IBM i Access for Web
WebSphere Application Server
Single Sign-on Using SPNEGO

Second Edition (February 2012)
This edition supplements the 6.1 and 7.1 IBM i Access for Web Information Center documentation.

1. Overview

Starting in V6.1, WebSphere Application Server enables use of a Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) to authenticate users using Windows domain credentials when accessing secured resources. This document describes the configuration necessary to enable single sign-on (SSO) to IBM i Access for Web in WebSphere Application Server using SPNEGO.

In this web serving environment, users log on to their Windows workstation using a domain account. They then use IBM i Access for Web to access IBM i resources. The user is authenticated to 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 Basic Authentication (in which the browser prompts for user credentials) or form-based authentication (in which a web page containing a form is used to prompt for user credentials). With SPNEGO, SSO is extended to the Windows workstation log-on, and the user is not prompted to provide additional credentials.

1.1 Supported Kerberos Encryption Types

Until recently, IBM i has supported only DES encryption types for Kerberos. The following PTFs add support for RC4 and AES encryption types.

5.4 (5722SS1)	SI43920, SI43034, SI44052
6.1 (5761SS1)	SI43919, SI42957, SI44058
7.1 (5770SS1)	SI43918, SI42919, SI44060

Table 1: PTF information for additional Kerberos encryption types

After applying the PTFs, follow the instructions in the cover letters to enable support for RC4 and AES encryption types.

1.2 Configuration Tasks

Configuring this Web serving environment consists of the following tasks:

2. Configure IBM i
   - 2.1. Configure Network Authentication Service
   - 2.2. Configure Time Synchronization
   - 2.3. Configure Enterprise Identity Mapping
   - 2.4. Create krbsvr400 Service Principal
   - 2.5. Create HTTP Service Principal
   - 2.6. Create JGSS Configuration

3. Configure WebSphere Application Server
   - 3.1. Create Profile
   - 3.2. Secure Profile Using Microsoft Active Directory
   - 3.3. Configure Single Sign-on
   - 3.4. Configure SPNEGO
   - 3.5. Configure IBM i Access for Web

4. Configure User Access
   - 4.1. Create IBM i User Profile
   - 4.2. Create Home Directory for IBM i User Profile
   - 4.3. Create EIM Identifier and Associations
   - 4.4. Configure Web Browser
   - 4.5. Access IBM i Access for Web

These tasks assume the Windows domain already exists, user accounts have already been created in the domain, and workstations have already been added to the domain.

If you are already using IBM i Access for Windows with integrated Windows domain login for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), many of these tasks have already been completed.

1.3 Example Environment

This document uses these tasks to configure an example environment using the following information.

IBM i system	LP11UT11.RCHLAND.IBM.COM
Windows domain	DEPT144.RCHLAND.IBM.COM
Windows domain controller	eap2003.rchand.ibm.com
LDAP server	X1519P4.RCHLAND.IBM.COM

Table 2: Information about example environment used in configuration tasks

Values based on this example environment will be used in the steps for each task.

2. Configure IBM i

Each IBM i system that will have a SPNEGO-enabled WebSphere Application Server profile must be configured for Kerberos. This involves configuring the network authentication service, synchronizing the system time to match the Windows domain controller, adding the system to the Enterprise Identity Mapping (EIM) domain, creating the "krbsvr400" and "HTTP" service principals in the Windows domain, and creating the JGSS configuration.

These tasks assume the Windows domain already exists.

2.1 Configure Network Authentication Service

The following information describes how to configure network authentication service on IBM i using a Windows domain controller as a Key Distribution Center (KDC). Network authentication service allows IBM i to use Kerberos credentials from a Windows domain for authentication. Use the network authentication service wizard to perform the configuration.

If you are already using IBM i Access for Windows with integrated Windows domain logon for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), this task has already been completed.

IBM i system	LP11UT11.RCHLAND.IBM.COM
Realm name (Windows domain)	DEPT144.RCHLAND.IBM.COM
KDC name (Windows domain controller)	eap2003.rchand.ibm.com
KDC port	88
Service principal password	kerberos

Table 3: Sample values from example environment used in network authentication service configuration task

Configuring the network authentication service consists of the following steps:

1. Use *System i Navigator* to access IBM i system settings
2. Add the IBM i system to the list of connections if necessary (for example, add `LP11UT11.RCHLAND.IBM.COM` to *My Connections* if it is not already listed)
3. Select the IBM i system in the list of connections (for example, select `LP11UT11.RCHLAND.IBM.COM`)
4. Sign on using a user profile with *ALLOBJ special authority
5. Expand the IBM i system in the list of connections
6. Select **Security** > **Network Authentication Service**
7. Select **Configure Network Authentication Service** in the *Security tasks* window to start the network authentication service configuration wizard

8. Select **Next** on the *Welcome* page
9. Configure the realm information on the *Specify Realm Information* page
    a. Specify the realm name in the **Default realm** field (for example, specify `DEPT144.RCHLAND.IBM.COM`)
    b. Select the **Microsoft Active Directory is used for kerberos authentication** option if it is not already selected
    c. Select **Next**
10. Configure the KDC information on the *Specify KDC Information* page
    a. Specify the KDC name in the **KDC** field (for example, specify `eap2003.rchland.ibm.com`)
    b. Specify the KDC port in the **Port** field (for example, specify `88`)
    c. Select **Next**
11. Select the **No** option on the *Specify Password Server Information* page; select **Next**
12. Configure the keytab entries on the *Select Keytab Entries* page
    a. Select the **i5/OS Kerberos Authentication** option (this creates a keytab entry for the **krbsvr400** service principal)
    b. Clear all other options
    c. Select **Next**
13. Configure the password for the krbsvr400 service principal on the *Create i5/OS Keytab Entry* page
    a. Specify the service principal password in the **Password** and **Confirm password** fields (for example, specify `kerberos` in both fields)
    b. Select **Next**
14. Select the **No** option on the *Create Batch File* page; select **Next**
15. Review the information on the *Summary* page; select **Finish** to complete the wizard

2.2 Configure Time Synchronization

The following information describes how to configure the Simple Network Time Protocol (SNTP) client service to synchronize IBM i system time with a time server. Kerberos requires that time on a system be within a specified interval of the time on the KDC. This time interval is called clock skew. The default clock skew is five minutes (300 seconds). If time on a system is not within the clock skew, Kerberos operations fail. Configuring the IBM i system to synchronize time with the KDC (or with the time server used by the KDC) will keep the IBM i system time the same as the KDC and prevent Kerberos failures due to clock skew. Use the Simple Network Time Protocol (SNTP) client service to synchronize IBM i system time with the KDC.

This task assumes that your system has a correct date, time, and time zone configured. The SNTP client service will only adjust the time if it is within two hours (120 minutes) of the time on the time server. The IBM i system date, time, and time zone can be verified (and changed) in *System i Navigator* by expanding your system in the list of connections,

selecting **Configuration and Service** > **Time Management**, and selecting **View date and time system values** in the *Time Management tasks* window.

If you are already using IBM i Access for Windows with integrated Windows domain login for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), this task has already been completed.

