Infor WebTop Configuring WebSphere Application Server to Use Single Sign-on for Infor WebTop

Important Notices

Trademark Acknowledgements

Publication Information

Release: Infor WebTop 4.5

Publication date: August 18, 2014

Document code: WTCWASSSO_4.5_01

Contents

Introduction

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 IBM i. IBM provides several good 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 IBM 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 onto the system, reboot your PC to clear the cached logon credentials.

Prerequisites

- IBM i 6.1
- EIM installed and running on the IBM i server
    - AES Encryption used

      Make certain that Active Directory entries have *ONLY* AES encryption checked.
    - IBM i PTFs are required to support AES Encryption
    - V7R1
        - SI46494 Product: 5770SS1 Immediate Apply
          Note: Configuration changes required are documented in the PTF cover letter.
        - SI48602 Product: 5770SS1 Immediate Apply
        - SI43918 Product: 5770SS1 Immediate Apply
    - V6R1
        - SI46496 Product: 5761SS1 Immediate Apply
        - SI49022 Product: 5761SS1 Immediate Apply
        - SI43919 Product: 5761SS1 Immediate Apply
    - V5R4
        - SI46630 Product: 5722SS1 Immediate Apply
          Note: Configuration changes required are documented in the PTF cover letter.
        - SI47896 Product: 5722SS1 Immediate Apply
        - SI43920 Product: 5722SS1 Immediate Apply
- WAS v8.0.0.8 or higher. These instructions use WAS 8.5.5.1 Base.
- Using Microsoft Active Directory for authentication running on Windows Server 2008 Client Machine running Windows 7 Enterprise
- Default Application loaded and running for use of snoop servlet

Sample installation checklist

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

Item	Value (examples)
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 is 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)	eimpw1234 (This is a sample password. Do not use it in your installation.)
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
WAS system virtual name (new name in DNS for WAS system HTTP access). Do not create as an alias.	mywas

Item	Value (examples)
Domain Service Principal User ID for WebSphere Application Server system (for authenticating users)	myco\mywas
Uppercase Kerberos realm (this must be in 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 is set up correctly and running

Follow the instructions in this section to set up WAS to use Active Directory to perform authentication. These instructions were developed using a WAS 8.5.5.1 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:

   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 8.0.0.8 or higher.

Configuring WebSphere to use security

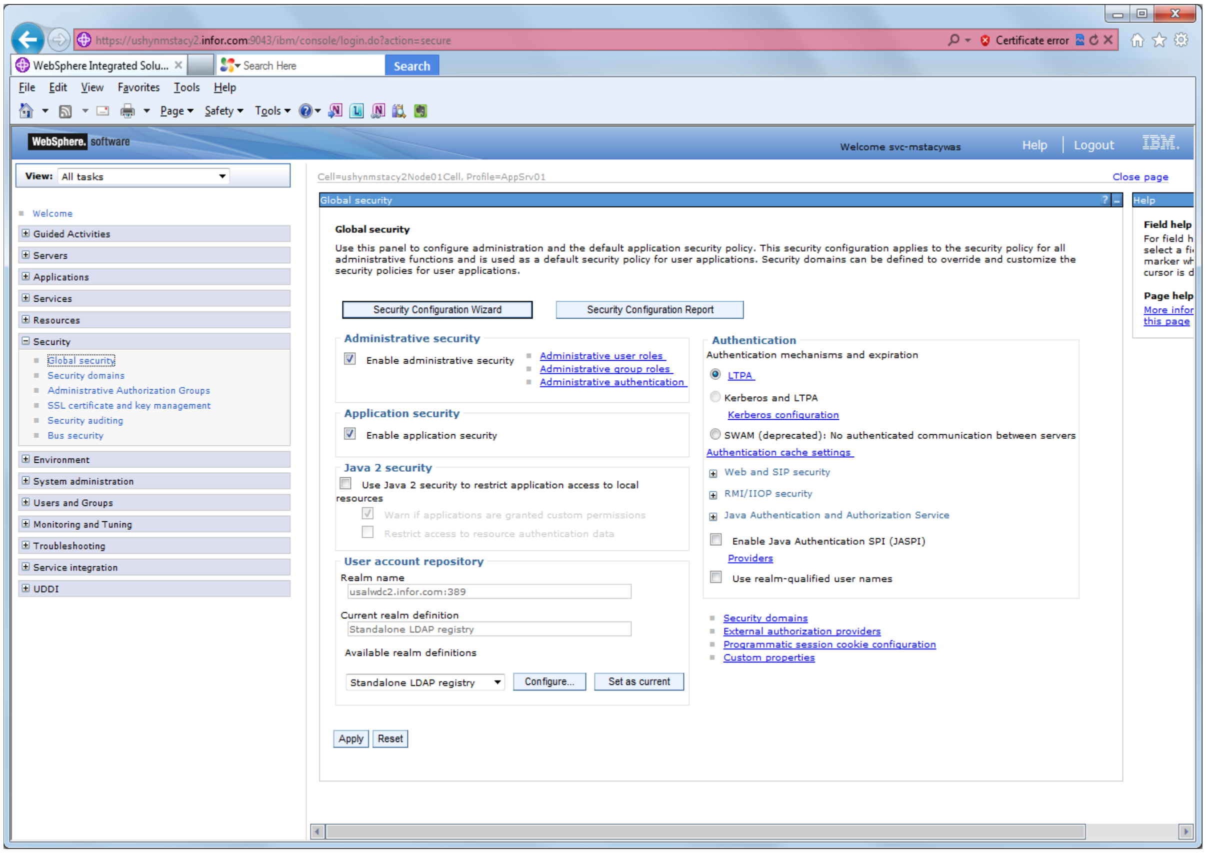
After you set up security, you will be prompted to open the Admin console. You must enter the user ID and password that you set up below. If the WebSphere server is set up to run as a service, you may not be able to stop it from the service screen, but only from the menu, after you enter the user ID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



Cell=ushynmstacy2Node01Cell, Profile=AppSrv01

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Realm name: usalwdc2.infor.com:389

Current realm definition: Standalone LDAP registry

Available realm definitions: Standalone LDAP registry | Configure... | Set as current

Authentication

Authentication mechanisms and expiration

● LTPA

○ Kerberos and LTPA

Kerberos configuration

○ SWAM (deprecated): No authenticated communication between servers

Authentication cache settings

⊞ Web and SIP security

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

□ Enable Java Authentication SPI (JASPI)

