WebSphere Portal 8.5

SPNEGO Integration

****
***** **Table of Content** *****
****

****

1 Information

This document will help with the setup of WebSphere Portal 8.5 and SPNEGO.

Useful links:

- WebSphere Portal 8.5 Infocenter
  http://www-01.ibm.com/support/knowledgecenter/#!/SSHRKX_8.5.0/welcome/wp_welcome.html

- WebSphere Portal 8.5 Detailed System Requirements
  http://www-01.ibm.com/support/docview.wss?uid=swg27007791

- WebSphere Application Server 8.5.5 Infocenter
  http://www-01.ibm.com/support/knowledgecenter/?lang=en#!/SSAW57_8.5.5/as_ditamaps/was855_welcome_ndmp.html

- Installation Manager Documentation
  http://www-01.ibm.com/support/knowledgecenter/#!/SSDV2W_1.7.0/com.ibm.cic.agent.ui.doc/helpindex_imic.html

This document is not written or supported by IBM Support

Name	Date	Version	Description
Loc Dang	03/30/17	V1	WebSphere Portal 8.5 with SPNEGO

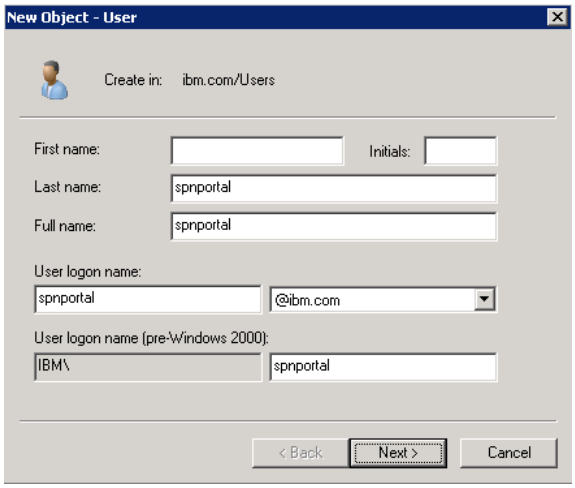
2 Prerequisites

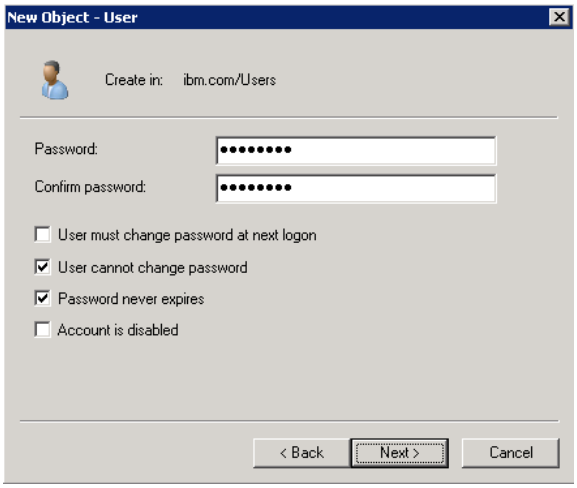
1. WebSphere Portal is installed and configured to Active Directory
2. If HTTP Server is used, install and configure the HTTP Server before starting the SPNEGO setup.
3. If a load balancer is used, configure the load balancer before starting the SPNEGO setup.

3 Active Directory

There can only be one spnego user per environment.

1. Login to the Active Directory file system





2. Create a user in Microsoft Active Directory that will be used for SPNEGO.

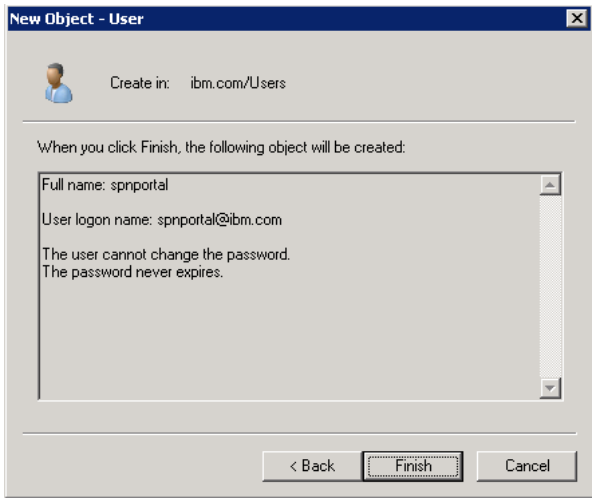
   Start > All Programs > Administrative Tools > Active Directory User and Computers

   SPNEGO_USER = _____

   Example:

```
spnportal
```

3. Click Next
4. Enter the password for the SPNEGO User
5. Uncheck “User must change password at next logon”
6. Check “User cannot change password”
7. Check “Password never expires”
8. Click Next



9. Click Finish
10. Open a console window

```
C:\Users\Administrator>setspn -A HTTP/wps85-64.ibm.com spnportal
Registering ServicePrincipalNames for CN=spnportal,CN=Users,DC=ibm,DC=com
        HTTP/wps85-64.ibm.com
Updated object
```

11. Run the following command to update the servicePrincipleName to the requesting hostname

```
setspn -A HTTP/<WPS_HOSTNAME> <SPNEGO_USER>
```