Time server (KDC name) (Windows domain controller)	eap2003.rchland.ibm.com
Poll interval	60 minutes
Minimum adjustment	20 milliseconds
Maximum adjustment	120 minutes
Adjustment threshold	180 seconds

Table 4: Sample values from example environment used in time synchronization configuration task

Configuring the SNTP client service consists of the following steps:

1. Use *System i Navigator* to access IBM i system settings
2. Add the IBM i system to the list of connections if necessary (for example, add `LP11UT11.RCHLAND.IBM.COM` to *My Connections* if it is not already listed)
3. Select the IBM i system in the list of connections
4. Sign on using a user profile with *ALLOBJ special authority
5. Expand the IBM i system in the list of connections
6. Select **Network** > **Servers** > **TCP/IP**
7. Select **SNTP** in the list of TCP/IP servers
8. Select **Properties** from the *File* menu
9. Select the **General** tab
    a. Select the **Client** option
    b. Clear the **Server** option
10. Select the **Client** tab
    a. Select the **Add** button for the **Time servers** field
        i. Specify the KDC name in the input field (for example, specify `eap2003.rchland.ibm.com`)
        ii. Select **OK**
    b. Specify a value in the **Poll interval** field (for example, specify `60`)
    c. Specify a value in the **Minimum adjustment** field (for example, specify `20`)

d. Specify a value in the **Maximum adjustment** field (for example, specify `120`)

e. Specify a value in the **Adjustment threshold** field (for example, specify `180`)

f. Select the **Only when adjusting the system clock** option under *Activity logging*

11. Select the **Server** tab
    a. Select the **None** option under *Server activity logging*
    b. Clear the **Server must be synchronized before valid time is served** option
12. Select **OK**
13. Expand the IBM i system in the list of connections
14. Select **Network** > **Servers** > **TCP/IP**
15. Select **SNTP** in the list of TCP/IP servers
16. Select **Start** > **Client** from the *File* menu to start the SNTP client service.

2.3 Configure Enterprise Identity Mapping

The following information describes how to configure Enterprise Identity Mapping on IBM i. EIM uses a Lightweight Directory Access Protocol (LDAP) server to store identity mapping data. The LDAP server is the EIM domain controller. The identity mapping data is the EIM domain. EIM configuration requires LDAP administrator credentials to create the EIM domain. Use the Enterprise Identity Mapping (EIM) wizard to perform the configuration.

This task assumes your system is joining an EIM domain which already exists and the EIM domain controller uses a distinguished name and password for authentication. For information on creating an EIM domain or using other authentication types, refer to the Enterprise Identity Mapping topic in the IBM i Information Center (http://www.ibm.com/systems/i/infocenter).

If you are already using IBM i Access for Windows with integrated Windows domain login for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), this task has already been completed.

EIM domain controller (LDAP server)	X1519P4.RCHLAND.IBM.COM
EIM domain controller port	389
LDAP administrator distinguished name	cn=administrator
LDAP administrator password	secret
EIM domain	EimDomain
IBM i system	LP11UT11.RCHLAND.IBM.COM
Realm name (Windows domain)	DEPT144.RCHLAND.IBM.COM

Table 5: Sample values from example environment used in EIM configuration task

Configuring EIM consists of the following steps:

1. Use *System i Navigator* to access IBM i system settings
2. Add the IBM i system to the list of connections if necessary (for example, add `LP11UT11.RCHLAND.IBM.COM` to *My Connections* if it is not already listed)
3. Select the IBM i system in the list of connections
4. Sign on using a user profile with *ALLOBJ special authority
5. Expand the IBM i system in the list of connections
6. Select **Network** > **Enterprise Identity Mapping**
7. Select **Configure system for EIM** in the *Enterprise Identity Mapping tasks* window to start the Enterprise Identity Mapping configuration wizard
8. Select the **Join an existing domain** option on the *Welcome* page; select **Next**
9. Select the **No** option on the *Configure Network Authentication Service* page (this was completed in a previous task); select **Next**
10. Configure the EIM domain controller information on the *Specify Domain Controller* page
    a. Specify the EIM domain controller name in the **Domain controller name** field (for example, specify `X1519P4.RCHLAND.IBM.COM`)
    b. Clear the **Use secure connection (SSL or TLS)** option if it is not already cleared
    c. Specify the EIM domain controller port in the **Port** field (for example, specify `389`)
    d. Select **Next**
11. Specify the LDAP administrator credentials on the *Specify User For Connection* page
    a. Select `Distinguished name and password` in the **User type** field
    b. Specify the LDAP administrator distinguished name in the **Distinguished name** field (for example, specify `cn=administrator`)
    c. Specify the LDAP administrator password in the **Password** and **Confirm password** fields (for example, specify `secret` in both fields)
    d. Select **Next**
12. Select your EIM domain from the **Domains** list on the *Specify Domains* page (for example, select `EimDomain`); select **Next**
13. Select the registries to create in the EIM domain on the *Registry Information* page
    a. Select the **Local i5/OS** option and verify your IBM i system is displayed in the associated input field (for example, verify `LP11UT11.RCHLAND.IBM.COM` is displayed)
    b. Select the **Kerberos** option and verify your realm name is displayed in the associated input field (for example, verify `DEPT144.RCHLAND.IBM.COM` is displayed)
    c. Clear the **Kerberos user identities are case sensitive** option
    d. Select **Next**

14. Specify the LDAP administrator credentials on the *Specify EIM System User* page
    a. Select `Distinguished name and password` in the **User type** field
    b. Specify the LDAP administrator distinguished name in the **Distinguished name** field (for example, specify `cn=administrator`)
    c. Specify the LDAP administrator password in the **Password** and **Confirm password** fields (for example, specify `secret` in both fields)
    d. Select **Next**
15. Review the information on the *Summary* page; select **Finish** to complete the wizard

    Note: If the Local i5/OS or Kerberos registries already exist in the EIM domain, an EIM configuration error dialog is displayed. Select the **No** option in the dialog and select **OK** to continue.

2.4 Create krbsvr400 Service Principal

The following information describes how to create the krbsvr400 service principal on the Windows domain controller. A service principal is created by assigning a service principal name to a user account. The account must also be trusted for delegation. Use the `DSADD` command to create a user account. Use the `KTPASS` command to assign the service principal name. Use *Active Directory Users and Groups* to trust the account for delegation.

If you are already using IBM i Access for Windows with integrated Windows domain login for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), this task has already been completed.

User account	krbsvr400_lp11ut11
Service principal name	krbsvr400/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
Password	kerberos

Table 6: Sample values from example environment used in krbsvr400 service principal creation task

Creating the krbsvr400 service principal consists of the following steps:

1. Log on to the Windows domain controller using a user account with administrative privileges
2. Open a command prompt

3. Create a user account using the DSADD command

   The following example creates account krbsvr400_lp11ut11 and assigns the password kerberos. The password does not expire and does not need to be changed.

```
dsadd user CN=krbsvr400_lp11ut11,CN=Users,DC=DEPT144,DC=RCHLAND,DC=IBM,DC=COM
      -pwd kerberos
      -display krbsvr400_lp11ut11
      -desc "Service principal (krbsvr400) for lp11ut11"
      -mustchpwd no
      -pwdneverexpires yes
```

4. Assign the krbsvr400 service principal name to the user account using the KTPASS command

   The following example assigns service principal name krbsvr400/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM to user account krbsvr400_lp11ut11 and assigns the password kerberos. If using one of the DES encryption types, add the +DesOnly parameter to the command.

```
ktpass -princ krbsvr400/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -mapuser krbsvr400_lp11ut11
       -mapop set
       -ptype KRB5_NT_PRINCIPAL
```

5. Open *Active Directory Users and Groups*
6. Expand the domain in the console tree (for example, expand DEPT144.RCHLAND.IBM.COM) and select **Users**
7. Select the user account in the details pane (for example, select krbsvr400_lp11ut11)
8. Select **Properties** from the *Actions* menu
9. Select the **Account** tab
10. Select the **Account is trusted for delegation** option under *Account options* (scroll the list of options to find this option)
11. Enable use of AES encryption types if desired (Windows Server 2008 or later)
    a. Select the **This account supports Kerberos AES 128 bit encryption** option under *Account options* (scroll the list of options to find this option)
    b. Select the **This account supports Kerberos AES 256 bit encryption** option under *Account options* (scroll the list of options to find this option)
12. Select **OK**

2.5 Create HTTP Service Principal

The following information describes how to create the HTTP service principal on the Windows domain controller. A service principal is created by assigning a service principal name to a user account. The account must also be trusted for delegation. Use the DSADD command to create a user account. Use the KTPASS command to assign the service principal name. Use *Active Directory Users and Groups* to trust the account for delegation.