Providers

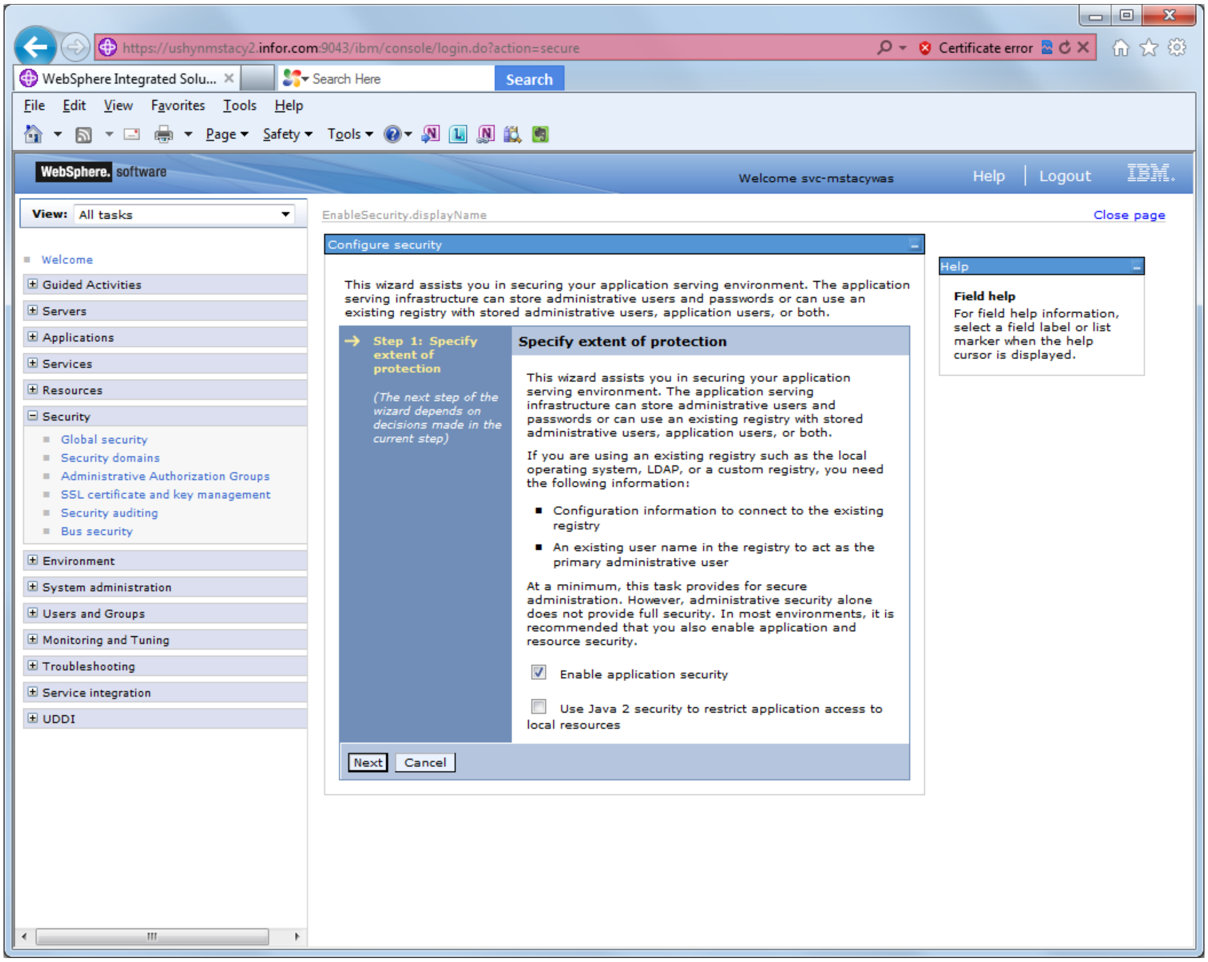
□ Use realm-qualified user names

- Security domains
- External authorization providers
- Programmatic session cookie configuration
- Custom properties

Apply | Reset

Figure 1: Global security

4 Click **Security Configuration Wizard**. The page below is displayed.



Configure security

This wizard assists you in securing your application serving environment. The application serving infrastructure can store administrative users and passwords or can use an existing registry with stored administrative users, application users, or both.

→ Step 1: Specify extent of protection

(The next step of the wizard depends on decisions made in the current step)

Specify extent of protection

This wizard assists you in securing your application serving environment. The application serving infrastructure can store administrative users and passwords or can use an existing registry with stored administrative users, application users, or both.

If you are using an existing registry such as the local operating system, LDAP, or a custom registry, you need the following information:

- Configuration information to connect to the existing registry
- An existing user name in the registry to act as the primary administrative user

At a minimum, this task provides for secure administration. However, administrative security alone does not provide full security. In most environments, it is recommended that you also enable application and resource security.

☑ Enable application security

☐ Use Java 2 security to restrict application access to local resources

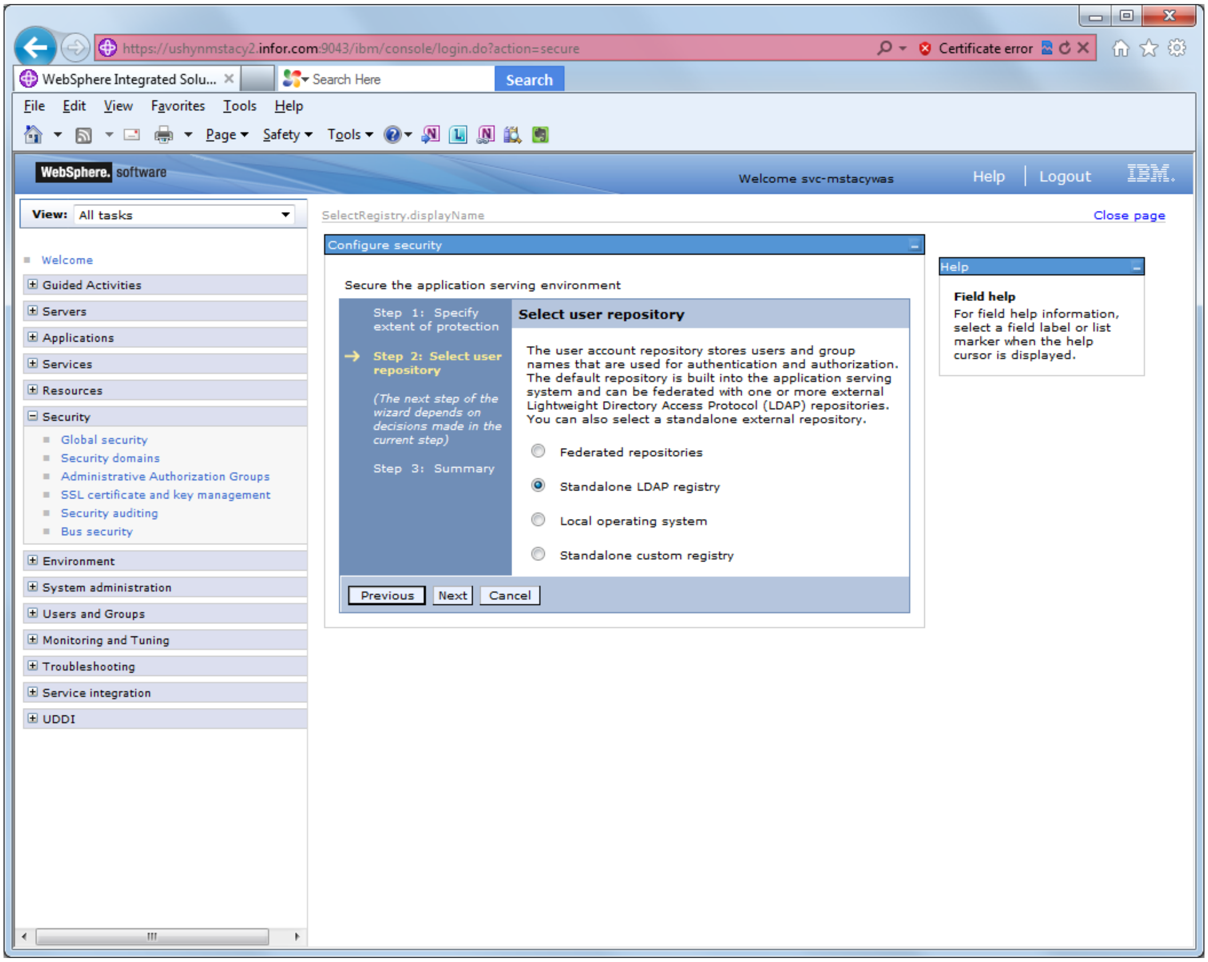
Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Figure 2: Configure security - Step 1: Specify extent of protection