Example:

```
PORTAL          setspn -A HTTP/wps85-64.ibm.com spnportal
WEBSERVER       setspn -A HTTP/myweb.ibm.com spnportal
LOAD BALANCER   setspn -A HTTP/mylb.ibm.com spnportal
```

NOTE: Enter the hostname of the URL a user will use to navigate to the WebSphere Portal environment through a browser. It will be either the load balancer, Web Server or portal server. In the screenshot, the WebSphere Portal Server hostname will be used.

```
C:\Users\Administrator>ktpass -out c:/temp/spnportal.keytab -princ HTTP/wps85-64.ibm.com@ibm.com
-mapuser IBM\spnportal -mapOp set -pass passw0rd -ptype KRB5_NT_PRINCIPAL
Targeting domain controller: my2008ad.ibm.com
Using legacy password setting method
Successfully mapped HTTP/wps85-64.ibm.com to spnportal.
Key created.
Output keytab to c:/temp/spnportal.keytab:
Keytab version: 0x502
keysize 64 HTTP/wps85-64.ibm.com@ibm.com ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC)
keylength 16 (0xb9f917853e3dbf6e6831ecce60725930)
```

12. Run the following command to create the keytab file

```
ktpass -out <KEYTAB_FILE> -princ HTTP/<WPS_HOSTNAME>@<DNS> -mapuser
<DOMAIN>\<SPNEGO_USER> -mapOp set -pass XXXX -ptype KRB5_NT_PRINCIPAL
```

Example: WebSphere Portal

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/wps85-
64.ibm.com@IBM.COM -mapuser IBM\spnportal -mapOp set -pass passw0rd -
ptype KRB5_NT_PRINCIPAL
```

Example: WebServer

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/myweb.ibm.com@IBM.COM
-mapuser IBM\spnportal -mapOp set -pass passw0rd -ptype
KRB5_NT_PRINCIPAL
```

Example: Load Balancer

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/mylb.ibm.com@IBM.COM -
mapuser IBM\spnportal -mapOp set -pass passw0rd -ptype
KRB5_NT_PRINCIPAL
```

NOTE: Certain configuration may require **-crypto RC4-HMAC-NT**

Example: WebSphere Portal

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/wps85-
64.ibm.com@IBM.COM -mapuser IBM\spnportal -mapOp set -pass passw0rd -
ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Example: WebServer

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/myweb.ibm.com@IBM.COM
-mapuser IBM\spnportal -mapOp set -pass passw0rd -ptype
KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Example: Load Balancer

```
ktpass -out c:/temp/spnportal.keytab -princ HTTP/mylb.ibm.com@IBM.COM -
mapuser IBM\spnportal -mapOp set -pass passw0rd -ptype
KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

13. Copy the keytab file to the WebSphere Portal Server file system.

    Example:

```
spnportal.keytab
```

4 Deployment Manager and WebSphere Portal

1. Start the require java process

```
Cluster         Deployment Manager and Nodeagent
Standalone      WebSphere_Portal
```

2. Login to the Deployment Manager file system if a cluster or the WebSphere Portal Server if a standalone

3. Create a directory where the SPNEGO keytab and configuration file will be stored

```
WIN     E:\IBM\SPNEGO
UNIX    /opt/IBM/SPNEGO
```

4. Copy the keytab file to the newly create directory

```
WIN     E:\IBM\SPNEGO\spnportal.keytab
UNIX    /opt/IBM/SPNEGO/spnportal.keytab
```

5. Navigate to the bin directory of the Deployment Manager profile if a cluster. Navigate to the bin directory of the WebSphere Portal profile if a standalone.

   Example: Cluster

```
WIN   E:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin
UNIX  /opt/IBM/WebSphere/AppServer\profiles\Dmgr01/bin
```

   Example: Standalone

```
WIN   E:\IBM\WebSphere\wp_profile\bin
UNIX  /opt/IBM/WebSphere/wp_profile/bin
```

6. Run the following command to connect to wsadmin

```
wsadmin.(bat/sh) -lang jython -user <WASADMIN> -password <WASPWD>
```

   Example:

```
WIN     wsadmin.bat -lang jython -user wpadmin -password XXXX
UNIX    wsadmin.sh -lang jython -user wpadmin -password XXXX
```

7. Run the following command to create the SPNEGO configuration file

```
AdminTask.createKrbConfigFile('[-krbPath <SPNEGO_DIR>/<SPNEGO_CONF> -
realm <DNS> -kdcHost <AD_HOSTNAME> -dns <DNS_HOSTNAME> -keytabPath
<SPNEGO_DIR>/<SPNEGO_KEYTAB>]')
```

   Example: WINDOWS

```
AdminTask.createKrbConfigFile('[-krbPath E:\IBM\SPNEGO\spnportal.conf -
realm IBM.COM -kdcHost my2008ad.ibm.com -dns my2008ad.ibm.com -
keytabPath E:\IBM\SPNEGO\spnportal.keytab]')
```

   Example: UNIX

```
AdminTask.createKrbConfigFile('[-krbPath /opt/IBM/SPNEGO/spnportal.conf
-realm IBM.COM -kdcHost my2008ad.ibm.com -dns my2008ad.ibm.com -
keytabPath /opt/IBM/SPNEGO/spnportal.keytab]')
```

8. Verify the response

```
'<SPNEGO_CONF> has been created.'
```

Example:

```
WIN     'E:\\IBM\\SPNEGO\\spnportal.conf has been created.'
UNIX    '/opt/IBM/SPNEGO/spnportal.conf as been created.'
```

9. Copy the SPNEGO directory to all WebSphere Portal Server environment.
10. If the Portal Remote Server shares the same Deployment Manager then copy the SPNEGO directory to the Remote Search Server.

