IBM Connections V4.5: How to configure SPNEGO

Visit <u>Enabling single sign-on for the Windows desktop</u> (also know as Enabling SPNEGO) in the information center to get more information about this topic.

Configure IBM® Connections to use SPNEGO for single sign-on (SSO). This configuration permits users to sign in to the Windows desktop and automatically authenticate with IBM Connections.

References

Configuring SPNEGO on WebSphere Application Server How to configure web browsers to support SPNEGO Creating a redirect page for users without SPNEGO support Filter criteria

Requirements

An administrator for IBM Connections that meets the following criteria:

- is from the configured LDAP used in Connections and is populated into the profiles databases (PROFILEDB).
- is configured as an Administrator of the Deployment Manager.

was used as the Connections administrator during the IBM Connections installation.

We refer to this user as: AdminFromLDAP.

Steps:

1. Mapping an Active Directory account to administrative roles. Change J2C authentication

Buses > <u>ConnectionsBus</u> > <u>Security for bus ConnectionsBus</u> > Users and groups in the bus connector role			
Users in the bus connector role are able to connect to the bus to perform messaging operations. Users can by specifically having that role, or because they are in a group with that role.			
Preferences			
New Delete			
Select	Name 🗘	Туре 🗘	
	AdminFromLDAP.	User	
Total 1			

_2. Creating a service principal name and keytab file

These steps were performed by the Active Directory Administrator who provided the following Keytab files for the IBM Connections Deployment Manager, Node1, and Node2.

__3. Merge all the keytab files to make the Deployment Manager aware of the SPNs for each node.

The following example demonstrates the procedure for merging keytab files.

a) Assuming that you have created the following keytab files:

http.keytab for the Deployment Manager krb5Node1.keytab for Node 1 krb5Node2.keytab for Node 2

b) Run the ktab command as follows:

mkdir /opt/keytab

- c) Copy the three keytab files into this directory: /opt/keytab
- d) Merge the three keytab files as follows:

cd /opt/IBM/WebSphere/AppServer/java/jre/bin [Note: use this version of ktab and NOT the http version]

./ktab -m /opt/keytab/krb5NodeA.keytab /opt/keytab/http.keytab ./ktab -m /opt/keytab/krb5NodeB.keytab /opt/keytab/http.keytab

e) Verify all three system are displayed in the keytab file correctly

cat http.keytab and you should see something like this result:

cat http.keytab	
SPNEGO.COMPANY.COM	go.company.com
BIGGOOGOCO ONA DEL SPNEGO.COMPANY.COM	TTP!dm&ihs.spnego.company.com
BIGGOGOGOCO GNA DE SPNEGO.COMPANY.COM	TTP!node1.spnego.company.com
33G00000C0 ONA bee SPNEGO.COMPANY.COM	TTP!node2.spnego.company.com

5. Create a Kerberos configuration file named krb5.conf

___a) Launch wsadmin and create the krb5.conf file as follows:

- i. cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin
- ii. ./wsadmin.sh -lang jacl -user AdminFromLDAP -password password

iii. At the prompt enter:

\$AdminTask createKrbConfigFile {-krbPath /opt/IBM/WebSphere/AppServer/java/jre/lib/security/krb5.conf
-realm SPNEGO.COMPANY.COM -kdcHost msad2008.spnego.company.com -dns spnego.company.com
-keytabPath /opt/keytab/http.keytab}

__b) Copy the **krb5.conf** file to the **/opt/keytab** folder, which should also have the merged keytab file (krb5.keytab)

____c) Verify the contents of the **krb5.conf**:

```
cat krb5.conf
 [libdefaults]
 default_realm = SPNEGO.COMPANY.COM
 default_keytab_name = FILE:/opt/keytab/http.keytab
 default_tkt_enctypes = rc4-hmac des-cbc-md5
 default_tgs_enctypes = rc4-hmac des-cbc-md5
 forwardable = true
 renewable = true
 noaddresses = true
 clockskew = 300
 [realms]
 SPNEGO.COMPANY.COM = {
 kdc = msad2008.spnego.company.com:88
 default_domain = spnego.company.com
 [domain_realm]
 .spnego.company.com = SPNEGO.COMPANY.COM
```

____d) Copy this folder and contents into the **same location** on the DM, Node1 & Node2 (ie **/opt/keytab** folder)

_6. Creating a redirect page for users without SPNEGO support

Use the example provided in the information center: Creating a redirect page for users without SPNEGO support

__7. Configuring SPNEGO on WebSphere Application Server

a. Log on to the WebSphere Application Server Integrated Solutions Console on the Deployment Manager and select Security -> Global Security.

b. In the Authentication area, click **Kerberos configuration** and then enter the following details .

