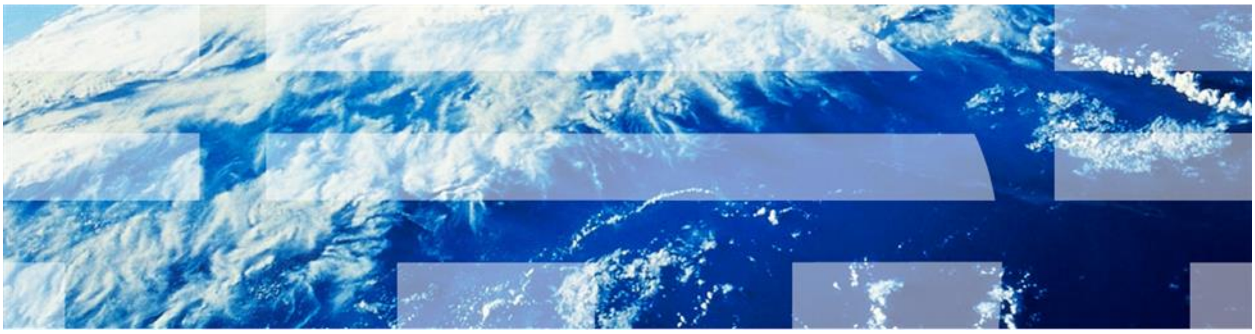
IBM Db2 Web Query for I Single Sign-on Using SPNEGO

Usage Instructions



Updated May 2, 2018

Overview

For IBM Db2 Web Query for i, this document describes the configuration necessary to enable single sign-on (SSO) using Simple and Protected GSS-API Negotiation Mechanism (SPNEGO). It assumes that you already have a Kerberos-based web serving environment configured for SSO and that you now want to additionally enable Web Query in that environment.

In this web serving environment, users log on to their Windows workstation using a domain account. The user is authenticated to the IBM i using their Windows domain credentials. The credentials are mapped to an IBM i user profile for use in authorizing the user to IBM i resources.

A Windows domain uses a Kerberos-based authentication method. SPNEGO enables web application servers and web browsers to automatically negotiate authentication using the Kerberos-based Windows credentials from the domain authentication instead of using HTTP authentication. With SPNEGO, SSO is extended to the Windows workstation log-on, and the user is not prompted to provide additional credentials.

For Web Query, SSO means that the login page is bypassed and users are taken directly to the portal when accessing the http://<system>:12331/webquery URL. The environment is “all or nothing”, meaning that when Web Query is enabled for SSO, all users and their workstations must be configured to the environment, as the traditional form-based sign on will no longer work.

1 Configuration Tasks

This document assumes that you already have a Kerberos-based web serving environment enabled for SSO. The following tasks should, therefore, already be completed:

For the Windows domain:
The domain should exist, user accounts should be created in the domain, and workstations should be added to the domain.

For the IBM i:
The network authentication service, time synchronization, Enterprise Identity Mapping (EIM), and service principals should be configured.

Note: Be sure that the HTTP service principal is created as a user account (*not* a computer account).

For each user:
An IBM i user profile should be created, a home directory for the profile should exist, the EIM identifier and associations should be created, and the user's web browsers should be enabled for SPNEGO.

If you need instructions for any of the initial setup tasks, refer to the "IBM i Access for Web WebSphere Application Server Single Sign-on Using SPNEGO" document at ftp://public.dhe.ibm.com/as400/products/clientaccess/web/files/v6r1/iWA_SPNEGO.pdf.