Example:

```
WIN     E:\IBM\SPNEGO
UNIX    /opt/IBM/SPNEGO
```

5 WebSphere Application Server Console

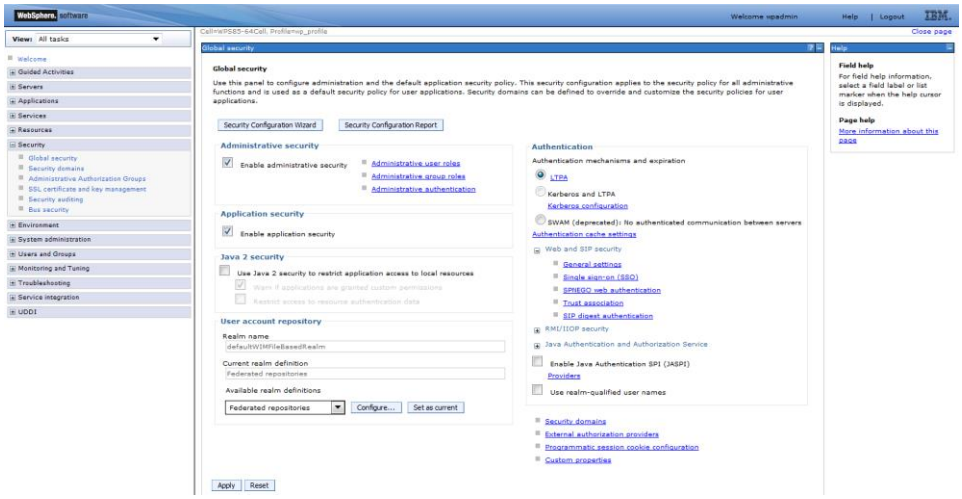
The screen shots are from a standalone environment but the instructure can be used for either a standalone or cluster environment.

1. Login to the WebSphere Application Server console

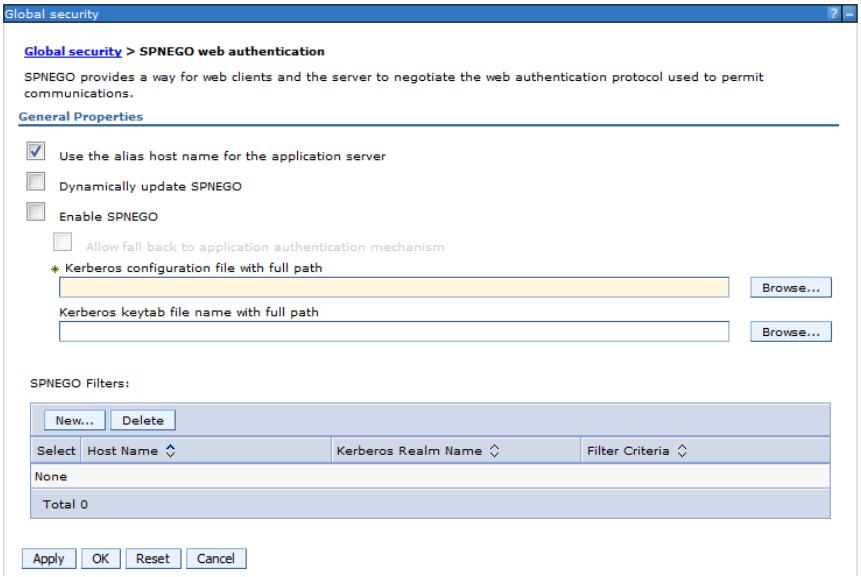
```
http://<HOSTNAME>:<PORT>/ibm/console
```

Example:

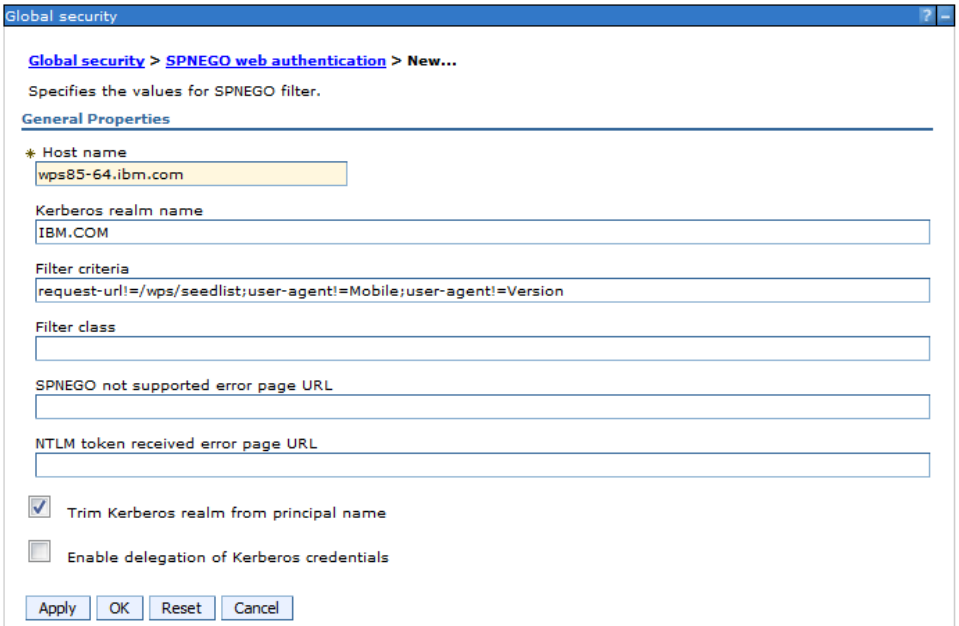
```
Standalone      https://wps85-64.ibm.com:10041/ibm/console
Cluster         https://mydmgr.ibm.com:9043/ibm/console
```



2. Navigate to Security > Global security
3. Under Authentication, expand Web and SIP security
4. Click on SPNEGO web authentication



5. Under SPNEGO Filters, click New…



6. In the **Host name** field, enter the hostname that will be configured with SPNEGO

   Example:

```
Portal          wps85-64.ibm.com
WebServer       myweb.ibm.com
Load Balancer   mylb.ibm.com
```

7. For Kerberos realm name, enter the domain

   Example: `IBM.COM`

8. For Filter criteria, enter the required filters. Leaving it blank will force all browsers and url with hostname to use SPNEGO

   Example of filters:

```
request-url!=/wps/seedlist;user-agent!=Mobile;user-agent!=Version
```

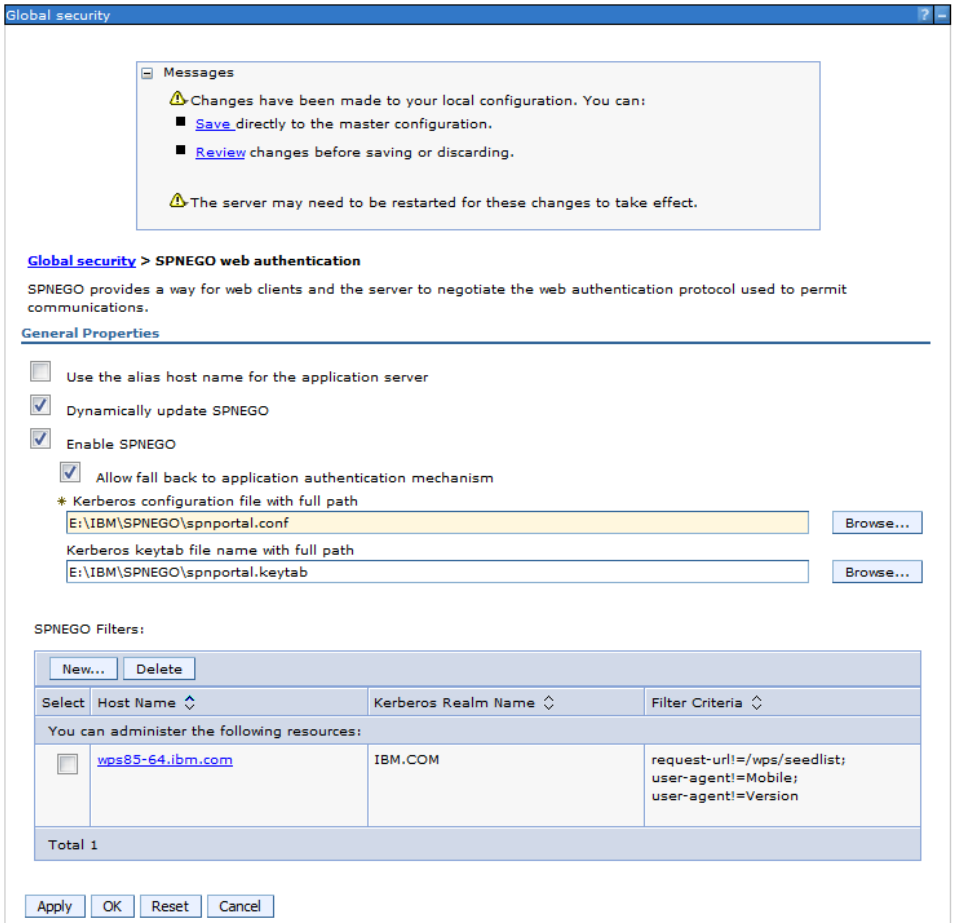
NOTE:

- When setting **request-url!=/wps/seedlist** the remote search URL configuration will not use SPNEGO
- When setting **user-agent!=Mobile** the mobile browsers will not use SPNEGO
- When setting **user-agent!=Version** the Safari browser will not use SPNEGO

9. Check **Trim Kerberos realm from principal**

10. If the user is set to use Kerberos credentials, then check **Enable delegation of Kerberos credentials**. In the screenshot, **Enable delegration of Kerberos credentials** was not checked

