.

33 Enter **false** in the value field.

34 Click **OK**.

35 Select **Save**.

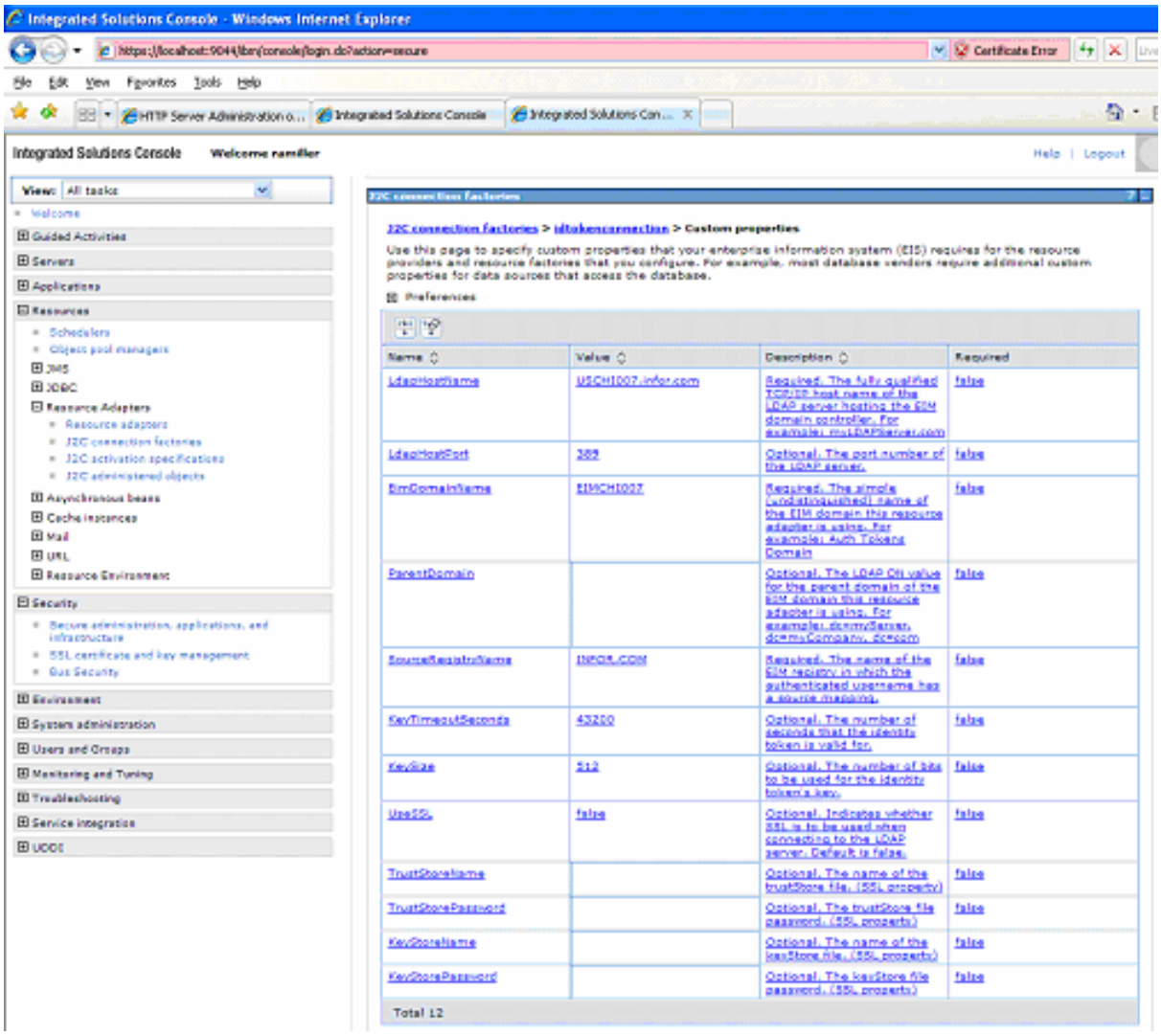

Figure 7: Custom Properties

Installing the identity token test application

In this part of the installation, you will copy the required JAR files from the System i to the windows WAS server.