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

6 Click **Next**. The page below is displayed.



Configure security

Secure the application serving environment

Step 1: Specify extent of protection

→ Step 2: Select user repository

(The next step of the wizard depends on decisions made in the current step)

Step 3: Summary

Select user repository

The user account repository stores users and group names that are used for authentication and authorization. The default repository is built into the application serving system and can be federated with one or more external Lightweight Directory Access Protocol (LDAP) repositories. You can also select a standalone external repository.

○ Federated repositories

● Standalone LDAP registry

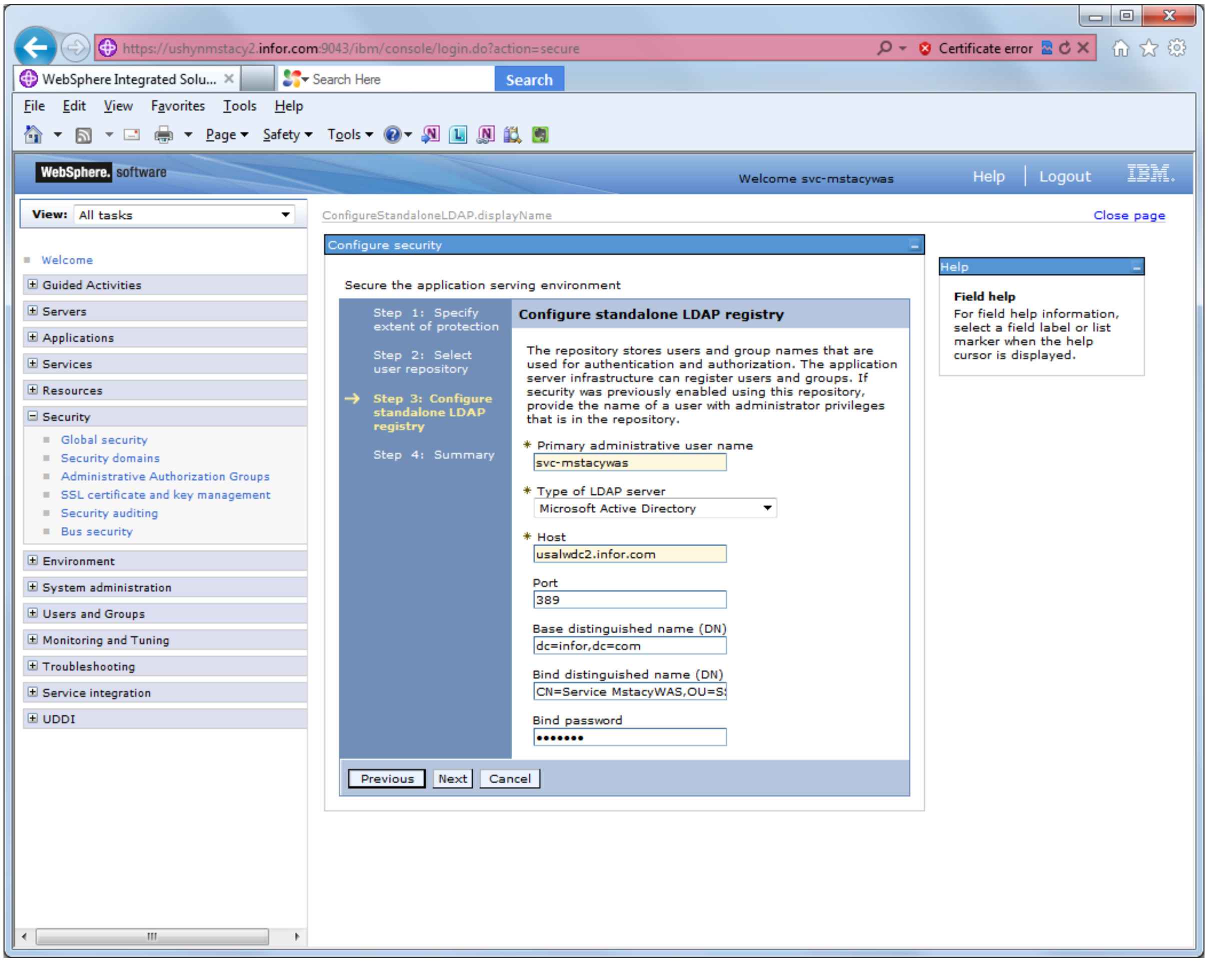
○ Local operating system

○ Standalone custom registry

Figure 3: Configure security - Step 2: Select user repository

7 Select **Standalone LDAP registry**.

8 Click **Next**. The page below is displayed.



Secure the application serving environment

Configure standalone LDAP registry

The repository stores users and group names that are used for authentication and authorization. The application server infrastructure can register users and groups. If security was previously enabled using this repository, provide the name of a user with administrator privileges that is in the repository.

* Primary administrative user name: svc-mstacywas

* Type of LDAP server: Microsoft Active Directory

* Host: usalwdc2.infor.com

Port: 389

Base distinguished name (DN): dc=infor,dc=com

Bind distinguished name (DN): CN=Service MstacyWAS,OU=S

Bind password: •••••••

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Figure 4: Configure security - Step 3: Configure standalone LDAP registry

9 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

Specify the base distinguished name, for example, **dc=myco,dc=com**

Bind distinguished name

Specify the bind distinguished name, for example, **CN=Service WASAdmin,OU=SSO,OU=Service Accounts,DC=myco,DC=com)**

Bind password

Specify the password for the Active Directory user profile.