11. Click OK



12. Uncheck **Use the alias host name for the application server**
13. Optional : Check **Dynamic update SPNEGO**
14. Check **Enable SPNEGO**
15. Check **Allow fall back to application authentication mechanism**
16. For **Kerberos configuration file with full path**, click browse and browse to the SPNEGO configuration file

    Example:

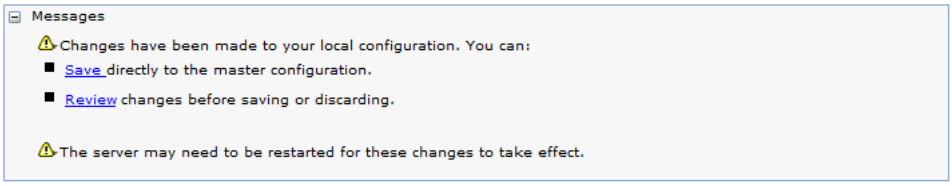
```
WIN     E:\IBM\SPNEGO\spnportal.conf
UNIX    /opt/IBM/SPNEGO/spnportal.conf
```

17. For **Kerberos keytab file name with full path**, click browse and browse to the SPNEGO keytab file

    Example:

```
WIN     E:\IBM\SPNEGO\spnportal.keytab
UNIX    /opt/IBM/SPNEGO/spnportal.keytab
```