User account	HTTP_lp11ut11
Service principal name	HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
Password	kerberos

Table 7: Sample values from example environment used in HTTP service principal creation task

Creating the HTTP service principal consists of the following steps:

1. Log on to the Windows domain controller using a user account with administrative privileges
2. Open a command prompt
3. Create a user account using the `DSADD` command

   The following example creates account `HTTP_lp11ut11` and assigns the password `kerberos`. The password does not expire and does not need to be changed.

```
dsadd user CN=HTTP_lp11ut11,CN=Users,DC=DEPT144,DC=RCHLAND,DC=IBM,DC=COM
      -pwd kerberos
      -display HTTP_lp11ut11
      -desc "Service principal (HTTP) for lp11ut11"
      -mustchpwd no
      -pwdneverexpires yes
```

4. Assign the HTTP service principal name to the user account using the `KTPASS` command

   The following example assigns service principal name `HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM` to user account `HTTP_lp11ut11` and assigns the password `kerberos`. If using one of the DES encryption types, add the `+DesOnly` parameter to the command.

```
ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -mapuser HTTP_lp11ut11
       -mapop set
       -ptype KRB5_NT_PRINCIPAL
```

5. Open *Active Directory Users and Groups*
6. Expand the domain in the console tree (for example, expand `DEPT144.RCHLAND.IBM.COM`) and select **Users**
7. Select the user account in the details pane (for example, select `HTTP_lp11ut11`)
8. Select **Properties** from the *Actions* menu
9. Select the **Account** tab
10. Select the **Account is trusted for delegation** option under *Account options* (scroll the list of options to find this option)

11. Enable use of AES encryption types if desired (Windows Server 2008 or later)
    a. Select the **This account supports Kerberos AES 128 bit encryption** option under *Account options* (scroll the list of options to find this option)
    b. Select the **This account supports Kerberos AES 256 bit encryption** option under *Account options* (scroll the list of options to find this option)
12. Select **OK**

2.6 Create JGSS Configuration

The following information describes how to create a Java Generic Security Service (JGSS) configuration for use by WebSphere Application Server. JGSS is an implementation of the GSS-API framework that uses Kerberos as the underlying security system. WebSphere Application Server uses JGSS with SPNEGO to authenticate users using Kerberos credentials. Web applications use JGSS to create Kerberos credentials for authenticating connections to other servers. JGSS configuration consists of a keytab file and a Kerberos configuration file. These files are used in a later task while configuring SPNEGO web authentication in a WebSphere Application Server profile. Use the `KTPASS` command to create the keytab file. Use a text editor to create the Kerberos configuration file.

Service principal	HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
Password	kerberos
Keytab file name	spnego.krb5.keytab
Kerberos configuration file name	spnego.krb5.conf
Realm name (Windows domain)	DEPT144.RCHLAND.IBM.COM
KDC name and port (Windows domain contoller)	eap2003.rchland.ibm.com:88
Network domain name	rchland.ibm.com

Table 8: Sample values from example environment used in the create JGSS configuration task

Configuring JGSS consists of the following steps:

1. Log on to the Windows domain controller using a user account with administrative privileges
2. Open a command prompt

3. Export keys for the HTTP service principal to a keytab file using the `KTPASS` command

   The keys can be exported with the following encryption types: `DES-CBC-CRC`, `DES-CBC-MD5`, `RC4-HMAC-NT`, `AES128-SHA1`, and `AES256-SHA1` (the AES encryption types are only supported with Windows Server 2008 or later).

   The following example exports a key with the `RC4-HMAC-NT` encryption type for the `HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM` service principal to a keytab file named `spnego.krb5.keytab`.

```
ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto RC4-HMAC-NT
       -out spnego.krb5.keytab
```

   The following example exports keys with multiple encryption types for the `HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM` service principal to a keytab file named `spnego.krb5.keytab`.

```
ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto DES-CBC-CRC
       -out spnego.krb5.keytab

ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto DES-CBC-MD5
       -out spnego.krb5.keytab
       -in spnego.krb5.keytab

ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto RC4-HMAC-NT
       -out spnego.krb5.keytab
       -in spnego.krb5.keytab

ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto AES128-SHA1
       -out spnego.krb5.keytab
       -in spnego.krb5.keytab

ktpass -princ HTTP/lp11ut11.rchland.ibm.com@DEPT144.RCHLAND.IBM.COM
       -pass kerberos
       -ptype KRB5_NT_PRINCIPAL
       -crypto AES256-SHA1
       -out spnego.krb5.keytab
       -in spnego.krb5.keytab
```

4. Create a Kerberos configuration file named `spengo.krb5.conf` containing the following text using a text editor

```
[libdefaults]
  default_realm = DEFAULT_REALM_VALUE
  default_keytab_name =FILE:/QIBM/UserData/OS400/NetworkAuthentication/keytab/spnego.krb5.keytab
  default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac des-cbc-md5 des-cbc-crc
  default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac des-cbc-md5 des-cbc-crc
  forwardable = true
  renewable = true
  noaddresses = true
  clockskew = 300
[realms]
  DEFAULT_REALM_VALUE = {
    kdc = KDC_VALUE
    default_domain = DEFAULT_DOMAIN_VALUE
  }
[domain_realm]
  .DEFAULT_DOMAIN_VALUE = DEFAULT_REALM_VALUE
```

   a. Replace `DEFAULT_REALM_VALUE` with the realm name of your Windows domain
   b. Replace `KDC_VALUE` with the fully-qualified DNS name and port of your KDC
   c. Replace `DEFAULT_DOMAIN_VALUE` with the domain name for your network

   The following example Kerberos configuration file uses values from the example environment.

```
[libdefaults]
  default_realm = DEPT144.RCHLAND.IBM.COM
  default_keytab_name =FILE:/QIBM/UserData/OS400/NetworkAuthentication/keytab/spnego.krb5.keytab
  default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac des-cbc-md5 des-cbc-crc
  default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac des-cbc-md5 des-cbc-crc
  forwardable = true
  renewable = true
  noaddresses = true
  clockskew = 300
[realms]
  DEPT144.RCHLAND.IBM.COM = {
    kdc = eap2003.rchland.ibm.com:88
    default_domain = rchland.ibm.com
  }
[domain_realm]
  .rchland.ibm.com = DEPT144.RCHLAND.IBM.COM
```

5. Copy the `spnego.krb5.conf` file to the `/QIBM/UserData/OS400/NetworkAuthentication` directory in the IBM i integrated file system
6. Copy the `spnego.krb5.keytab` file to the `/QIBM/UserData/OS400/NetworkAuthentication/keytab` directory in the IBM i integrated file system

3. Configure WebSphere Application Server

A WebSphere Application Server (WAS) profile must be created on the IBM i system and configured to use SPNEGO for authentication. This involves creating the WebSphere Application Server profile and associated HTTP server, securing the profile using Microsoft Active Directory as the user repository, configuring the profile for single sign-on, and configuring the profile to use SPENGO for authentication. Once the profile has been SPNEGO-enabled, IBM i Access for Web can be deployed in the profile.