The additional tasks required to enable SSO specifically for Web Query are:

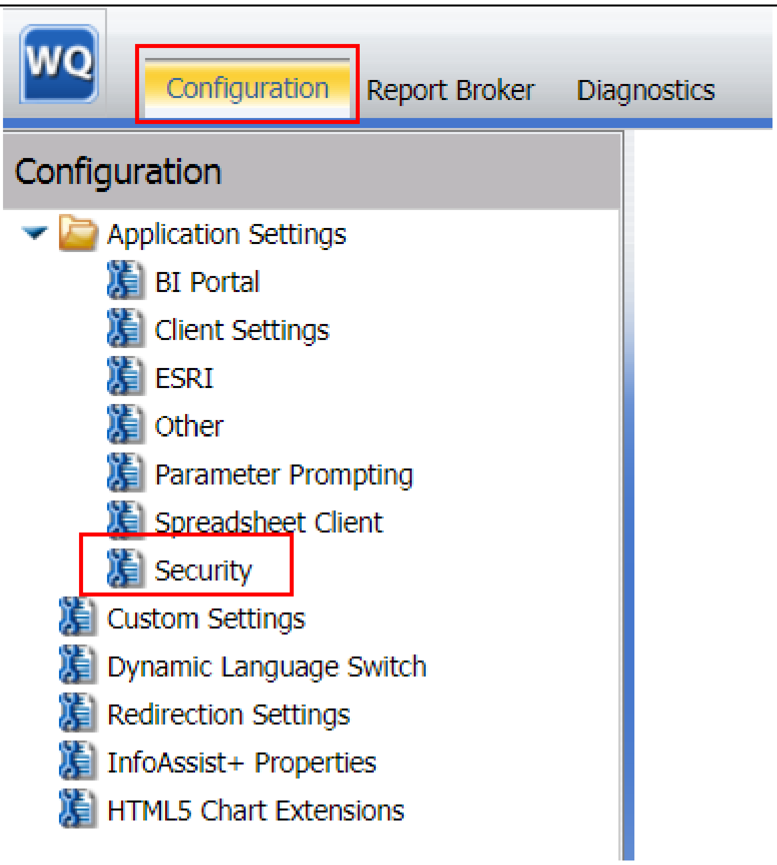
1. Set a redirection URL for sign outs.
2. Create an EIM identifier for QWQADMIN.
3. Create a JGSS configuration.
4. Enable SSO using SPNEGO.
5. Select the IWA option for Developer Workbench.

These tasks are described in detail in the following sections.

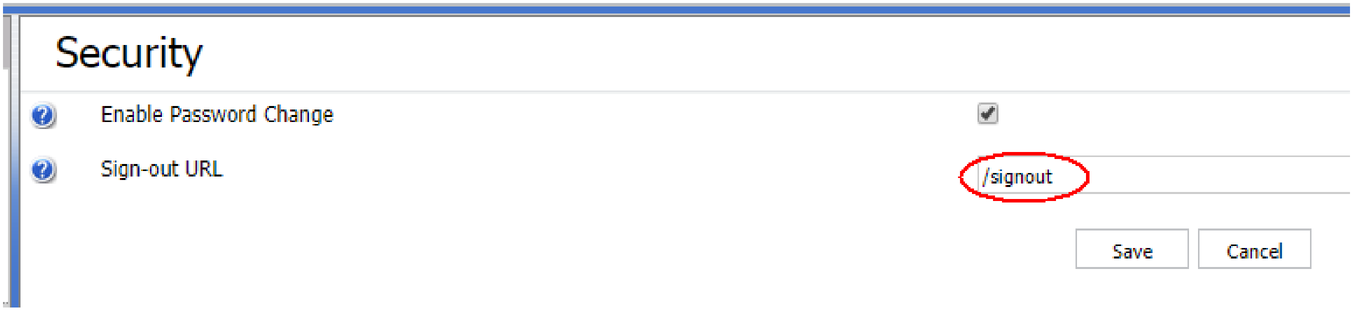
1.1 Setting a redirection URL for sign outs

Set a redirection URL for users in an SSO enabled environment who click Sign Out on the Web Query portal. Web Query must be active to perform these steps:

1. Sign into Web Query with the administrative profile, QWQADMIN.
2. Click Administration (top right), then Administration Console.
3. On the Web Query Administration Console, click the Configuration tab, expand Application Settings, then click Security.