18. Click OK

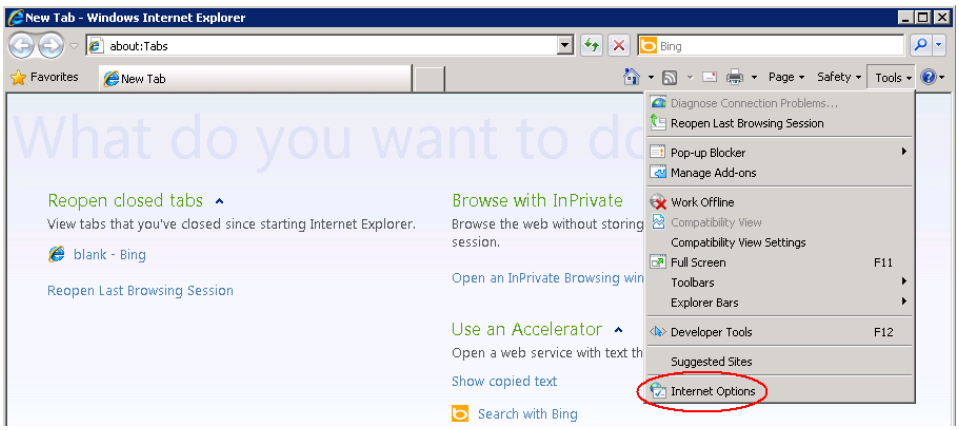


19. Click Save to save to the master configuration

20. Restart all java process

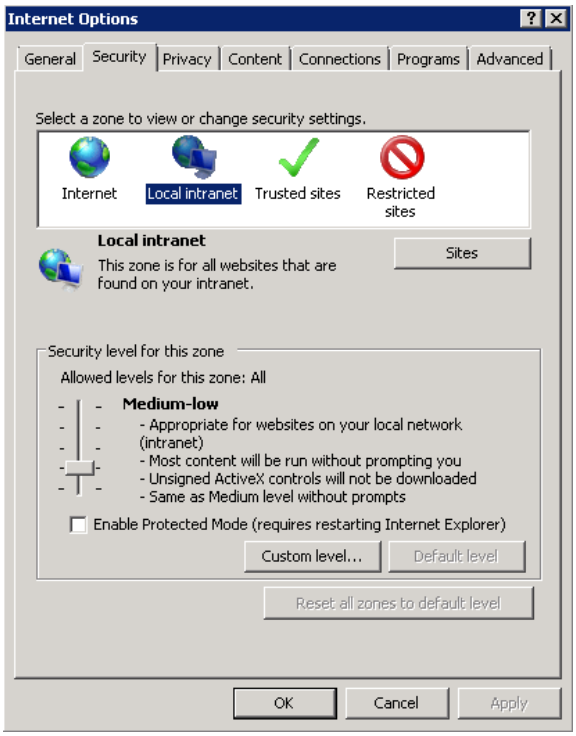
6 Browser

6.1 Microsoft Internet Explorer

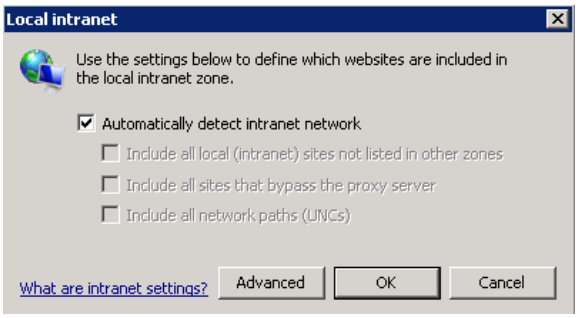


1. Open Microsoft Internet Explorer

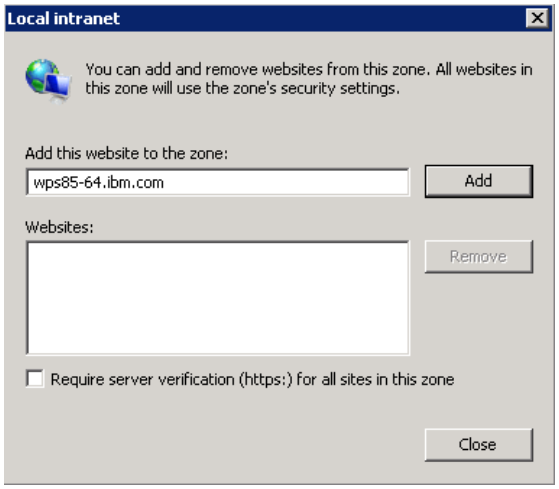
2. Click on Tools > Internet Options

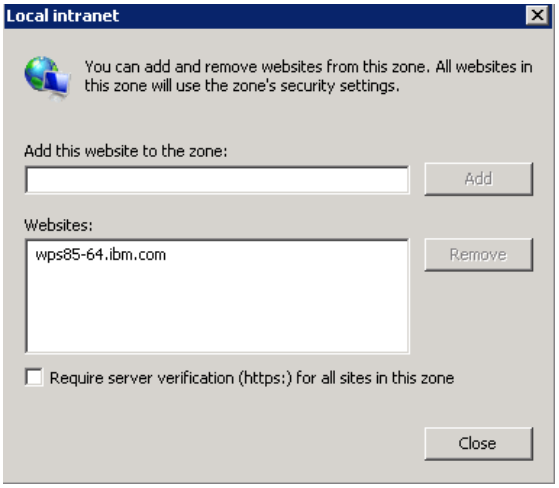


3. Click **Security** Tab
4. Click **Local intranet**
5. Click **Sites**



6. Click Advanced



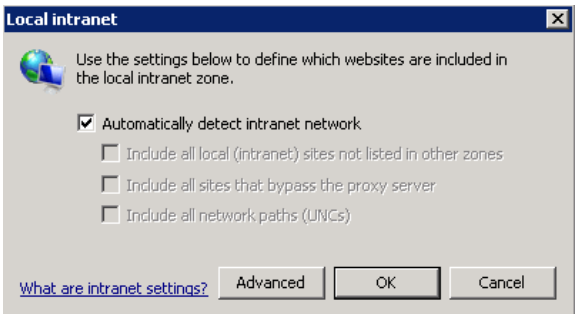


7. In the **Add this website to the zone** field, enter the hostname used by the client to reach the WebSphere Portal. This will either be the load balancer, webserver or portal server hostname.