3.1 Create Profile

The following information describes how to create a WebSphere Application Server profile and associated HTTP server. Use the Create Application Server wizard in IBM Web Administration for i to create the WebSphere Application Server profile.

This task assumes IBM Web Administration for i is already running.

IBM i system	LP11UT11.RCHLAND.IBM.COM
IBM Web Administration for i URL	http://lp11ut11.rchland.ibm.com:2001/HTTPAdmin
WebSphere Application Server option	V7.0 Express
Application server name	iwa70expk
HTTP server name	IWA70EXPK
HTTP server IP address	All IP addresses
HTTP server port	27600
Application server first port in range	27605

Table 9: Sample values from example environment used in the create profile task

Creating a WebSphere Application Server profile consists of the following steps:

1. Open a browser window
2. Specify the URL to IBM i Web Administration for i on your IBM i system (for example, specify `http://lp11ut11.rchland.ibm.com:2001/HTTPAdmin`)
3. Log on with a user profile that has the *ALLOBJ, *IOSYSCFG, *JOBCTL, and *SECADM special authorities
4. Select the **Setup** tab
5. Expand **Common Tasks and Wizards** if it is not already expanded
6. Select **Create Application Server** to start the Create Application Server wizard
7. Select **Next** on the welcome page

8. Select one of the options under **WebSphere Application Server** on the *Select Application Server Version and Type* page (for example, select `V7.0 Express`); select **Next**
9. Specify an application server name and description on the *Specify Application Server Name* page
    a. Specify a name for the WebSphere Application Server profile in the **Application server name** field (for example, specify `iwa70expk`)
    b. Specify a description for the profile in the **Server description** field or leave the default description
    c. Select **Next**
10. Select the **Create a new HTTP server (powered by Apache)** option on the *Select HTTP Server Type* page; select **Next**
11. Specify information for creating the HTTP server on the *Create a new HTTP server (powered by Apache)* page
    a. Specify a name for the HTTP server in the **HTTP server name** field (for example, specify `IWA70EXPK`)
    b. Specify a description for the HTTP server in the **HTTP server description** field or leave the default description
    c. Select the IP address on which your HTTP server will listen in the **IP address** field (for example, select `All IP addresses`)
    d. Specify the port on which your HTTP server will listen in the **Port** field (for example, specify `27600`)
    e. Select **Next**
12. Specify the first in a range of ports for the WebSphere Application Server profile to use in the **First port in range** field on the *Specify Internal Ports Used by the Application Server* page (for example, specify `27605`); select **Next**
13. Select **Next** on the *Select Sample Applications* page
14. Select the **Do not configure Identity Tokens** option on the *Configure Identity Token SSO for Web to Access IBM i* page; select **Next**
15. Review the information on the *Summary* page; select **Finish** to complete the wizard
16. Wait for the WebSphere Application Server profile to be created and have a status of **Stopped**
17. Start the WebSphere Application Server profile
18. Wait for the WebSphere Application Server profile to have a status of **Running**

3.2 Secure Profile Using Microsoft Active Directory

The following information describes how to secure a WebSphere Application Server profile using Microsoft Active Directory as a user account repository. Use the security configuration wizard from the security tasks in the WebSphere Integrated Solutions Console to secure the WebSphere Application Server profile.

There are several options for user account repositories when securing a WebSphere Application Server profile. The default user account repository is built into WebSphere Application Server and can be federated with one or more external LDAP repositories. Other options include a stand-alone external LDAP registry or the local operating system. For more information on securing a WebSphere Application Server profile, see the *Securing applications and their environment* article in the WebSphere Application Server information center. The WebSphere Application Server information centers can be found at the WebSphere Application Server Library (http://www.ibm.com/software/webservers/appserv/was/library/).

This task secures the WebSphere Application Server profile using Microsoft Active Directory as a stand-alone LDAP registry.

This task assumes the WebSphere Application Server profile is already running.

WebSphere Integrated Solutions Console URL	http://lp11ut11.rchland.ibm.com:27606/ibm/console/
Administrative user name	wasadmin
Type of LDAP server	Microsoft Active Directory
LDAP server name	eap2003.rchland.ibm.com
LDAP server port	389
Base distinguished name	dc=dept144,dc=rchland,dc=ibm,dc=com
Bind distinguished name	cn=wasadmin,cn=users,dc=dept144,dc=rchland,dc=ibm,dc=com
Bind password	wasadmin

Table 10: Sample values from example environment used in the secure profile task

Securing a WebSphere Application Server profile using Microsoft Active Directory as a stand-alone LDAP registry consists of the following steps:

1. Open a browser window
2. Specify the URL to the WebSphere Integrated Solutions Console for the profile (for example, specify `http://lp11ut11.rchland.ibm.com:27606/ibm/console/`)
3. Select **Log in** to log on to the console (credentials are not required until security is enabled)
4. Select **Security** > **Global security** in the list of tasks (for WAS V6.1, select **Security** > **Secure administration, applications, and infrastructure**)
5. Select **Security Configuration Wizard** to start a wizard for enabling security
6. Specify the security options on the *Specify extent of protection* page
   a. Select the **Enable application security** option if it is not already selected

b. Clear the **Use Java 2 security to restrict application access to local resources** option if it is not already cleared

c. Select **Next**

7. Select **Standalone LDAP registry** on the *Select user repository* page; select **Next**
8. Specify information about the LDAP registry on the *Configure user repository* page
   a. Specify the administrative user name in the **Primary administrative user name** field (for example, specify `wasadmin`)
   b. Select the type of LDAP server in the **Type of LDAP server** field (for example, select `Microsoft Active Directory`)
   c. Specify the name of the LDAP server in the **Host** field (for example, specify `eap2003.rchland.ibm.com`)
   d. Specify the port used by the LDAP server in the **Port** field (for example, specify `389`)
   e. Specify the base distinguished name used for searches in the directory in the **Base distinguished name (DN)** field (for example, specify `dc=dept144,dc=rchland,dc=ibm,dc=com`)
   f. Specify the distinguished name used to bind to the LDAP server in the **Bind distinguished name (DN)** field (for example, specify `cn=wasadmin,cn=users,dc=dept144,dc=rchland,dc=ibm,dc=com`)
   g. Specify the password used to bind to the LDAP server in the **Bind password** field (for example, specify `wasadmin`)
   h. Select **Next**
9. Review the information on the *Summary* page; select **Finish** to complete the wizard
10. Select **Save** in the *Messages* box at the top of the page to save the changes

3.3 Configure Single Sign-on

The following information describes how to configure single sign-on for a WebSphere Application Server profile. Use the WebSphere Integrated Solutions Console to configure single sign-on for the WebSphere Application Server profile.