To copy the JAR files:

1 Go to the /QIBM/ProdData/OS400/security/eim folder on a mapped drive to the System i.

2 Select the eim.jar, **eimos400.jar**, right click, and select **Copy**.

3 Go to the IBM Appserver directory, for example: c:\Program Files\IBM\WebSphere\AppServer\lib\ext. Right click and select **Paste**. This action copies the two

jar files from the IFS directory on the System i to the file system of the Wndows WebSphere server.

4 Go to the /QIBM/ProdData/HTTP/Public/jt400/lib folder on a mapped drive to the System i.

5 Select the jt400.jar, right click, and select **Copy**.

6 Go to the IBM Appserver directory, for example: c:\Program Files\IBM\WebSphere\AppServer\lib\ext. Right click and select **Paste**. This action copies the jt400.jar from the IFS directory of the System i to the file system of the Windows WebSphere server.

Installing the identity Token Ear file

To install the EAR file:

1 Expand the **Applications** topic.

2 Select **Enterprise Applications**.

3 Click **Install**.

4 Select the browse button.

5 Using a mapped drive to the System i, go to /QIBM/Proddata/os400/security/eim, and select the testidentitytoken.ear.

6 Click **Open**.

7 Click **Next**.

8 Click **Next**.

9 Select the **TestIdentityTokenWeb** check box.

10 Select all Clusters and servers.

11 Click **Apply**.

12 Click **Next**.

13 Click **Finish**.

14 Select **Save**.

15 Select the **testidentitytoken application** check box.

16 Click **Start**.

17 Open a browser.

18 Enter the following URL: Error! Hyperlink reference not valid., changing **host** and **port** to the appropriate values.