- Kerberos service name HTTP
- Kerberos configuration file • Full path to your Kerberos configuration file
- Kerberos keytab file name • Full path to your keytab file
- Kerberos realm name .
- Name of your Kerberos realm
- Select Trim Kerberos realm from principal name if it is not already selected.
- Select Enable delegation of Kerberos credentials if it is not already selected. ٠

The settings should look like this:

lobal security	
<u>Global security</u> > Kerberos When configured, Kerberos will be the primary authentication mechanism. Configure EJB authentication to resources by acc on the applications details panel.	essing the resource references linl
Kerberos Authentication Mechanism	Related Configuration
+ Kerberos service name HTTP	SPNEGO Web authentication
* Kerberos configuration file with full path /opt/keytab/krb5.conf Browse	Federated user repositories
Verberos regre anno en ante en la participada de	CSIv2 inbound communications
SPNEGO.COMPANY.COM	CSIv2 outbound communications
🔽 Enable delegation of Kerberos credentials	
Apply OK Reset Cancel	г

____c. Select OK, then Save

d. Click Kerberos configuration and in the Related Configuration area, click SPNEGO Web authentication.

Note: SPNEGO Web authentication and Kerberos authentication use the same Kerberos client configuration and keytab files.

_e. Specify the values for SPNEGO filter.

In the SPNEGO Filters area select New and enter the following details:

Host name - enter the host name of the deployment manager

Kerberos realm name - enter your Kerberos realm name

Filter criteria - check the information center for any updates to the Filter criteria. In this example the following criteria was used:

request-url!=noSPNEGO;request-url!=/mobile;request-url!=/nav;request-url!=/bundles/js;request-url!=/static;request-url!=/activities/oauth;request-url!=/bundles/js;request-url!=/static; =/blogs/oauth;request-url!=/dogear/oauth;request-url!=/communities/calendar/oauth;request-url!=/communities/service/abover/calendar/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/communities/recomm/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/opensocial/oauth;request-url!=/connections/ope =/connections/opensocial/anonymous/rest;request-url!=/connections/opensocial/common;request-url!=/connections/opensocial/gadgets;request-url! =/connections/opensocial/ic;request-url!=/connections/opensocial/rpc;request-url!=/connections/opensocial/social;request-url!=/connections/opensocial/xrds;r

=/connections/resources/ic;request-url!=/files/oauth;request-url!=/forums/oauth;request-url!=/homepage/oauth;request-url!=/news/oauth;request-url! url!=/wikis/oauth;request-url!=/search/oauth;request-url!=/connections/core/oauth/;request-url!=/resources;request-url!=/oauth2/endpoint

Note: Ensure that you separate each filter with a semicolon (;). No other character is allowed as a separator.

Filter class - leave this field blank to allow the system to use the default filter class (com.ibm.ws.security.spnego.HTTPHeaderFilter).

SPNEGO not supported error page URL - enter the URL to the redirect page that you created. For example: http://webserver/NoSpnegoRedirect.html. - where webserver is the name of your IBM HTTP Server instance and NoSpnegoRedirect.html is the name of the redirect page.

NTLM token received error page URL - enter the URL to the redirect page that you created. For example: http://webserver/NoSpnegoRedirect.html.

Select Trim Kerberos realm from principal name. Select Enable delegation of Kerberos credentials.

Click **OK** and then click **Save**.

For example the setting should look like this:

lm&ihs.spnego.company.com		
rberos realm name		
SPNEGO.COMPANY.COM		
ter criteria		
quest-url!=noSPNEGO;request-url!=/mobi	le;request-url!=/nav;request-url!=/bundles/is;rec	quest-url!=/static
PNEGO not supported error page URL ttp://dm&ihs.spnego.company.com	:/NoSpnegoRedirect.html	
TLM token received error page URL	/NoSppegoRedirect.html	
Trim Kerberos realm from principal nam	ne	

_8. On the SPNEGO Web authentication page, complete the following steps:

- Select Dynamically update SPNEGO.
- Select Enable SPNEGO.
- Select Allow fall back to application authentication mechanism.
- Enter the path to the Kerberos configuration file in the Kerberos configuration file with full path field.
- Enter the path to the Kerberos keytab file in the Kerberos keytab file name with full path field.