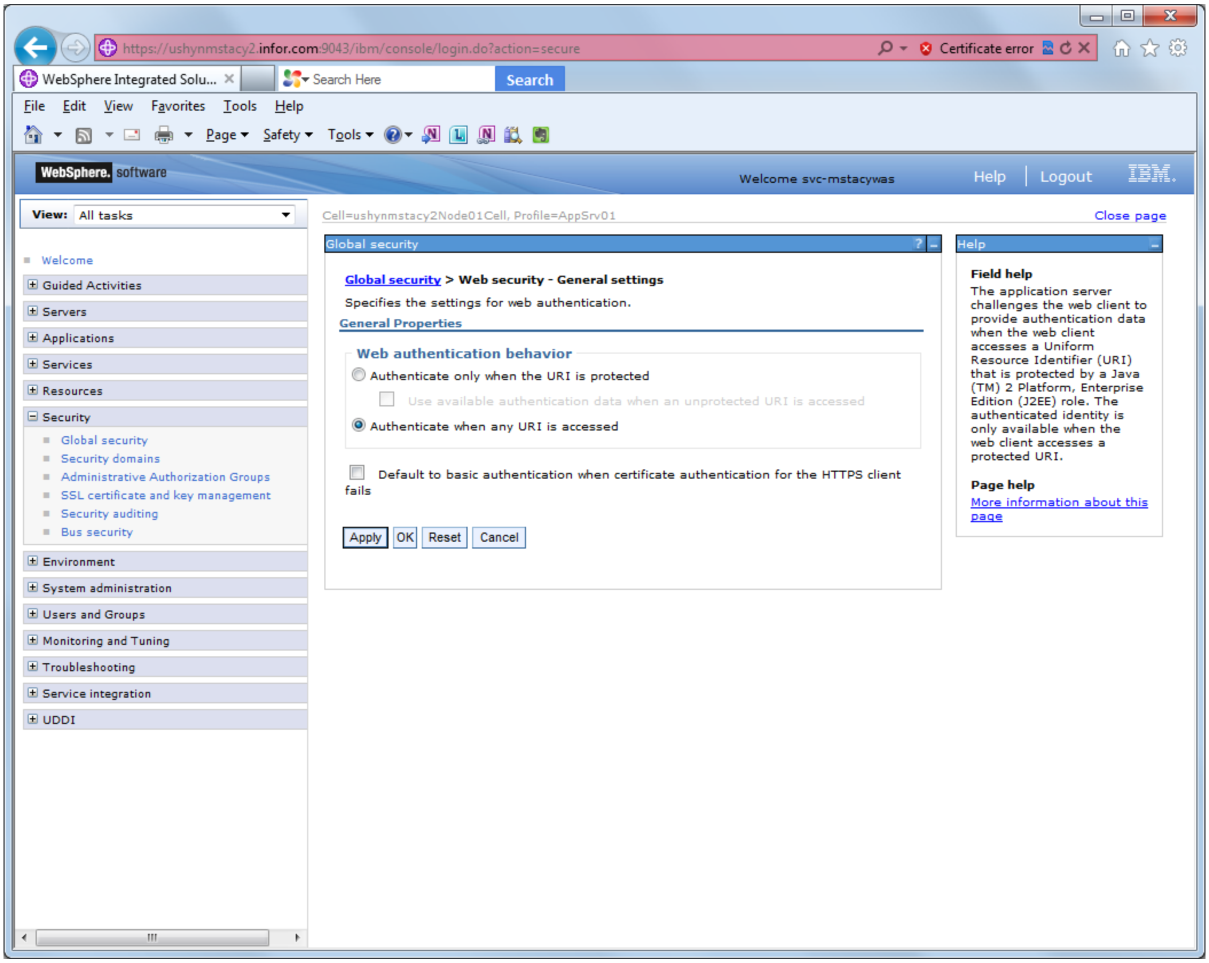
10 Click **Next**.

11 Click **Finish**.

12 Select **Save**.

13 Expand the **Web and SIP security** topic in the Authentication area.

14 Select **General Settings**. The page below is displayed.



Global security > **Web security - General settings**

Specifies the settings for web authentication.

General Properties

Web authentication behavior

○ Authenticate only when the URI is protected

□ Use available authentication data when an unprotected URI is accessed

● Authenticate when any URI is accessed

□ Default to basic authentication when certificate authentication for the HTTPS client fails

Apply | OK | Reset | Cancel

Field help

The application server challenges the web client to provide authentication data when the web client accesses a Uniform Resource Identifier (URI) that is protected by a Java (TM) 2 Platform, Enterprise Edition (J2EE) role. The authenticated identity is only available when the web client accesses a protected URI.

Page help

More information about this page

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\8.5\WebSphere\AppServer\bin>WASService.exe -add [Service Name] -serverName [server name] –profilePath [path to profile] -stopArgs "-username [userID] -password [password]"

   For example:

   C:\IBM\v85\WebSphere\AppServer\bin>WASService.exe -add WAS85TWO -serverName server2 -profilePath c:\ibm\v85\WebSphere\appserver\profiles\AppSrv02 -stopArgs "-username svc-mstacysso -password P$sswUrd"

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 the **Primary Administrative User Name** field in Step 9 of the “Configuring WebSphere to use security” section
[password]	Password that you entered in the **Bind password** field in Step 9 of the “Configuring WebSphere to use security” section.

You should see the following in your command prompt:

```
Adding Service: WAS85TWO
```

```
Config Root: c:\ibm\v85\WebSphere\appserver\profiles\AppSrv02\config
 Server Name: server2
  Profile Path: c:\ibm\v85\WebSphere\appserver\profiles\AppSrv02
  Was Home: C:\IBM\v85\WebSphere\AppServer\
  Start Args:
 Restart: 1
Service already exists, updating parameters...
```