19 Because security is enabled, you should be challenged for a user ID and password.

20 Enter a valid active directory username and password. The Identity Token Test Client JSP page is displayed.

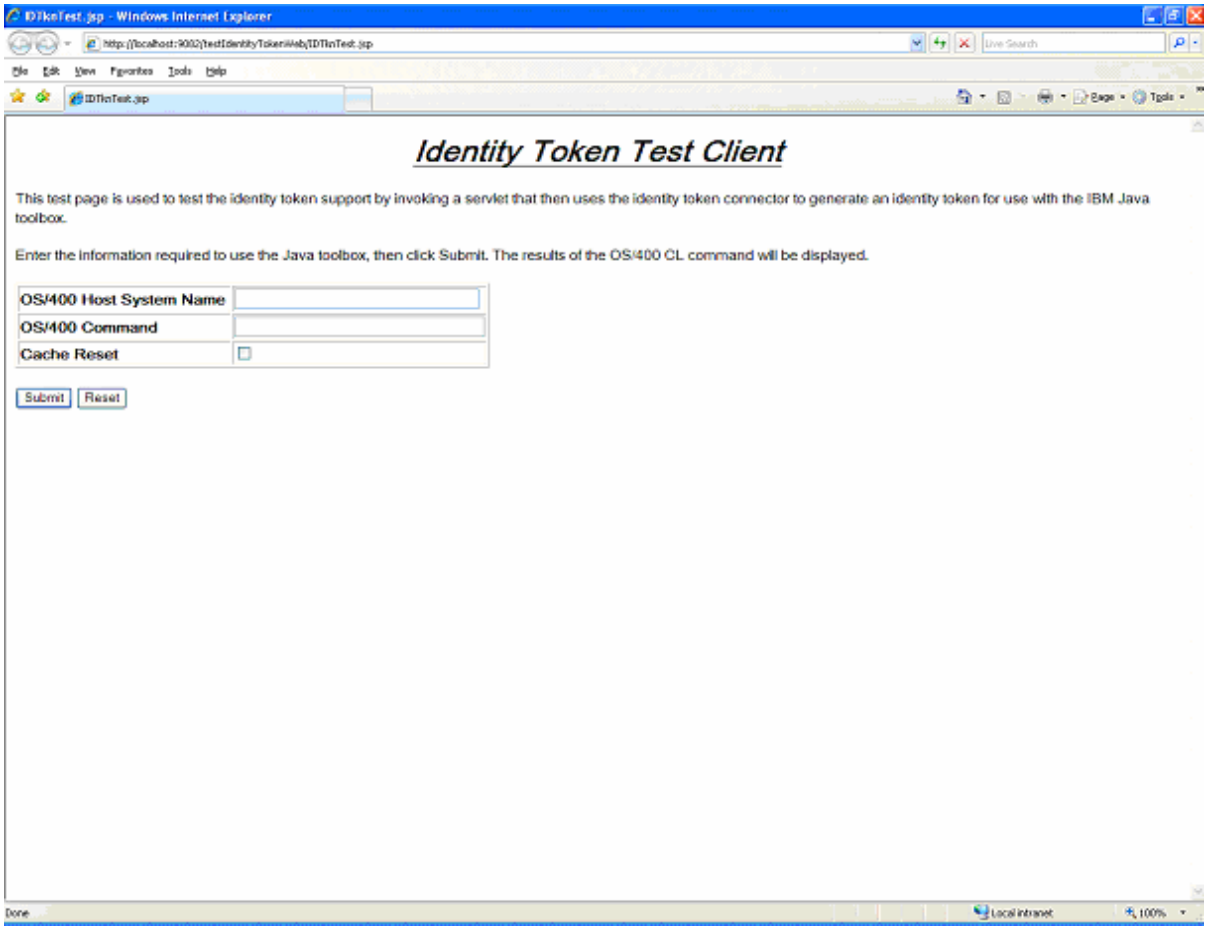

Figure 8: Identity Token Test Client

21 Enter an **OS/400 Host System Name** that is set up in EIM.

22 Enter an OS/400 command. Example: **crtlib #TEST1234**.

23 Click **Submit**. If everything is set up correctly, the following screen is displayed.

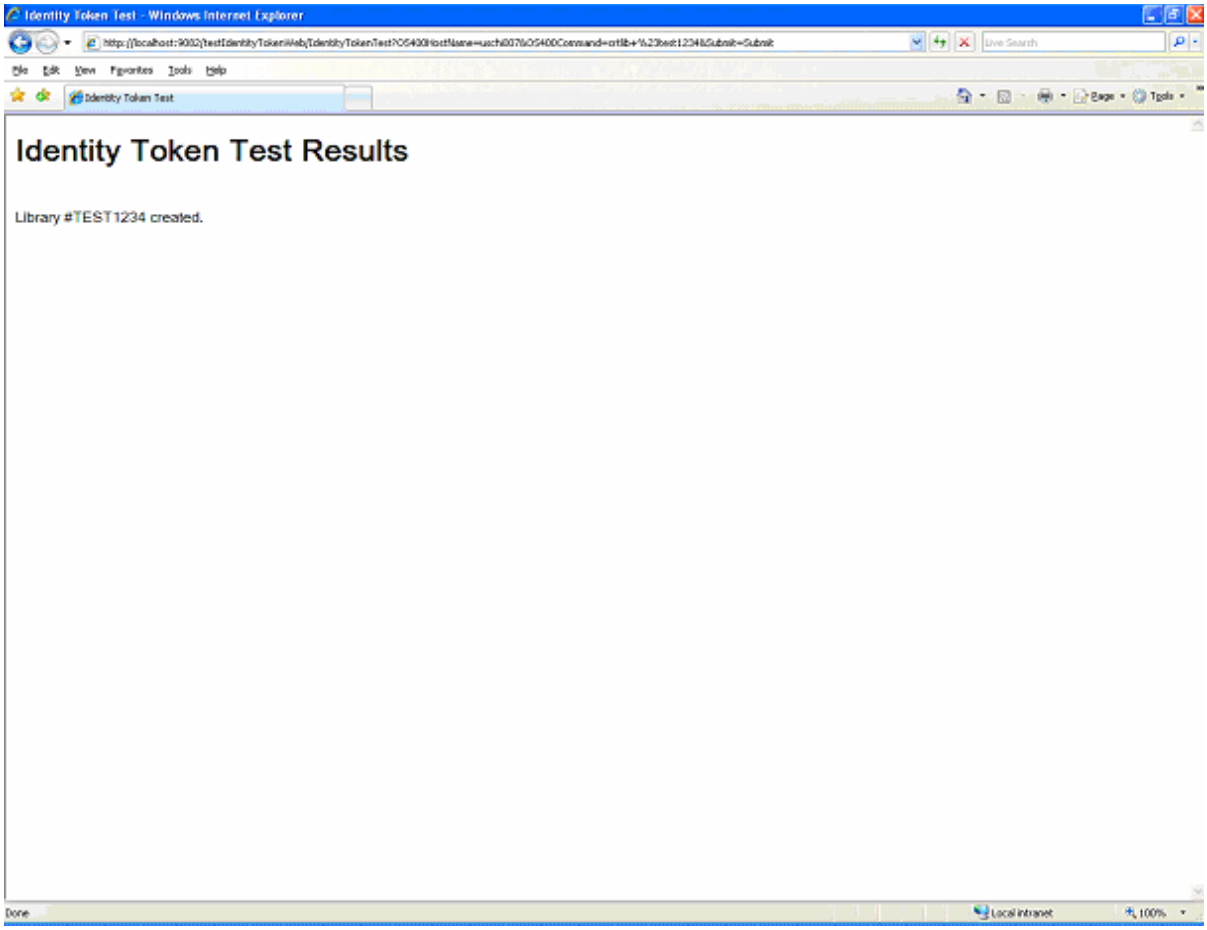

Figure 9: Identity Token Test Results

Installing SPNEGO

Read the “Single Server SPNEGO” section of the *WebSphere with a side of SPNEGO* white paper from IBM (http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101065). This white paper explains how to set up SPNEGO with WebSphere.

To install SPNEGO, create a virtual host name as described below. The steps that follow are adapted from the IBM whitepaper.

Create a virtual host name for WebSphere

Because WebSphere runs on a Windows server, and because the active directory contains entries for the Windows server, SPNEGO requires the use of a virtual host name.

WebSphere 6.1 uses the ISSW SPNEGO TAI. The virtual host cannot be set up as an alias. Your IT department must set up an additional name as an A record in the DNS with the same IP address as your WAS server. This name cannot be set up as an alias (CNAME).

See this IBM document for additional information: (http://www.ibm.com/developerworks/websphere/library/techarticles/0809_lansche/0809_lansche.html)

Step 1 – Generate a user ID for application server