4. Set the IBI_Signout_Redirect_URL parameter to `/signout`,and click Save.


Security

Enable Password Change ☑

Sign-out URL /signout

1.2 Creating Identifier Mapping for QWQADMIN

EIM on IBM i maps a Windows domain user to an IBM i user profile. It uses a Lightweight Directory Access Protocol (LDAP) server to store the identity mapping data.

EIM configuration requires LDAP administrator credentials. Contact the EIM domain administrator to request a new EIM identifier and add an association for the Web Query administrative profile, QWQADMIN. Detailed steps to create an EIM identifier can be found in section 4.3 in the "IBM i Access for Web WebSphere Application Server Single Sign-on Using SPNEGO" document.

1.3 Creating a JGSS Configuration

Java Generic Security Service (JGSS) is an implementation of the GSS-API framework that uses Kerberos as the underlying security system. Web Query use JGSS with SPNEGO to authenticate users using Kerberos credentials.

A JGSS configuration consists of a keytab file and a Kerberos configuration file. To create the JGSS configuration, do this:

1. Export keys for the HTTP service principal to a keytab file named `krb5.keytab`. Contact your Windows domain administrator to assist with this step because it must be performed on the Windows domain controller and must be performed with administrative privileges. The administrator will use the KTPASS command to export the keys. For an example command, refer to section 2.6 in the "IBM i Access for Web WebSphere Application Server Single Sign-on Using SPNEGO" document.

2. Use file mapping or FTP to copy the krb5.keytab file to the /qibm/userdata/qwebqry/extensions/kerberos directory in the IBM i integrated file system. (Note: if you use FTP, transfer the file in binary mode.)

3. Sign onto the i with QWQADMIN profile (or with a profile that has *ALLOBJ or *SECOFR authority).

4. Enter this CL command to change the owner of the keytab file to QWQADMIN:

```
CHGOWN
   OBJ('/qibm/userdata/qwebqry/extensions/kerberos/krb5.keytab')
   NEWOWN(QWQADMIN)
```

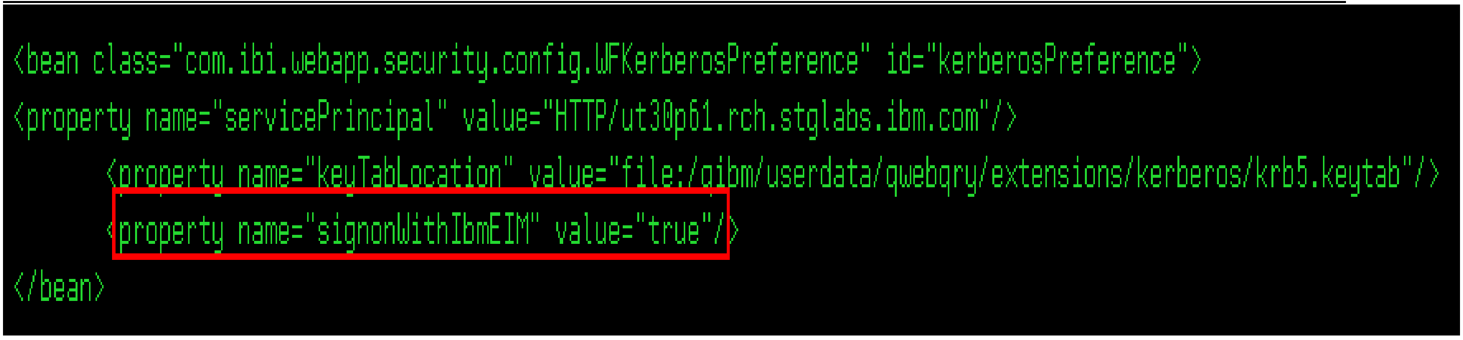
5. Enter this CL command to set *PUBLIC authority to *EXCLUDE:

```
CHGAUT
  OBJ('/qibm/userdata/qwebqry/extensions/kerberos/krb5.keytab')
  USER(*PUBLIC) DTAAUT(*EXCLUDE) OBJAUT(*NONE)
```

Note: Your administrator may point out to you that there is already a system-level.conf file in the /qibm/userdata/os400/NetworkAuthentication directory. Using the Web Query .conf file provides isolation from other SSO applications on the system, such as iNavigator and 5250. It ensures there are no conflicts between Web Query and other applications using SPNEGO and JGSS or with other i tasks using the network authentication service.