This task assumes the **Secure Profile Using Microsoft Active Directory** task has just been completed. The WebSphere Integrated Solutions Console is displaying the *Global security* page (for WAS V6.1, the *Secure administration, applications, and infrastructure* page).

Domain name (Network domain name)	rchland.ibm.com
LTPA V1 cookie name (WAS 8.0 only)	LtpaToken
LTPA V2 cookie name (WAS 8.0 only)	LtpaToken2

Table 11: Sample values from example environment used in the configure single sign-on task

Configuring single sign-on for a WebSphere Application Server profile consists of the following steps:

1. Select **Web and SIP security** > **Single sign-on (SSO)** in the *Authentication* group (for WAS V6.1, select **Web security** > **single sign-on (SSO)**)
2. Select the **Enabled** option if it is not already selected
3. Clear the **Requires SSL** option if it is not already cleared
4. Specify the network domain name in the **Domain name** field (for example, specify `rchland.ibm.com`)
5. Select the **Interoperability Mode** option if it is not already selected
6. Specify the names for the LTPA cookies if using WAS V8.0
   a. Specify the name for the LTPA V1 cookie in the **LTPA V1 cookie name** field (for example, specify `LtpaToken`)
   b. Specify the name for the LTPA V2 cookie in the **LTPA V2 cookie name** field (for example, specify `LtpaToken2`)
7. Select the **Web inbound security attribute propagation** option if it is not already selected
8. Select the **Set security cookies to HTTPOnly to help prevent cross-site scripting attacks** option if using WAS V8.0 and it is not already selected
9. Select **OK**
10. Select **Save** in the *Messages* box at the top of the page to save the changes

3.4 Configure SPNEGO

The following information describes how to configure SPNEGO for a WebSphere Application Server profile. Use the WebSphere Integrated Solutions Console to configure SPNEGO for the WebSphere Application Server profile.

WebSphere Application Server V6.1 provides SPNEGO support via a Trust Association Interceptor (TAI). WebSphere Application Server V7.0 and later provide SPNEGO support via SPNEGO web authentication. This task provides steps for configuring both the SPNEGO TAI and SPNEGO web authentication. Use the steps that apply to your version of WebSphere Application Server.

This task assumes the **Configure Single Sign-on** task has just been completed. The WebSphere Integrated Solutions Console is displaying the *Global security* page (for WAS V6.1, the *Secure administration, applications, and infrastructure* page).

3.4.1 Configure SPENGO TAI (WAS V6.1)

IBM i system	lp11ut11.rchland.ibm.com
Application server	iwa61expk
JGSS Kerberos configuration file	/QIBM/UserData/OS400/NetworkAuthentication/spnego.krb5.conf

Table 12: Sample values from example environment used in the configure SPNEGO TAI task

Configuring the SPNEGO Trust Association Intercepter for a WebSphere Application Server V6.1 profile consists of the following steps:

1. Select **Web security** > **Trust association** in the *Authentication* group
2. Select the **Enable trust association** option
3. Select **Apply**
4. Select **Interceptors** under *Additional Properties*
5. Select **com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl**
6. Select **Custom properties** under *Additional Properties*
7. Select **New**
8. Specify information for the hostname custom property
   a. Specify `com.ibm.ws.security.spnego.SPN1.hostName` in the **Name** field
   b. Specify the name of your IBM i system in the **Value** field (for example, specify `lp11ut11.rchland.ibm.com`)
   c. Select **OK**
9. Select **New**
10. Specify information for the enable credential delegation custom property
    a. Specify `com.ibm.ws.security.spnego.SPN1.enableCredDelegate` in the **Name** field
    b. Specify `true` in the **Value** field
    c. Select **OK**
11. Select **Save** in the *Messages* box at the top of the page to save the changes
12. Select **Servers** > **Application servers** in the list of tasks
13. Select your application server from the *Application servers* list (for example, select `iwa61expk`)

14. Select **Java and Process Management** > **Process Definition** under *Server Infrastructure*
15. Select **Java Virtual Machine** under *Additional Properties*
16. Select **Custom Properties** under *Additional Properties*
17. Select **New**
18. Specify information for the enable SPNEGO custom property
    a. Specify `com.ibm.ws.security.spnego.isEnabled` in the **Name** field
    b. Specify `true` in the **Value** field
    c. Select **OK**
19. Select **New**
20. Specify information for the Kerberos configuration file custom property
    a. Specify `java.security.krb5.conf` in the **Name** field
    b. Specify the fully-qualified path to the JGSS Kerberos configuration file in the **Value** field (for example, specify `/QIBM/UserData/OS400/NetworkAuthentication/spnego.krb5.conf`)
    c. Select **OK**
21. Select **Save** in the *Messages* box at the top of the page to save the changes
22. Select **Logout** to log out of the WebSphere Integrated Solution Console
23. Restart the WebSphere Application Server profile to enable the security changes

3.4.2 Configure SPNEGO web authentication (WAS V7.0 and later)

IBM i system	lp11ut11.rchland.ibm.com
JGSS Kerberos configuration file	/QIBM/UserData/OS400/NetworkAuthentication/spnego.krb5.conf

Table 13: Sample values from example environment used in the configure SPNEGO web authentication task

Configuring SPNEGO web authentication for a WebSphere Application Server V7.0 or later profile consists of the following steps:

1. Select **Web and SIP security** > **SPNEGO web authentication** in the *Authentication* group
2. Select the **New** under *SPNEGO Filters*
3. Specify information to configure the filter
    a. Specify the name of your IBM i system in the **Host name** field (for example, specify `lp11ut11.rchland.ibm.com`)
    b. Select the **Trim Kerberos realm from principal name** option

c. Select the **Enable delegation of Kerberos credentials** option

d. Select **OK**

4. Clear the **Use the alias host name for the application server** option if using WAS V8.0
5. Clear the **Dynamically update SPNEGO** option if it is not already cleared
6. Select the **Enable SPNEGO** option
7. Clear the **Allow fall back to application authentication mechanism** option if it is not already cleared
8. Specify the fully-qualified path to the JGSS Kerberos configuration file in the **Kerberos configuration file with full path** field (for example, specify `/QIBM/UserData/OS400/NetworkAuthentication/spnego.krb5.conf`)
9. Select **OK**
10. Select **Save** in the *Messages* box at the top of the page to save the changes
11. Select **Logout** to log out of the WebSphere Integrated Solution Console
12. Restart the WebSphere Application Server profile to enable the security changes

3.5 Configure IBM i Access for Web

The following information describes how to configure IBM i Access for Web to run in a SPNEGO-enabled WebSphere Application Server profile. Use the IBM i Access for Web `CFGACCWEB2` CL command or `cfgaccweb2` Qshell script to configure IBM i Access for Web.

Two commands are provided for configuring IBM i Access for Web: the `QIWA2/CFGACCWEB2` CL command and the `/QIBM/ProdData/Access/Web2/install/cfgaccweb2` Qshell script. The command to use depends on the version and fix level of IBM i Access for Web, and the version of WebSphere Application Server. Use the command indicated for your environment in the following table. If both commands are listed, either command can be used.