Your IT department must set up a new user to be used to validate users to the active directory. Refer to the step 1 in the *WebSphere with a Side of SPNEGO* white paper.

Step 2 – Assign the Service Principle Name and create a key file

After you have a user ID and virtual host, you must create the keytab file for this user. Refer to Step 2 in the *WebSphere with a Side of SPNEGO* white paper.

```
ktpass -princ HTTP/mywas.myco.com@MYCO.COM -mapuser wasadmin @myco.com -
pass waspw1234 -out c:\winnt\mywas.keytab -crypto DES-CBC-MD5
```

Be sure you have the correct version of ktpass. Check this Microsoft document for the latest version:

http://support.microsoft.com/kb/919557/en-us

Step 3 – Set up Kerberos Configuration on the application server

1 Open a text editor such as Notepad.

2 Copy the following lines into the open editor.

```
[libdefaults]
default_realm = {Uppercase Kerberos realm}
default_keytab_name = FILE:{keytab file location and name}
default_tkt_enctypes = des-cbc-md5 rc4-hmac
default_tgs_enctypes = des-cbc-md5 rc4-hmac
kdc_default_options = 0x54800000
[realms]
{Uppercase Kerberos realm }= {
kdc = {key distribution center name}:88
default_domain = {lower case domain name}
}
[domain_realm]
.{lower case domain name} = {Uppercase Kerberos realm}
```

3 Change these parameters:

Parameter	Description
{Uppercase Kerberos realm}	Specify the Kerberos realm name. Upper case is required.
{keytab file location and name}	Specify the location and name of the keytab file. Example: c:\winnt\mywas.keytab
{key distribution center name}	Specify the domain's KDC.
{lower case domain name}	Specify the lower case domain name.

4 Save the file on the file system of the WebSphere server as “krb5.conf”. Records that begin with # are comments and are optional.