1.4 Enabling EIM and SSO

To enable identity mapping (EIM) for Web Query, use the WRKLNK command, option 2, to edit **/qibm/userdata/qwebqry/base80/config/securitysettings.xml**. Change the value of the property `signonWithIbmEIM` to `true`.



```
<bean class="com.ibi.webapp.security.config.WFKerberosPreference" id="kerberosPreference">
<property name="servicePrincipal" value="HTTP/ut30p61.rch.stglabs.ibm.com"/>
      <property name="keyTabLocation" value="file:/qibm/userdata/qwebqry/extensions/kerberos/krb5.keytab"/>
      <property name="signonWithIbmEIM" value="true"/>
</bean>
```

Lastly, to turn on SSO for Web Query, follow these steps:

1. Sign onto the i with QWQADMIN profile or with a profile that has *ALLOBJ or *SECOFR authority.

2. Enter the CFGWQSSO command, press F4, and enter these values:
    a. Specify *ENABLED in the STATUS parameter.
    b. Specify your HTTP service principal name in the HTTPSRVPRN parameter.
    c. Specify the name of your Windows domain in the WINDOM parameter.
    d. Specify the fully-qualified DNS name and port of your key distribution center (KDC) in the KDC parameter.
    e. Specify your domain name for your network in the DFTDOM parameter.
    f. Specify whether to enable EIM mapping.
    Note: It is highly recommended to use EIM for Web Query SSO. This ensures secure associations between Windows user IDs and IBM i user IDs.

    Example:

    ```
    CFGWQSSO
        STATUS(*ENABLED)
        TRACE(*OFF
        HTTPSRVPRN('HTTP/lp12ut21.rch.stglabs.ibm.com')
        WINDOM('VDSB.COM')
        KDC('smartbizmon.rch.stglabs.ibm.com:88')
        DFTDOM('.rch.stglabs.ibm.com')
        EIM(*YES)
        ENBMLTZON(*NO)
    ```

3. End Web Query and restart it using the WRKWEBQRY command.

1.5 Enabling multi-zone support

When SSO is enabled, the default behavior forces all users to use SSO when accessing Db2 Web Query. There may be an exception list that you would like to configure. That is, the ability to set up specific users (identified by their IP addresses) that do not want this mode of access: they may prefer to log into Db2 Web Query the traditional way (by accessing the BI Portal sign on screen and signing on manually).

You can enable this multiple zone support by taking the following steps:

1. Sign onto the i with QWQADMIN profile (or with a profile that has *ALLOBJ or *SECOFR authority).

2. Enter the CFGWQSSO command, press F4, and do the following:
    a. Specify *YES for the ENBMLTZON parameter
    b. Specify the list of exception IP addresses in the IPADR parameter.

The following example enables multiple zone support and allows the users of the four specified IP addresses to bypass SSO and log in manually:

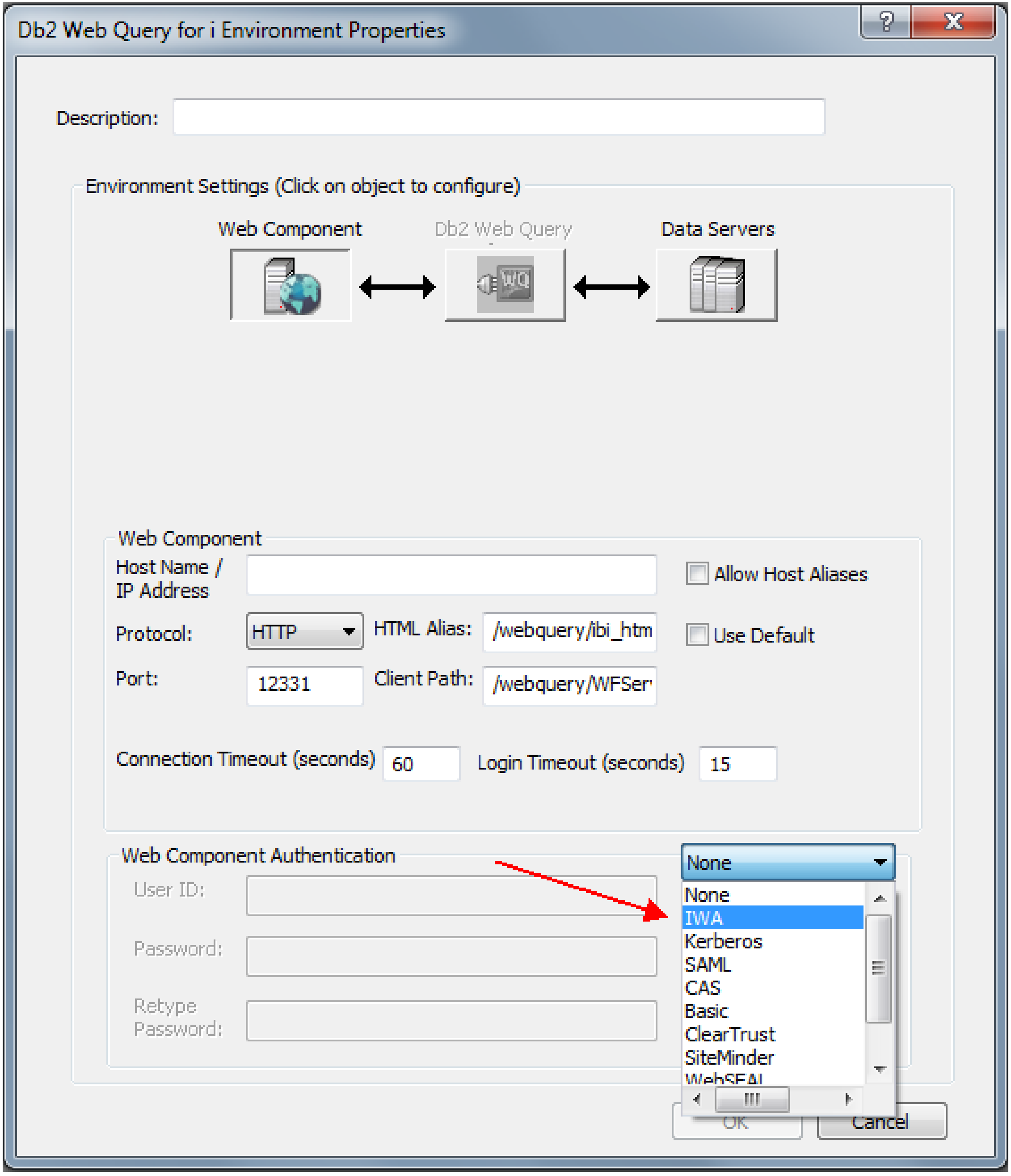
```
CFGWQSSO
      ENBMLTZON(*YES)
      IPADR('9.123.135.172' '127.0.0.1' '9.10.111.61' '9.123.135.142')
```

1.6 Select the IWA option for Developer Workbench

Licensed users of Web Query's Developer Workbench feature can optionally enable Integrated Windows Authentication (IWA) for one or more of their environments. When using IWA, they will not get prompted for a user name and password and instead, the Kerberos authentication will be used.

IWA is available in the Environment Properties dialog in Developer Workbench. In the

Web Component Authentication pull down, select IWA as shown below, and click OK.



Db2 Web Query for i Environment Properties

Description:

Environment Settings (Click on object to configure)

Web Component

Host Name / IP Address:

□ Allow Host Aliases

Protocol: HTTP

HTML Alias: /webquery/ibi_htm

□ Use Default

Port: 12331

Client Path: /webquery/WFSer

Connection Timeout (seconds) 60

Login Timeout (seconds) 15

Web Component Authentication: None

User ID:

Password:

Retype Password:

1.7 Disabling the SSO Environment

If you later want to disable the SSO environment for Web Query and go back to the traditional sign on, follow these steps:

1. Sign onto the i with QWQADMIN profile (or with a profile that has *ALLOBJ or *SECOFR authority).

2. Enter the CL Command:
   CFGWQSSO STATUS(*DISABLED)

3. Developer Workbench users should set the Web Component Authentication to ‘None’ in the Environment Properties dialog for each of their environments.