1.11	provides a way for web clients and the s nications.	erver to negotiate the web authenticati	un protocol usea to pe	arrin C
neral	Properties			
	vnamically update SPNEGO			
₩ Fr	able SPNEGO			
	7	184 - 52 - 52		
I	Allow fall back to application authentication	ation mechanism		
* Kerberos configuration file with full path				During
//opt/keytab/krbb.cont				browse
Kerberos Keytab Tile name with tuli path			Browse	
1.00				
PNEG) Filters:			
Nev	Delete			
Select	Host Name 🗘	Kerberos Realm Name 🗘	Filter Criteria 🗘	Ĵ,
You	can administer the following resources:			
	dm&ihs.spnego.company.com	SPNEGO.COMPANY.COM	request-url!=noSPNEGO;request- url!=/mobile;request-url!=/nav; request-url!=/bundles /js;request-url!=/static	
Total	1			

____9. Specify the level of authentication that users must go through to access your IBM Connections deployment. In the following choices, you can force users to always authenticate or allow users to access Blogs, Bookmarks, Communities, Files, Profiles, and Wikis anonymously. These anonymous users must log in only if they try to access a private area. For more information about forcing authentication, see the Forcing users to log in before they can access an application topic.

The default is to **Allow anonymous access to IBM Connections** (also known as **Lazy SPNEGO**) and this is what is use in this example: See

Enterprise Applications

Enterprise Applications > <u>Activities</u> > Security role to user/group mapping

Security role to user/group mapping

Each role that is defined in the application or module must map to a user or group fro The accessIds are required only when using cross realm communication in a multi dom the accessId will be determined during the application start based on the user or group user and group information that is used for Java Platform, Enterprise Edition authorizat default authorization engine. The format for the accessIds is user:realm/uniqueUserII Entering wrong information in these fields will cause authorization to fail. AllAuthenticat that any valid user in the trusted realms be given the access. AllAuthenticated: This in current realm be given the access.

Map Users Map Groups Map Special Subjects 🔻			
Select	Role	Special subjects	
	person	All Authenticated in Application's Realm	
	everyone	Everyone	
	reader	Everyone	

___10. Disable TAI authentication:

Important: If you are configuring Tivoli® Access Manager with SPNEGO, or SiteMinder with SPNEGO. Those configurations require the default value of true for this parameter.

Select Security > Global Security > Custom properties > New and enter:

NAME: com.ibm.websphere.security.performTAIForUnprotectedURI			
Value: false			
	com.ibm.websphere.security.performTAIForUnprotectedURI	false	

11. Verify that LTPA is slected as the default Authentication mechanism

In **Global Security** under Authentication verify that "**LTPA**" is selected as the default for "**Authentication mechanisms and expiration**" If it is not, then select this option and save.



_12. Edit the following files:

a. files-config.xml set values to 'false'

```
<security reauthenticateAndSaveSupported="false">
<logout href="/files/ibm_security_logout" />
<inlineDownload enabled="false" />
</security>
```

b. LCC.xml (this should be already set:) - Verify customAuthenticator name="DefaultAuthenticator"

<customAuthenticator name="DefaultAuthenticator"/>

- _13. Stop and restart all servers:
- a) Do a Full Resynchronization of all Nodes.
- b) In System administration > Node agents do a Restart of all node agents
- c) On the Webserver do a Generate Plug-In and then Propagate Plug-In
- d) Stop and restart the webserver
- e) Stop all Connections' Clusters
- f) Stop and Restart the Deployment Manager
- g) Start all Connections' Clusters (this will take several minutes)

14. Configure a supported web browser to support SPNEGO

see How to configure web browsers to support

_

_15. Verify that Connections is configured for SPNEGO

Entering the following URL: https://dm&ihs.spnego.company.com/homepage in to your browser that has been configured for SPNEGO. The Connections' Home page should appear and you should be automatically logged in.