XH2 Version	Required XH2 PTF	WAS Version	Supported Command
6.1		V6.1	`CFGACCWEB2` CL command `cfgaccweb2` Qshell script
6.1	SI33318 or supersede	V7.0	`cfgaccweb2` Qshell script
7.1		V6.1	`CFGACCWEB2` CL command `cfgaccweb2` Qshell script
7.1		V7.0	`CFGACCWEB2` CL command `cfgaccweb2` Qshell script
7.1	SI45095 or supersede	V8.0	`cfgaccweb2` Qshell script

Table 14: Commands supported for configuring IBM i Access for Web based on XH2 version and PTF, and WAS version

This task assumes the **Configure SPNEGO** task has been completed and the WebSphere Application Server profile is already running.

Application server type (APPSVRTYPE, -appsvrtype)	*WAS70EXP
WAS profile name (WASPRF, -wasprf)	iwa70expk
Application server name (APPSVR, -appsvr)	iwa70expk
WAS install location (WASINSDIR, -wasinsdir)	/QIBM/ProdData/WebSphere/AppServer/V7/Express
Authentication type (AUTHTYPE, -authtype)	*APPSVR
Authentication method (AUTHMETHOD, -authmethod)	*KERBEROS
WAS administrative user (WASUSRID, -wasusrid)	wasadmin
WAS administrative user password (WASPWD, -waspwd)	wasadmin

Table 15: Sample values from example environment used in the configure IBM i Access for Web task

3.5.1 Use CFGACCWEB2 CL Command

Configuring IBM i Access for Web using the `QIWA2/CFGACCWEB2` CL command consists of the following steps:

1. Start a 5250 display session to the IBM i system
2. Sign on using a user profile with *ALLOBJ special authority
3. Configure IBM i Access for Web using the `CFGACCWEB2` CL command

```
QIWA2/CFGACCWEB2 APPSVRTYPE(*WAS70EXP)
        WASPRF(iwa70expk) APPSVR(iwa70expk)
        WASINSDIR('/QIBM/ProdData/WebSphere/AppServer/V7/Express')
        AUTHTYPE(*APPSVR) AUTHMETHOD(*KERBEROS)
        WASUSRID(wasadmin) WASPWD(wasadmin)
```

4. Restart the WebSphere Application Server profile and associated HTTP server

3.5.2 Use cfgaccweb2 Qshell Script

Configuring IBM i Access for Web using the `cfgaccweb2` Qshell script consists of the following steps:

1. Start a 5250 display session to the IBM i system

2. Sign on using a user profile with *ALLOBJ special authority
3. Start the Qshell environment using the `QSH` CL command
4. Configure IBM i Access for Web using the `cfgaccweb2` Qshell script

```
/QIBM/ProdData/Access/Web2/install/cfgaccweb2 -appsvrtype *WAS70EXP
        -wasprf iwa70expk -appsvr iwa70expk
        -wasinsdir /QIBM/ProdData/WebSphere/AppServer/V7/Express
        -authtype *APPSVR -authmethod *KERBEROS
        -wasusrid wasadmin -waspwd wasadmin
```

5. Restart the WebSphere Application Server profile and associated HTTP server

4. Configure User Access

Each user of the SPNEGO-enabled WebSphere Application Server profile must have their environment configured to use SPNEGO. This involves creating an IBM i user profile, creating the home directory for the IBM i user profile, creating an EIM identifier and associations, configuring the browser to use SPNEGO, and accessing IBM i Access for Web.

These tasks assume a user account has already been created in the Windows domain, and the workstation has already been added to the domain.

4.1 Create IBM i User Profile

The following information describes how to create a user profile on the IBM i system. Use the `CRTUSRPRF` CL command to create a user profile.

Complete this task only if a user profile does not already exist.

User profile (USRPRF)	TSMITH
Password (PASSWORD)	*NONE
Text 'description' (TEXT)	User profile for Tom Smith

Table 16: Sample values from example environment used in user profile creation task

Creating the user profile consists of the following steps:

1. Start a 5250 display session to the IBM i system
2. Sign on using a user profile with *SECADM special authority
3. Create a user profile using the `CRTUSRPRF` CL command

   The following example creates user profile `tsmith` without a password.

```
QSYS/CRTUSRPRF USRPRF(TSMITH) PASSWORD(*NONE)
               TEXT('User profile for Tom Smith')
```

4.2 Create Home Directory for IBM i User Profile

The following information describes how to create the home directory for the user profile in the integrated file system. Use the `CRTDIR` CL command to create the home directory. Use the `CHGOWN` CL command to make the user profile the owner of the home directory.

The **Home directory** attribute of the user profile specifies the path of the home directory. Use the `DSPUSRPF` CL command to display the path of the home directory. Use the `WRKLNK` CL command to determine if the home directory exists. Complete this task only if a home directory for the user profile does not already exist.

User profile	TSMITH
Home directory (DIR)	/home/TSMITH

Table 17: Sample values from example environment used in home directory creation task

Creating the home directory for the user profile consists of the following steps:

1. Start a 5250 display session to the IBM i system
2. Sign on using a user profile with *SECADM special authority
3. Create the home directory for the user profile using the `CRTDIR` CL command

   The following example creates the `/home/TSMITH` directory in the integrated file system.

   ```
   QSYS/CRTDIR DIR('/home/TSMITH')
   ```

4. Make the user profile the owner of the home directory

   The following example makes `TSMITH` the owner of the `/home/TSMITH` directory.

   ```
   QSYS/CHGOWN OBJ('/home/TSMITH') NEWOWN(TSMITH) RVKOLDAUT(*YES)
   ```

4.3 Create EIM Identifier and Associations

The following information describes how to create an EIM identifier. Associations are added to the identifier in order to allow the Windows domain user to be mapped to an IBM i user profile. Use the Enterprise Identity Mapping tasks in *System i Navigator* to create the identifier and add associations.

If you are already using IBM i Access for Windows with integrated Windows domain login for your connections (Properties > Connection > Signon information > Use Kerberos principal name, no prompting), this task has already been completed.

IBM i system	LP11UT11.RCHLAND.IBM.COM
EIM domain name	EimDomain
Parent distinguished name	None
EIM domain controller (LDAP server)	X1519P4.RCHLAND.IBM.COM
EIM domain controller port	389
LDAP administrator distinguished name	cn=administrator
LDAP administrator password	secret
EIM identifier name	Tom Smith/Rochester/IBM
Windows domain EIM registry (Windows domain) (Realm name)	DEPT144.RCHLAND.IBM.COM

Windows domain user account	toms
IBM i EIM registry (IBM i system)	LP11UT11.RCHLAND.IBM.COM
IBM i user profile	TSMITH

Table 18: Sample values from example environment used in EIM identifier and associations creation task

Creating an EIM identifier and adding associations consists of the following steps:

1. Use *System i Navigator* to access IBM i system settings
2. Add the IBM i system to the list of connections if necessary (for example, add `LP11UT11.RCHLAND.IBM.COM` to *My Connections* if it is not already listed)
3. Select the IBM i system in the list of connections
4. Sign on using a user profile with *ALLOBJ special authority
5. Expand the IBM i system in the list of connections
6. Select **Network** > **Enterprise Identity Mapping** > **Domain Management**
7. Add the EIM domain to the list of domains if it is not listed
   a. Select **Add a domain** from the *Enterprise Identity Mapping tasks* window
   b. Specify the EIM domain name in the **Domain** field (for example, specify `EimDomain`)
   c. Specify the parent distinguished name of the EIM domain within the directory in the **Parent DN** field (for example, specify `None`)
   d. Specify the name of the EIM domain controller in the **Domain controller** field (for example, specify `X1519P4.RCHLAND.IBM.COM`)
   e. Clear the **Use secure connection (SSL or TLS)** option
   f. Specify the EIM domain controller port in the **Port** field (for example, specify `389`)
   g. Select **OK**
8. Expand **Domain Management**
9. Select the EIM domain (for example, select `EimDomain`)
10. Specify the credentials for connecting to the EIM domain controller in the *Connect to EIM Domain Controller* window
    a. Select Distinguished name in the **User type** field
    b. Specify the LDAP administrator distinguished name in the **Distinguished name** field (for example, specify `cn=administrator`)
    c. Select the **Specify password** option and specify the LDAP administrator password in the input field (for example, specify `secret`)
    d. Select **OK**