4. Start the WAS Server.
5. Run the 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)**.

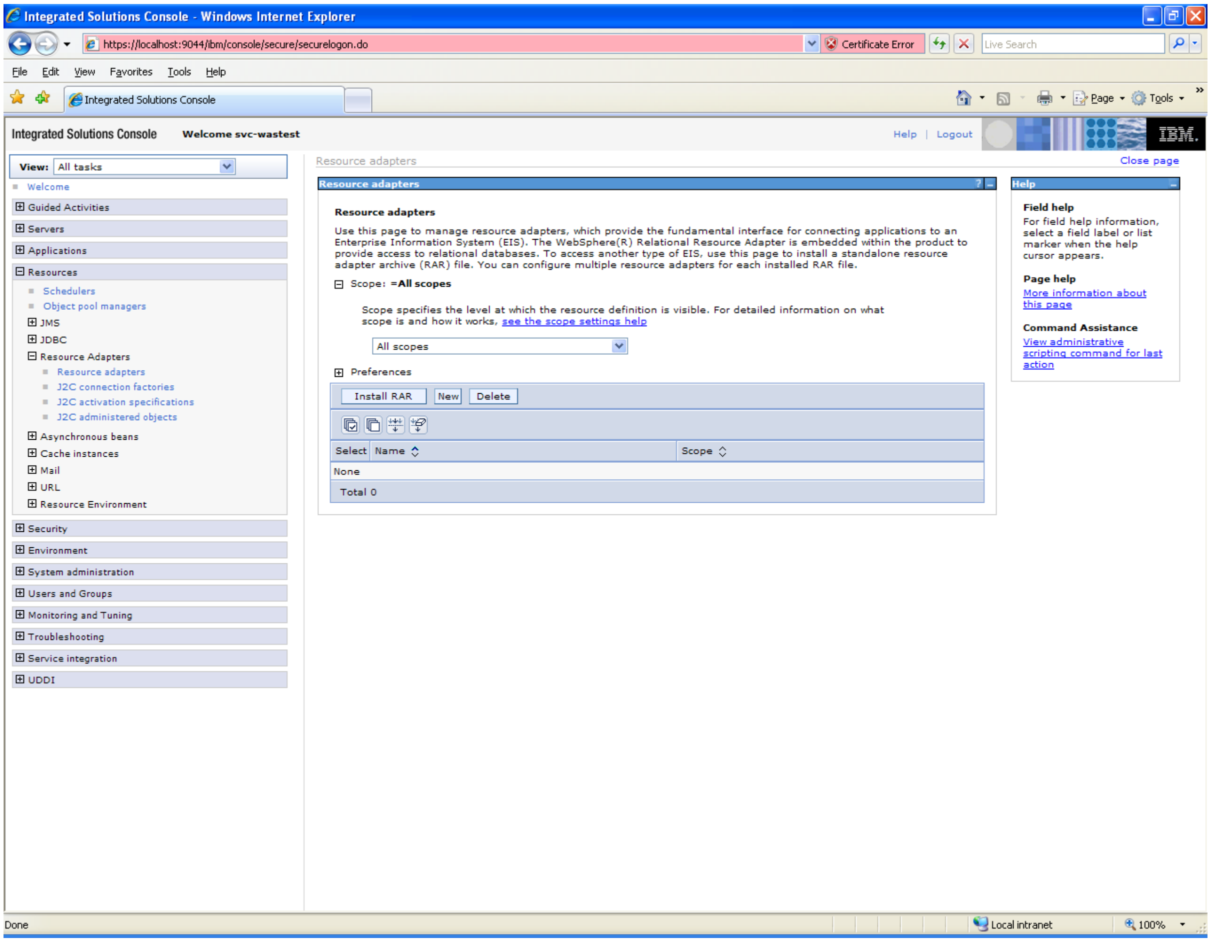
6 You have the option to add the certificate as a trusted certificate.

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** menu topic.

10 Select the **Resource adapters** link. The page below is displayed.



Resource adapters

Resource adapters

Use this page to manage resource adapters, which provide the fundamental interface for connecting applications to an Enterprise Information System (EIS). The WebSphere(R) Relational Resource Adapter is embedded within the product to provide access to relational databases. To access another type of EIS, use this page to install a standalone resource adapter archive (RAR) file. You can configure multiple resource adapters for each installed RAR file.

⊟ Scope: **=All scopes**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help

All scopes

⊞ Preferences

Install RAR | New | Delete

Select	Name	Scope
None		
Total 0		

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

Command Assistance

View administrative scripting command for last action

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 IBM i, go to /QIBM/Proddata/os400/security/eim, and select **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 **Global security**.

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 Leave the default value of BASIC_PASSWORD for the authentication **Preference** drop down.

11 Select **DefaultPrincipalMapping** 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 the value field, specify the EIM LDAP directory Server, for 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 important.

18 Click **OK**.

19 Select **Save**.

20 Select the **EimDomainName**.

21 Enter the EIM domain name in the value field, for 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 set up in EIM. This name is used to validate the user and to get the target user ID in the value field. For example: **MYCO.COM**.

26 Click **OK**.

27 Select **Save**.

28 Select the **KeyTimeoutSeconds**.

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

30 Click **OK**.

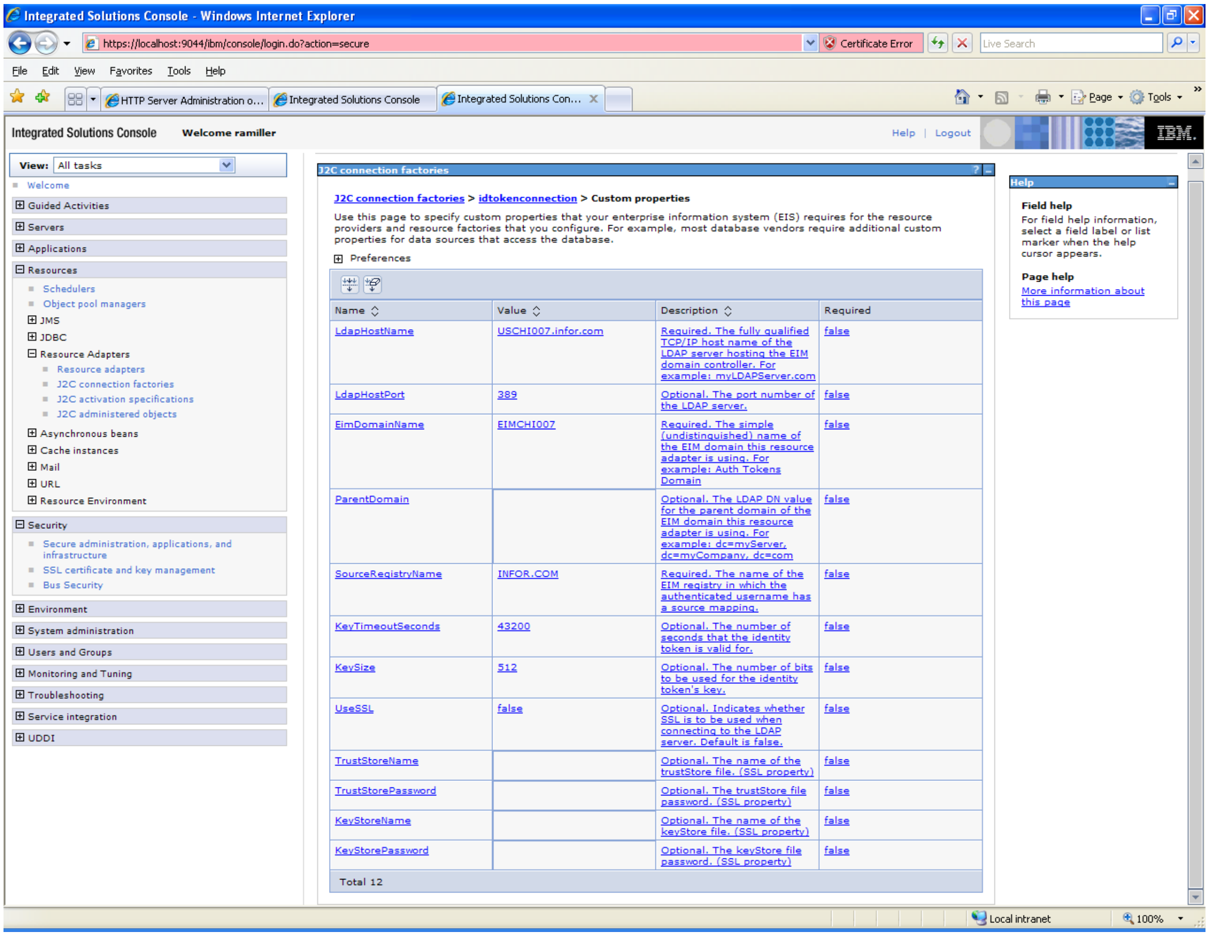
31 Select **Save**.