This is an example of a completed file:

```
[libdefaults]
  default_realm = MYCO.COM
  default_keytab_name = FILE:c:\winnt\mywas.keytab
  default_tkt_enctypes = des-cbc-md5 rc4-hmac
```

```
  default_tgs_enctypes = des-cbc-md5 rc4-hmac
  kdc_default_options = 0x54800000
# forwardable = true
# proxiable = true
# noaddresses = true
[realms]
  MYCO.COM = {
    kdc = mywdc1:88
    default_domain = myco.com
  }
[domain_realm]
  .myco.com = MYCO.COM
```

Step 4 – Enable WebSphere Security

WebSphere security was enabled earlier. No further action is required.

Step 5 – Enable SSO

To enable single sign on:

1. Expand the **security** menu node.
2. Select the **Secure Administration, applications and infrastructure**.
3. Expand the **Web security** node.
4. Select **single sign-on (SSO)**.
5. Make sure that **Enabled** is checked.
6. Click **OK**.
7. Select **Save** if prompted.

Step 6 – Enable trust association

To enable trust association:

1. Expand the **security** menu node.
2. Select the **Secure Administration, applications and infrastructure**.
3. Expand the **Web security** node.

4 Select **Trust association**.

5 Make sure that **Enabled trust association** is checked.

6 Click **OK**.

7 Select **Save**.

8 Expand the **Web security** node.

9 Select **Trust association**.

10 Select **Interceptors**.

11 Select **com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl**.

12 Select the **Custom Properties**.

13 Click **New**.

14 In the **Name** field, specify **com.ibm.ws.security.spnego.SPN1.enableCredDelegate**.

15 In the **Value** field, specify **true**.

16 Click **OK**.

17 Select **Save**.

18 Click **New**.

19 In the **Name** field, specify **com.ibm.ws.security.spnego.SPN1.hostName**.

20 In the **Value** field, specify the fully qualified virtual host name from Step A. Example: **mywas.myco.com**. This name is the virtual host name.

21 Click **OK**.

22 Select **Save**.

Step 7 – Disable Security Pre-Invoke

This step is not required at this time.

Step 8 – Enable SPNEGO at the JVM level

To enable SPNEGO:

1 Expand the **Servers** menu node.

2 Select **Application servers**.

3 Select your server, typically, **server1**.

4 Expand the **Java and process management** topic.

5 Select **Process Definition**.

6 Select **Java Virtual Machine**.

7 Select **Custom Properties**.

8 Click **New**.

9 In the **Name** field, specify **com.ibm.security.jgss.debug**.

10 In the **Value** field, specify **off**.

11 Click **OK**.

12 Select **Save**.

13 Click **New**.

14 In the **Name** field, specify **com.ibm.security.krb5.Krb5Debug**.

15 In the **Value** field, specify **off**.

16 Click **OK**.

17 Select **Save**.

18 Click **New**.

19 In the **Name** field, specify **com.ibm.ws.security.spnego.isEnabled**.

20 In the **Value** field, specify **true**.

21 Click **OK**.

22 Select **Save**.

23 Click **New**.

24 In the **Name** field, specify **java.security.krb5.conf**.

25 Specify the path to the Kerberos config file. This path and file name were created in Step 3 above. Example: **c:\development\krb\krb5.conf**.

26 Click **OK**.

27 Select **Save**.

Step 9 – Turn on SPNEGO Logging and Tracing

This step is not required at this time. If you encounter any issues, this may have to be turned on to debug a problem.

Step 10 – Restart WebSphere

No steps should be necessary to do this. Make sure the WAS server stops by using the snoop servlet. If a page not found message is displayed, the WAS server has been stopped.

Step 11 – Configure Browsers

Perform steps in document.

Step 12 – Test the configuration

To test the configuration:

1. Open a browser.
2. Enter this URL:

   http://{host}:{port}/testIdentityTokenWeb/IDTknTest.jsp, change the host and port to the appropriate values. Make certain that the host name is fully qualified with the default domain name and the host name defined in step A.

   Example: **http://mywas.myco.com:9083/testIdentityTokenWeb/IDTknTest.jsp**

   SPNEGO is now configured so there should be no authentication challenge.
3. Enter a command. Example: **crtlib #TEST1234**
4. Click **Submit**. If everything is set up correctly, the following screen is displayed.