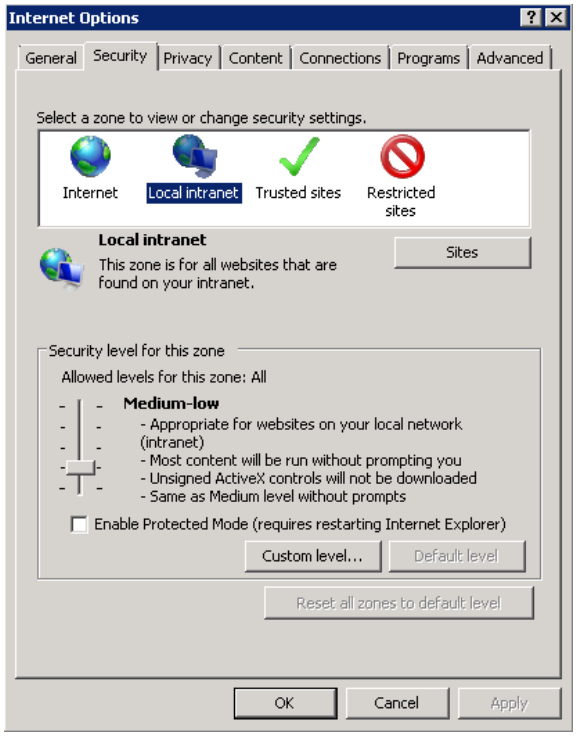
   HOSTNAME = _____

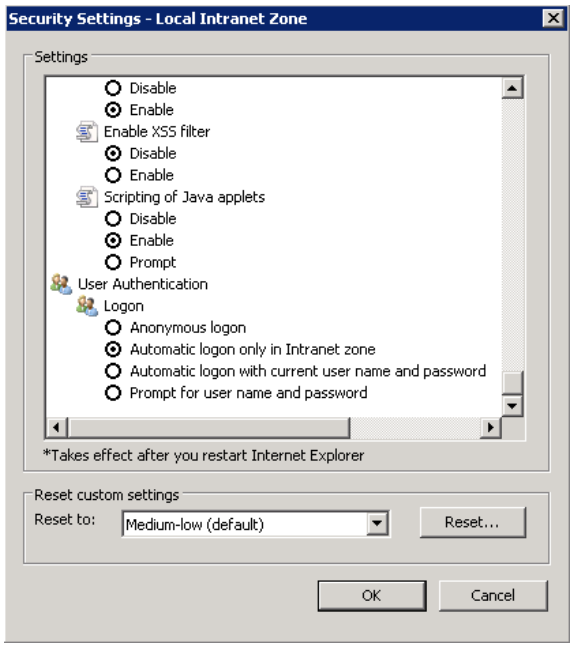
   Example: `wps85-64.ibm.com`

8. Click Add
9. Click Close

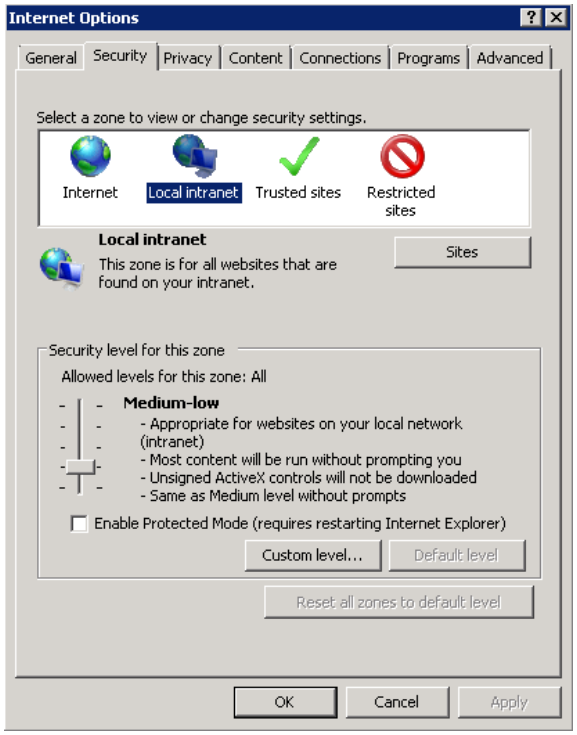


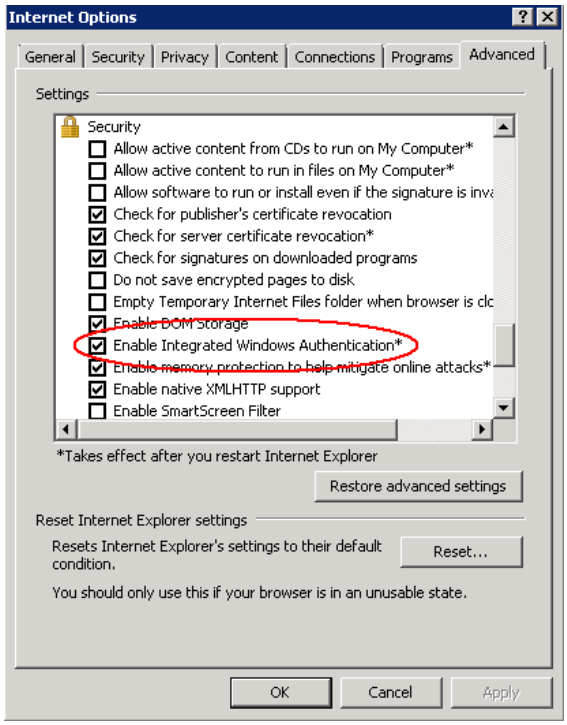
10. Click OK





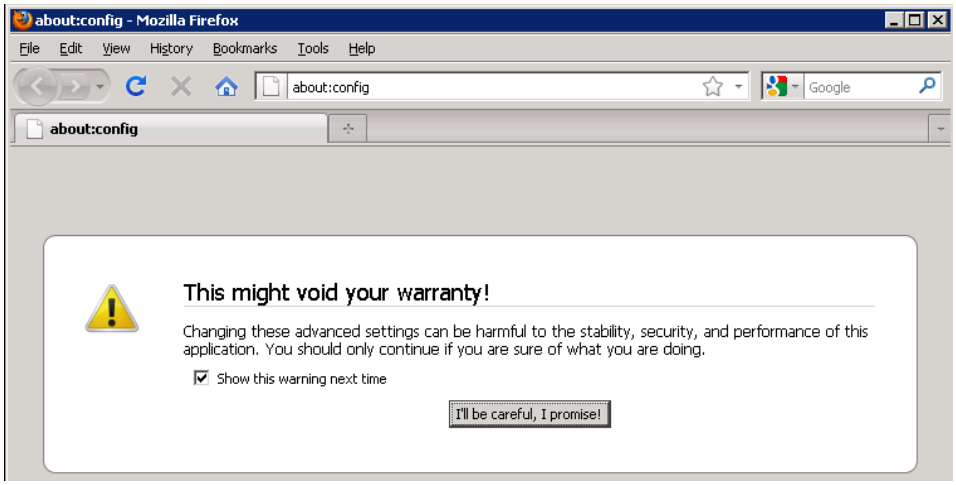
11. Click **Custom level…**
12. Under **Settings**, scroll to **User Authentication**
13. Verify/Select Automatic logon only in **Intranet zone**
14. Click OK