32 Select **UseSSL**.

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

34 Click **OK**.

35 Select **Save**.



J2C connection factories > idtokenconnection > Custom properties

Use this page to specify custom properties that your enterprise information system (EIS) requires for the resource providers and resource factories that you configure. For example, most database vendors require additional custom properties for data sources that access the database.

Name	Value	Description	Required
LdapHostName	USCHI007.infor.com	Required. The fully qualified TCP/IP host name of the LDAP server hosting the EIM domain controller. For example: myLDAPServer.com	false
LdapHostPort	389	Optional. The port number of the LDAP server.	false
EimDomainName	EIMCHI007	Required. The simple (undistinguished) name of the EIM domain this resource adapter is using. For example: Auth Tokens Domain	false
ParentDomain		Optional. The LDAP DN value for the parent domain of the EIM domain this resource adapter is using. For example: dc=myServer, dc=myCompany, dc=com	false
SourceRegistryName	INFOR.COM	Required. The name of the EIM registry in which the authenticated username has a source mapping.	false
KeyTimeoutSeconds	43200	Optional. The number of seconds that the identity token is valid for.	false
KeySize	512	Optional. The number of bits to be used for the identity token's key.	false
UseSSL	false	Optional. Indicates whether SSL is to be used when connecting to the LDAP server. Default is false.	false
TrustStoreName		Optional. The name of the trustStore file. (SSL property)	false
TrustStorePassword		Optional. The trustStore file password. (SSL property)	false
KeyStoreName		Optional. The name of the keyStore file. (SSL property)	false
KeyStorePassword		Optional. The keyStore file password. (SSL property)	false

Total 12

Figure 7: J2C connection factories

Installing jar files in the lib/ext folder of the server

To copy the required jar files from the IBM i to the Windows WAS server:

1. Go to the /QIBM/ProdData/OS400/security/eim folder on a mapped drive to the IBM 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 IBM i to the file system of the Windows WebSphere server.
4. Go to the /QIBM/ProdData/HTTP/Public/jt400/lib folder on a mapped drive to the IBM 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 IBM i to the file system of the Windows WebSphere server.

If using AES256, replacing the JCE jar files

To replace the JCE jar files:

1. Download the unrestricted JCE policy files from:

   http://www.ibm.com/developerworks/java/jdk/security/index.html

2. Unzip the downloaded file unrestricted.zip.
3. Place the unzipped jar files in *WEBSPHERE_INSTALLATION_DIRECTORY*/AppServer/java/jre/lib/security.

Installing the identity Token Ear file

To install the EAR file:

1. Expand the **Applications** topic.
2. Expand **Applications Types**.
3. Select **WebSphere enterprise applications**.
4. Click **Install**.
5. Select the browse button.
6. Using a mapped drive to the IBM i, go to /QIBM/Proddata/os400/security/eim, and select the testidentitytoken.ear.
7. Click **Open**.
8. Click **Next**.
9. Select **Detailed - Show all installation options and parameters**.
10. Click **Next**.
11. Click **Continue**.
12. Click **Next**.
13. Select the **TestIdentityTokenWeb** check box.
14. Select all clusters and servers.
15. Click **Apply**.
16. Click **Next**.
17. Click **Next**.
18. Click **Next**.
19. Click **Next**.
20. Click **Next**.

21 Click **Continue**.

22 Click **Next**.

23 Click **Next**.

24 Click **Next**.

25 Click **Next**.

26 Click **Next**.

27 Click **Finish**.

28 Select **Save**.

29 Expand the **Applications** topic.

30 Expand **Applications Types**.

31 Select **WebSphere enterprise applications**.

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

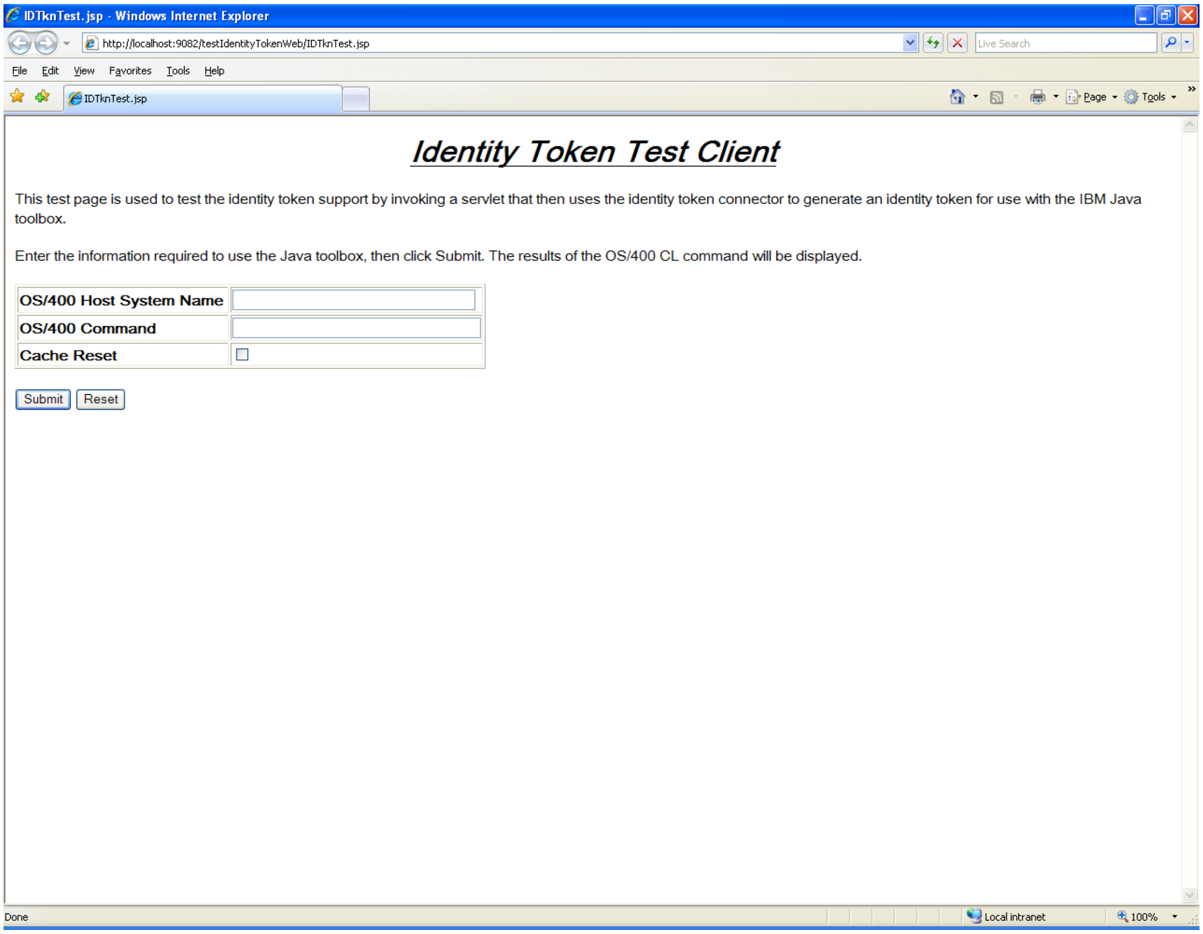
33 Click **Start**.