2 Appendix – Manual configuration steps

These steps are only provided in the event the CFGWQSSO command does not function properly.

2.1 Creating a JGSS Configuration

1. Edit the Kerberos configuration file on the i:
   a. Enter: edtf ‘/qibm/userdata/qwebqry/extensions/kerberos/krb5.conf’
   b. Replace `DEFAULT_REALM_VALUE` with the realm name of your Windows domain.
   c. Replace the `KDC_VALUE` with the fully-qualified DNS name and port of your key distribution center (KDC).
   d. Replace `DEFAULT_DOMAIN_VALUE` with your domain name for your network.
   e. Check with your Windows domain administrator to determine if other parameters are required for your network. For example, the admin_server is needed if the host where the Kerberos administration daemon is running is not the same as the master key distribution center (KDC).

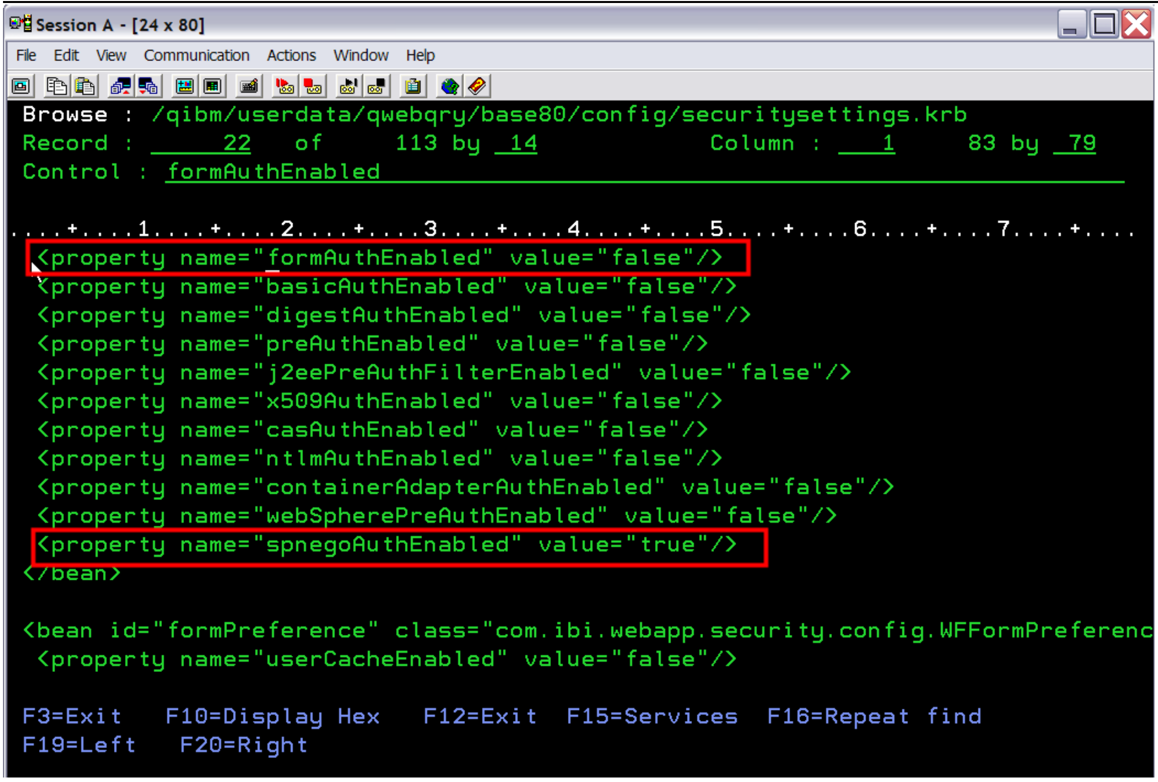
      Following is an example of an edited file with required parameter values for Web Query.

```
[libdefaults]
default_keytab_name =  /QIBM/UserData/qwebqry/extensions/kerberos/krb5.keytab
default_realm = VDSB.COM
kdc_use_tcp = 1
forwardable = true
renewable = true
noaddresses = true
clockskew = 300
[realms]
VDSB.COM = {
  kdc = smartbizmon.rch.stglabs.ibm.com:88
    }
[domain_realm]
  .rch.stglabs.ibm.com = VDSB.COM
[capaths]
```