11. Expand the EIM domain (for example, expand `EimDomain`)
12. Select **Identifiers**
13. Select **Create a new identifier** from the *Enterprise Identity Mapping tasks* window
14. Specify the information for the identifier in the *New EIM Identifier* window
    a. Specify a unique name for the EIM identifier in the **Identifier** field (for example, specify `Tom Smith/Rochester/IBM`)
    b. Clear the **Generate unique identifier** field if it is not already cleared
    c. Specify a description for the EIM identifier in the **Description** field if desired
    d. Select **OK**
15. Select the identifier in the list of identifiers (scroll the list to find the identifier)
16. Select **Properties** from the *File* menu
17. Select the **Associations** tab
18. Select the **Add...** button
19. Specify the information for the Windows domain association in the **Add Association** window
    a. Specify the name of the EIM registry representing the Windows domain in the **Registry** field (for example, specify `DEPT144.RCHLAND.IBM.COM`)
    b. Specify the Windows domain user account in the **User** field (for example, specify `toms`)
    c. Select `Source` in the **Association type** field
    d. Select **OK**
20. Select the **Add...** button
21. Specify the information for the IBM i system association in the **Add Association** window
    a. Specify the name of the EIM registry representing the IBM i system in the **Registry** field (for example, specify `LP11UT11.RCHLAND.IBM.COM`)
    b. Specify the IBM i user profile in the the **User** field (for example, specify `TSMITH`)
    c. Select `Target` in the **Association type** field
    d. Select **OK**
22. Select **OK**

4.4 Configure Web Browser

The following information describes how to configure the browser to enable SPNEGO.

Internet Explorer, Mozilla Firefox, and Google Chrome support SPNEGO. This task provides steps for configuring each browser. Use the steps for the browser used in your environment.

4.4.1 Internet Explorer

This task assumes you are logged on to a workstation in the Windows domain using a Windows domain user account.

IBM i Access for Web base URL	http://lp11ut11.rchland.ibm.com
WebSphere Integrated Solutions Console base URL	https://lp11ut11.rchland.ibm.com

Table 19: Sample values from example environment used in the Internet Explorer configuration task

Configuring Internet Explorer to enable SPNEGO consists of the following steps:

1. Open Internet Explorer
2. Select **Internet Options** from the *Tools* menu
3. Select the **Security** tab
4. Select `Local intranet` in the **Select a zone to view or change security settings** group
5. Select **Sites**
6. Select **Advanced** in the *Local intranet* window
7. Add the URL for IBM i Access for Web to the trusted sites
   a. Specify the base URL used to access IBM i Access for Web on your IBM i system in the **Add this website to the zone** field (for example, specify `http://lp11ut11.rchland.ibm.com`)
   b. Select **Add**
8. Add the URL for the WebSphere Integrated Solutions Console to the trusted sites if configuring the browser for the Windows domain user account that is the WAS administrative user
   a. Specify the base URL used to access the WebSphere Integrated Solutions Console for the WAS profile in the **Add this website to the zone** field (for example, specify `https://lp11ut11.rchland.ibm.com`)
   b. Select **Add**
9. Select **Close**
10. Select **OK**
11. Select the **Advanced** tab
12. Select the **Enable Integrated Windows Authentication** option under *Settings* > *Security* if it is not already selected (scroll the list of options to find this option)
13. Select **OK**
14. Restart the workstation to enable the changes

4.4.2 Mozilla Firefox

This task assumes you are logged on to a workstation in the Windows domain using a Windows domain user account.

IBM i system	lp11ut11.rchland.ibm.com

Table 20: Sample values from example environment used in the Mozilla Firefox configuration task

Configuring Mozilla Firefox to enable SPNEGO consists of the following steps:

1. Open Mozilla Firefox
2. Specify `about:config` in the **Go to a Website** field
3. Select **I'll be careful, I promise!** in the *This might void your warranty!* window
4. Specify `network.n` in the **Filter** field
5. Select the **network.negotiate-auth.delegation-uris** preference in the list of preferences
6. Press **Enter** to modify the value
7. Specify the name of your IBM i system in the input field (for example, specify `lp11ut11.rchland.ibm.com`)
8. Select **OK**
9. Select the **network.negotiate-auth.trusted-uris** preference in the list of preferences
10. Press **Enter** to modify the value
11. Specify the name of your IBM i system in the input field (for example, specify `lp11ut11.rchland.ibm.com`)
12. Select **OK**
13. Restart Mozilla Firefox to enable the changes

4.4.3 Google Chrome

Google Chrome uses policies or command line options to enable SPNEGO support.

The `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies specify a list of server names enabled for SPNEGO. Multiple servers are separated with commas. Wildcards (*) are allowed in the names. The policies are stored in the Windows registry under `HKEY_LOCAL_MACHINE` or `HKEY_CURRENT_USER` in path `Software\Policies\Google\Chrome`. Both policies are strings (REG_SZ). Details about the Google Chrome policies can be found at http://www.chromium.org/administrators/policy-list-3. Policy templates for applying policies can be found at http://www.chromium.org/administrators/policy-templates.

The `--auth-server-whitelist` and `--auth-negotiate-delegate-whitelist` command line options specify a list of server names enabled for SPNEGO. Multiple servers are separated with commas. Wildcards (*) are allowed in the names. Details about these

command line options can be found at http://dev.chromium.org/developers/design-documents/http-authentication under *Integrated Authentication* and *Kerberos Delegation (Forwardable Tickets)*.

IBM i system	lp11ut11.rchland.ibm.com

Table 21: Sample values from example environment used in the Google Chrome configuration task

If using policies to enable SPNEGO, specify the name of your IBM i system as the value of both policies (for example, specify `lp11ut11.rchland.ibm.com`).

If using command line options to enable SPNEGO, specify the name of your IBM i system as the value of both command line options. The following example command uses values from the example environment.

```
"C:\Documents and Settings\Administrator\Local Settings\Application
Data\Google\Chrome\Application\chrome.exe"
        --auth-server-whitelist=lp11ut11.rchland.ibm.com
        --auth-negotiate-delegate-whitelist=lp11ut11.rchland.ibm.com
```

4.5 Access IBM i Access for Web

The following information describes how to access the IBM i Access for Web home page in a SPNEGO-enabled WebSphere Application Server profile. Use a SPNEGO-enabled browser to access IBM i Access for Web home page.

This task assumes you are logged on to a workstation in the Windows domain using a Windows domain user account.