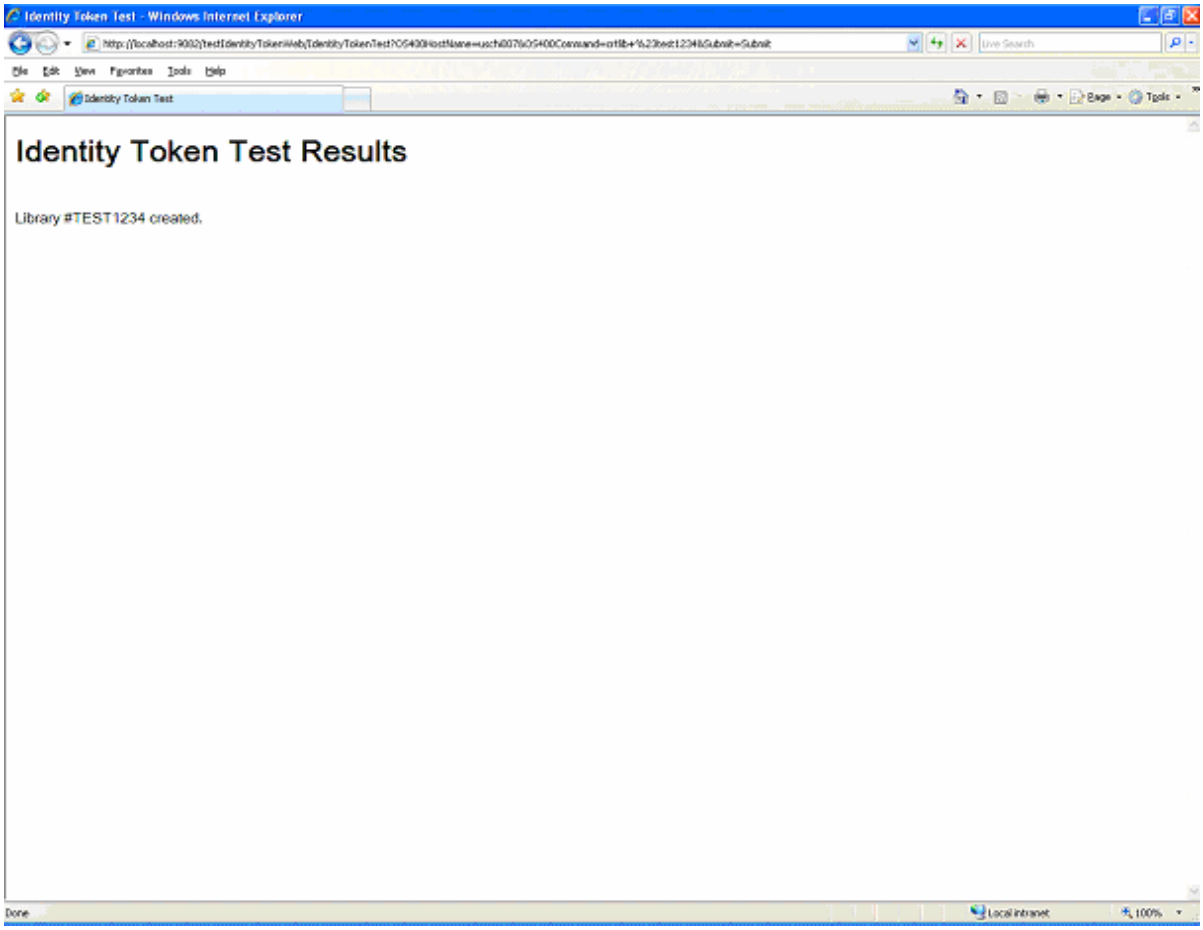

Figure 10: Identity Token Test Results

Step 13 – Update HTTP Configuration

To update the HTTP configuration increasing the request field size:

1. Open the httpd.conf file in a text editor, for example: TEXTPAD.
2. Type **16380** as the HTTP Directive **LimitRequestFieldSize**.
3. Save the changes to the httpd.conf file.
4. Stop the HTTP server.
5. Start the HTTP server.