34 Open a browser.

35 Enter the following URL: “http://{host}:{port}/testIdentityTokenWeb/IDTknTest.jsp,” changing **host** and **port** to the appropriate values.

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

37 Enter a valid active directory user name and password that is a valid identity entry in EIM on the target IBM i. The Identity Token Test Client JSP page is displayed.



IDTknTest.jsp - Windows Internet Explorer
http://localhost:9082/testIdentityTokenWeb/IDTknTest.jsp
Live Search
File
Edit
View
Favorites
Tools
Help
IDTknTest.jsp
Page
Tools
Done
Local intranet
100%

Identity Token Test Client

This test page is used to test the identity token support by invoking a servlet that then uses the identity token connector to generate an identity token for use with the IBM Java toolbox.

Enter the information required to use the Java toolbox, then click Submit. The results of the OS/400 CL command will be displayed.

OS/400 Host System Name	
OS/400 Command	
Cache Reset	□

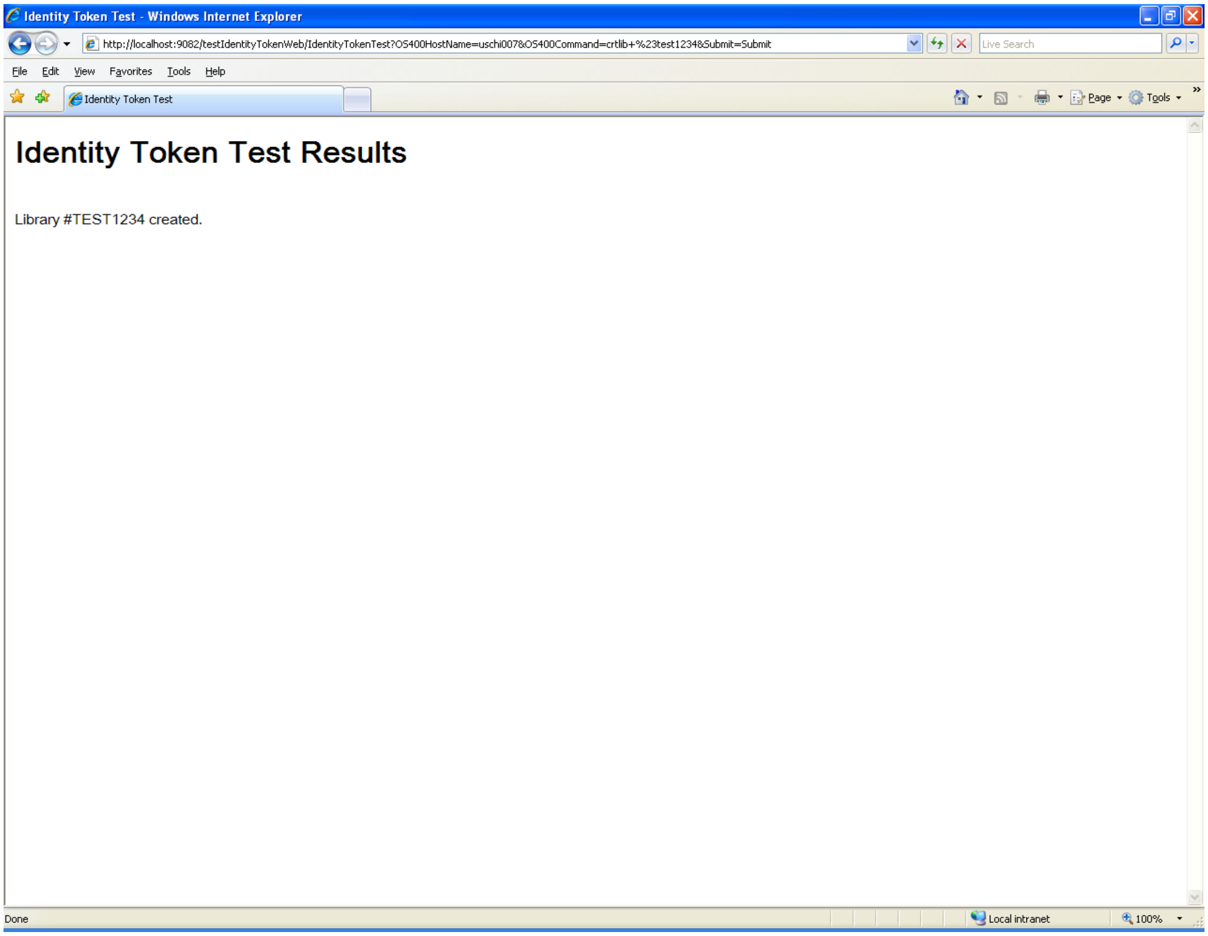
Submit Reset

Figure 8: Identity Token Test Client

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

39 Enter an OS/400 command, for example, **crtlib #TEST1234**.

40 Click **Submit**. If everything is set up correctly, the following page is displayed.


Identity Token Test - Windows Internet Explorer
Live Search
File Edit View Favorites Tools Help
Identity Token Test
Page Tools
Done
Local intranet
100%

http://localhost:9082/testIdentityTokenWeb/IdentityTokenTest?OS400HostName=uschi007&OS400Command=crtlib+%23test1234&Submit=Submit

Identity Token Test Results

Library #TEST1234 created.

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.

Creating 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 for the same IP address that is not an alias.

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 Step 1 in the *WebSphere with a Side of SPNEGO* white paper.

Step 2 - Assign the Service Principal 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 -out c:.keytab -MAPUSER svc-mstacywas@infor.com -PRINC
HTTP/mstacywas2.infor.com@INFOR.COM -PASS 4in4W@s -crypto AES256-SHA1 -ptype
KRB5_NT_PRINCIPAL
```

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 = AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96
default_tgs_enctypes = AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96
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. For example: c:\winnt\mywas.keytab
{key distribution center name}	Specify the domain 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”.

The following is an example of a filled out file where

```
[libdefaults]
    default_realm = MYCO.COM
    default_keytab_name = FILE:c:\winnt\mywas.keytab
    default_tkt_enctypes = AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96
    default_tgs_enctypes = AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96
```

```
     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 **Global Security.**
3. Expand the **Web and SIP 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 **Global Security.**
3. Expand the **Web and SIP security** node.
4. Select **Trust association**.

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

6 Click **OK**.

7 Select **Save**.

8 Expand the **Web and SIP security** node.

9 Select **Trust association**.

10 Select **Interceptors**.

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

12 Select the **Custom Properties**.

13 Under **Custom Properties**, 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 Expand the **security** menu node.

19 Select the **Global Security.**

20 Expand the **Web and SIP security** node.

21 Select **Trust association**.

22 Select **Interceptors**.

23 Click **New**.

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

25 In the **Value** field, specify the fully qualified virtual host name from the “Creating a virtual host name for WebSphere” section on page 27. Example: **mywas.myco.com**. This name is the virtual host name.