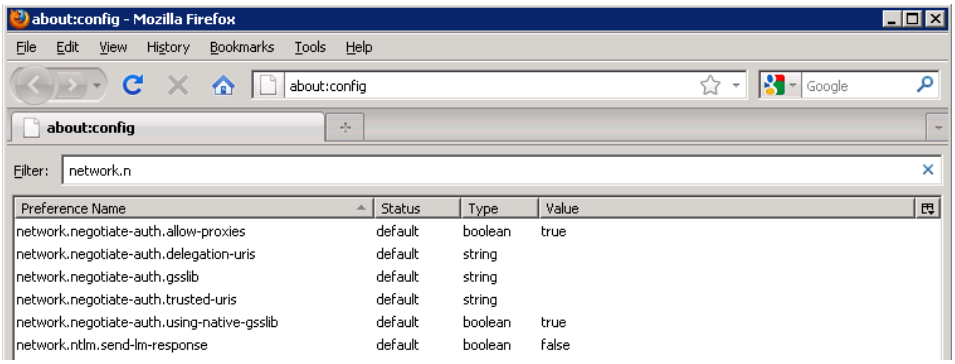


15. Click the **Advanced** tab
16. Scroll to Security
17. Verify/Check **Enable Integrated Windows Authentication***
18. Click **OK**

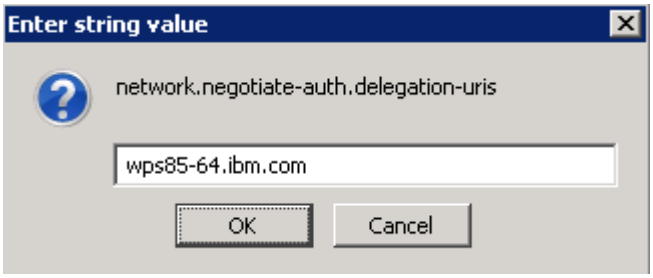
6.2 Firefox



1. Open Fiefox and set the URL to **about:config**
2. Click **I'll be careful, I promise!**



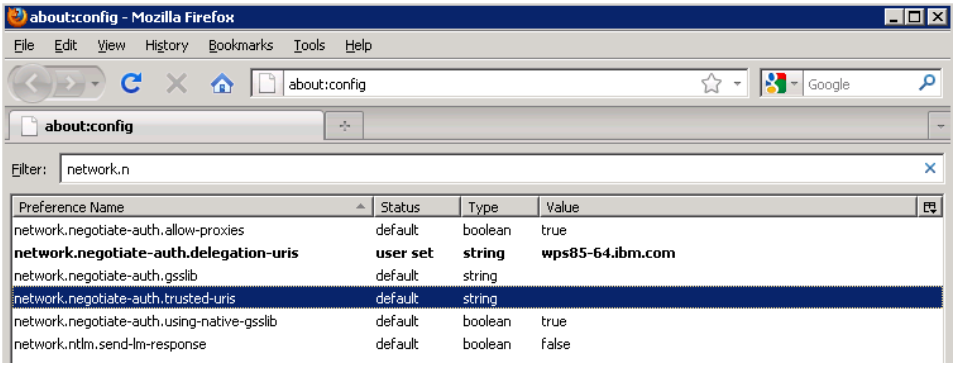
3. In the **Filter** field, enter "network.n"
4. Double click **network.negoticate-auth.delegation-uris**



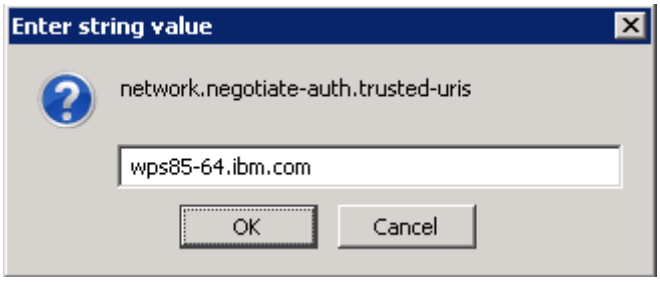
5. Enter the hostname used by the client to reach the WebSphere Portal. This will either be the load balancer, webserver or portal server hostname.

   Example: `wps85-64.ibm.com`

6. Click OK



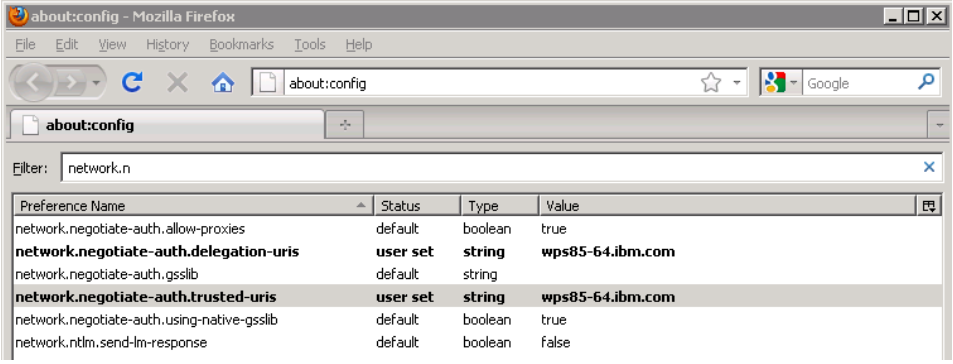
7. Double Click network.negotiate-auth.trusted-uris



8. Enter the hostname used by the client to reach the WebSphere Portal. This will either be the load balancer, webserver or portal server hostname.

   Example: `wps85-64.ibm.com`

9. Click OK



6.3 Google Chrome

Google Chrome uses Microsoft Internet Explorer settings. No other steps are required.