2. Save the file.

2.2 Enabling SSO

1. Enter: wrklnk '/qibm/userdata/qwebqry/base80/config/securitysettings.xml'
2. Select option 2=Edit for the securitysettings.xml file.
3. Set the formAuthEnabled value to false and set the spnegoAuthEnabled value to true.



```
 Browse : /qibm/userdata/qwebqry/base80/config/securitysettings.krb
 Record :      22   of      113 by  14            Column :    1      83 by  79
 Control :  formAuthEnabled

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
  <property name="formAuthEnabled" value="false"/>
  <property name="basicAuthEnabled" value="false"/>
  <property name="digestAuthEnabled" value="false"/>
  <property name="preAuthEnabled" value="false"/>
  <property name="j2eePreAuthFilterEnabled" value="false"/>
  <property name="x509AuthEnabled" value="false"/>
  <property name="casAuthEnabled" value="false"/>
  <property name="ntlmAuthEnabled" value="false"/>
  <property name="containerAdapterAuthEnabled" value="false"/>
  <property name="webSpherePreAuthEnabled" value="false"/>
  <property name="spnegoAuthEnabled" value="true"/>
 </bean>

 <bean id="formPreference" class="com.ibi.webapp.security.config.WFFormPreferenc
  <property name="userCacheEnabled" value="false"/>

 F3=Exit   F10=Display Hex   F12=Exit  F15=Services  F16=Repeat find
 F19=Left   F20=Right
```

3. Search the file for *kerberosPreference*. Set the servicePrincipal value in the kerberosPreference bean to your HTTP service principal name. Following is an example for system LP61UT27 on domain rch.stglabs.ibm.com:

```
<bean id="kerberosPreference" class="com.ibi.webapp.security.config.WFKerberosPreference">
    <property name="servicePrincipal" value="HTTP/lp61ut27.rch.stglabs.ibm.com" />
    <property name="keyTabLocation" value="file:/qibm/userdata/qwebqry/extensions/kerberos/krb5.keytab"/>
    <property name="signonWithIbmEIM" value="true"/>
</bean>
```

4. Save the file.
5. Enter: wrklnk '/qibm/UserData/qwebqry/base80/client/wfc/etc/odin.cfg'
6. Select option 2=Edit.
7. Add the following 3 lines highlighted in bold red, and press F3 to save.

```
;Copyright 1996-2011 Information Builders, Inc. All rights
reserved


;TCP Client
NODE = EDASERVE
BEGIN
  PROTOCOL = TCP
  CLASS = CLIENT
  HOST=localhost
  PORT=12332
  SECURITY = TRUSTED
  TRUST_ID_SRC = IBIMR_user
  TRUST_GRPS_SRC = IBIMR_memberof
END
```

2.3 Disabling SSO

1. Enter: wrklnk '/qibm/userdata/qwebqry/base80/config/securitysettings.xml'. Use option 2=Edit to set the formAuthEnabled value to true and set the spnegoAuthEnabled value to false.

2. Enter: wrklnk '/qibm/UserData/qwebqry/base80/client/wfc/etc/odin.cfg'. Use option 2=Edit to remove these 3 lines:

```
 SECURITY = TRUSTED
TRUST_ID_SRC = IBIMR_user
TRUST_GRPS_SRC = IBIMR_memberof
```

[End of document]