26 Click **OK**.

27 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 Expand **Server Types**.

3 Select **WebSphere application servers**.

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

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

6 Select **Process Definition**.

7 Select **Java Virtual Machine**.

8 Select **Custom Properties**.

9 Click **New**.

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

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

12 Click **OK**.

13 Select **Save**.

14 Click **New**.

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

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

17 Click **OK**.

18 Select **Save**.

19 Click **New**.

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

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

22 Click **OK**.

23 Select **Save**.

24 Click **New**.

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

26 In the **Value** field, 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**.

27 Click **OK**.

28 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 – Test the configuration

To test the configuration:

1 Open a browser.

2 Enter this URL:

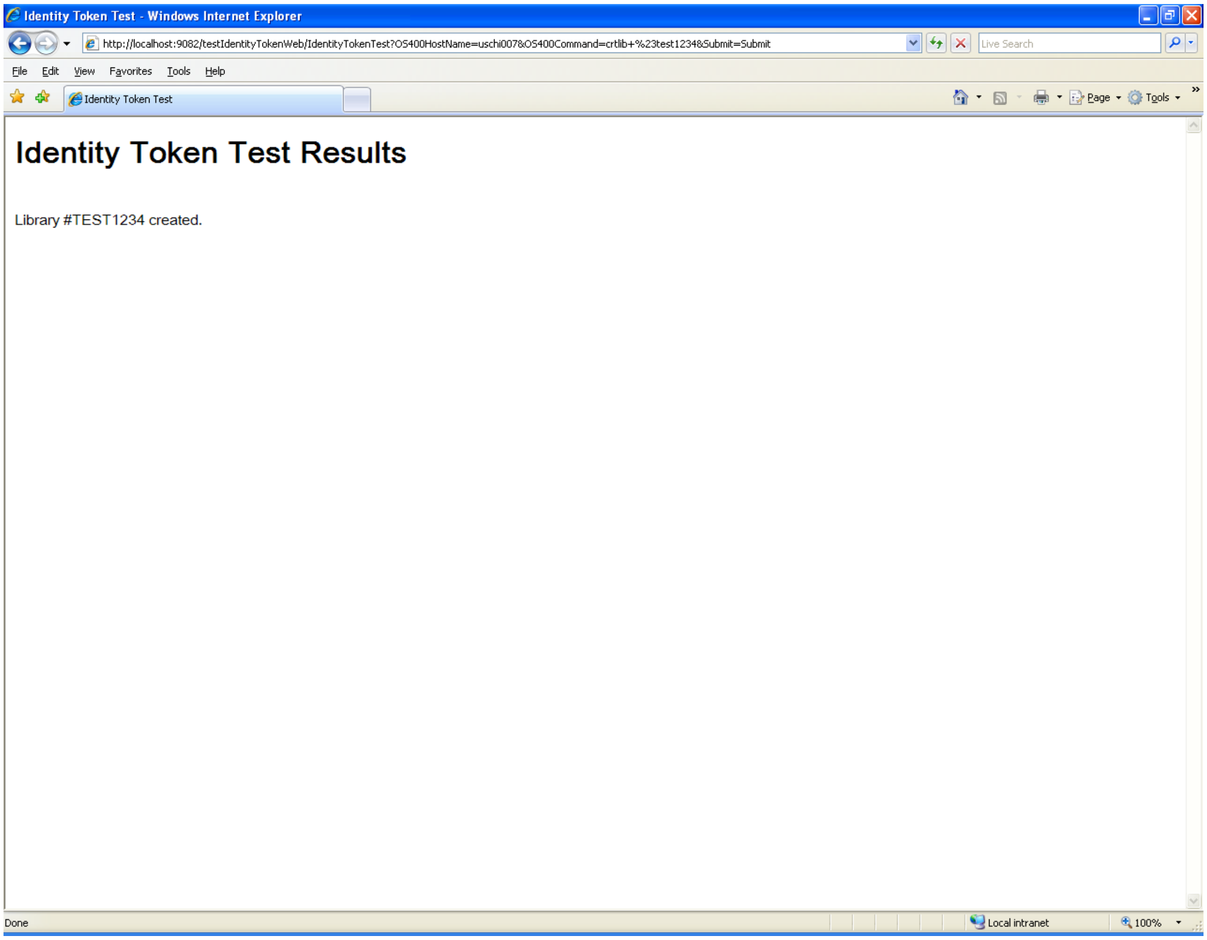
  http://{host}:{port}/testIdentityTokenWeb/IDTknTest.jsp, change the host and port to the appropriate values. Make certain that the host name is fully qualified with the default domain name and the host name defined in the “Creating a virtual host name for WebSphere” section on page 27.

  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 page is displayed.



http://localhost:9082/testIdentityTokenWeb/IdentityTokenTest?OS400HostName=uschi007&OS400Command=crtlib+%23test1234&Submit=Submit

Identity Token Test Results

Library #TEST1234 created.

Figure 10: Identity Token Test Results

Updating WebTop

Using Single Sign-on with IBM WebTop for IBM i requires an IWEBTOP.ear installation that supports Single Sign On.

To determine if the IWEBTOP.ear file supports Single Sign-on, do the following:

1 Open the WebSphere administrative console.

2 Expand **Applications**.

3 Expand **Application Types**.

4 Select **WebSphere enterprise applications**.

5 Select the IWEBTOP application by clicking the text **IWEBTOP**.

6 Under **References**, select **Resource references**. If you have a target resource reference eis/IdentityToken for the module IWEBTOP, then the IWEBTOP application supports Single Sign-on.

If your current IWEBTOP enterprise application EAR does not support Single Sign-on with IBM WebTop for IBM i, you must install a new IWEBTOP.ear file:

1 Un-install the existing IWEBTOP.ear file.

2 Install the new IWEBTOP.ear file from Infor following the standard WebTop installation instructions provided with the product.

Appendix - Blank SSO Configuration Checklist

Item	Value (example)
WebSphere Server name and port	
Windows domain user name for secure admin of WAS	
Windows domain user name password for secure admin of WAS	
Bind Distinguished Name for the admin user	
Windows Kerberos Authentication Server name (usually the Domain Controller)	
Windows Kerberos Authentication Server name port (usually the Domain Controller)	
Base Distinguished Name for the domain (from Microsoft Active Directory)	
EIM Admin User ID (created during EIM setup)	
EIM Admin User password (created during EIM setup)	
EIM LDAP Directory Server (created during EIM setup)	
EIM Domain Name (created during EIM setup)	
EIM Source User Registry Name (created during EIM setup)	
WAS system virtual name (new name in DNS for WAS system HTTP access). Do not create as an alias.	
Domain Service Principal User ID for WebSphere Application Server system (for authenticating users)	
Uppercase Kerberos realm (Note that this must be in upper case.)	
Keytab file location and name	
Key distribution center name	
Lower case domain name	