IBM i Access for Web home page URL	http://lp11ut11.rchland.ibm.com:27600/webaccess/iWAHome
Windows domain user account	toms
IBM i user profile	TSMITH

Table 22: Sample values from example environment used in the accessing IBM i Access for Web task

Accessing the IBM i Access for Web home page consists of the following steps:

1. Open a browser window
2. Specify the URL to the IBM i Access for Web home page (for example, specify `http://lp11ut11.rchland.ibm.com:27600/webaccess/iWAHome`)

The IBM i Access for Web home page is displayed without prompting for credentials. The user displayed in the header of IBM i Access for Web pages is the IBM i user profile

specified in the target association of the EIM identifier for the user (for example, `TSMITH` is displayed).

5. Additional Information

If you are not able to access the IBM i Access for Web home page in the SPNEGO-enabled environment, it is necessary to determine which part of the environment is not working correctly. This involves listing the contents of the client ticket cache, listing the contents of the keytab files, testing the EIM mapping for the user, and enabling diagnostic tracing for the WebSphere Application Server profile.

5.1 List Contents of Client Ticket Cache

The following information describes how to list the contents of the Kerberos ticket cache on the Windows workstation. Use the `klist` command to list the contents of the Kerberos ticket cache.

The `klist` command can be downloaded from Microsoft.

This task assumes you are logged on to a workstation in the Windows domain using a Windows domain user account.

Listing the contents of the Kerberos ticket cache consists of the following steps:

1. Open a command prompt
2. List the ticket cache using the `klist` command

   The following example lists the ticket cache.

   ```
   klist tickets
   ```

5.2 List Contents of Keytab Files

The following information describes how to list the contents of the keytab files on the IBM i system. Use the `keytab` command in the Qshell environment to list the contents of the keytab files.

IBM i keytab file	/QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab
SPNEGO keytab file	/QIBM/UserData/OS400/NetworkAuthentication/keytab/spnego.krb5.keytab

Table 23: Sample values from example environment used in the list contents of keytab files task

Listing the contents of the keytab files using the `keytab` command in the Qshell environment consists of the following steps:

1. Start a 5250 display session to the IBM i system
2. Sign on using a user profile with authority to read files in the `/QIBM/UserData/OS400/NetworkAuthentication/keytab` directory
3. Start the Qshell environment using the `QSH` CL command

4. List the contents of the keytab file used by the network authentication service on the IBM i system

```
keytab list
```

5. List the contents of the SPNEGO keytab file used with JGSS for the WebSphere Application Server profile

```
keytab list
  -k /QIBM/UserData/OS400/NetworkAuthentication/keytab/spnego.krb5.keytab
```

5.3 Test EIM Mapping

The following information describes how to test an EIM mapping. Use the Enterprise Identity Mapping tasks in *System i Navigator* to test a mapping.

IBM i system	LP11UT11.RCHLAND.IBM.COM
EIM domain name	EimDomain
Parent distinguished name	None
EIM domain controller (LDAP server)	X1519P4.RCHLAND.IBM.COM
EIM domain controller port	389
LDAP administrator distinguished name	cn=administrator
LDAP administrator password	secret
Windows domain EIM registry (Windows domain) (Realm name)	DEPT144.RCHLAND.IBM.COM
Windows domain user account	toms
IBM i EIM registry (IBM i system)	LP11UT11.RCHLAND.IBM.COM
IBM i user profile	TSMITH

Table 24: Sample values from example environment used in the test EIM mapping task

Testing an EIM mapping consists of the following steps:

1. Use *System i Navigator* to access IBM i system settings
2. Add the IBM i system to the list of connections if necessary (for example, add `LP11UT11.RCHLAND.IBM.COM` to *My Connections* if it is not already listed)
3. Select the IBM i system in the list of connections
4. Sign on using a user profile with *ALLOBJ special authority
5. Expand the IBM i system in the list of connections
6. Select **Network** > **Enterprise Identity Mapping** > **Domain Management**

7. Add the EIM domain to the list of domains if it is not listed
   a. Select **Add a domain** from the *Enterprise Identity Mapping tasks* window
   b. Specify the EIM domain name in the **Domain** field (for example, specify `EimDomain`)
   c. Specify the parent distinguished name of the EIM domain within the directory in the **Parent DN** field (for example, specify `None`)
   d. Specify the name of the EIM domain controller in the **Domain controller** field (for example, specify `X1519P4.RCHLAND.IBM.COM`)
   e. Clear the **Use secure connection (SSL or TLS)** option
   f. Specify the EIM domain controller port in the **Port** field (for example, specify `389`)
   g. Select **OK**
8. Expand **Domain Management**
9. Select the EIM domain (for example, select `EimDomain`)
10. Specify the credentials for connecting to the EIM domain controller in the *Connect to EIM Domain Controller* window
    a. Select Distinguished name in the **User type** field
    b. Specify the LDAP administrator distinguished name in the **Distinguished name** field (for example, specify `cn=administrator`)
    c. Select the **Specify password** option and specify the LDAP administrator password in the input field (for example, specify `secret`)
    d. Select **OK**
11. Select **Test an EIM mapping** from the *Enterprise Identity Mapping tasks* window
12. Specify the credentials for connecting to the EIM domain controller in the *Connect to EIM Domain Controller* window
    a. Select Distinguished name in the **User type** field
    b. Specify the LDAP administrator distinguished name in the **Distinguished name** field (for example, specify `cn=administrator`)
    c. Select the **Specify password** option and specify the LDAP administrator password in the input field (for example, specify `secret`)
    d. Select **OK**
13. Specify the information for the EIM mapping in the *Test a Mapping* window
    a. Specify the name of the EIM registry representing the Windows domain in the **Source registry** field (for example, specify `DEPT144.RCHLAND.IBM.COM`)
    b. Specify the Windows domain user account in the **Source user** field (for example, specify `toms`)
    c. Specify the name of the EIM registry representing the IBM i system in the **Registry** field (for example, specify `LP11UT11.RCHLAND.IBM.COM`)
    d. Select **Test**

14. Review the results of the test in the **Mapping found** box of the *Test a Mapping* window
    a. The IBM i user profile is displayed in the **Target user** field (for example, `TSMITH` is displayed)
    b. Other information specifying how the mapping was resolved is displayed in the other fields
15. Select **Close**

5.4 Enable Diagnostic Trace for SPNEGO

The following information describes how to enable diagnostic tracing for SPNEGO in a SPNEGO-enabled WebSphere Application Server profile. Use the WebSphere Integrated Solutions Console to enable diagnostic tracing for SPENGO.

This task assumes the WebSphere Application Server profile was secured using Microsoft Active Directory as a stand-alone LDAP registry.

This task assumes you are logged on to a workstation in the Windows domain using the Windows domain user account specified as the primary administrative user for the WebSphere Application Server profile.

This task assumes the URL for the WebSphere Integrated Solutions Console has been added to the trusted sites if using Internet Explorer.

This task assumes the WebSphere Application Server profile is already running.

WebSphere Integrated Solutions Console URL	https://lp11ut11.rchland.ibm.com:27608/ibm/console/
Application server	iwa70expk

Table 25: Sample values from example environment used in the secure profile task

Enabling diagnostic tracing for SPNEGO in a SPNEGO-enabled WebSphere Application Server profile consists of the following steps:

1. Open a browser window
2. Specify the URL to the WebSphere Integrated Solutions Console for the profile (for example, specify `https://lp11ut11.rchland.ibm.com:27608/ibm/console/`)
3. Accept the site's security certificate if a warning is displayed indicating the certificate cannot be verified or is not trusted.
4. Select **Servers** > **Server Types** > **WebSphere application servers** in the list of tasks (for WAS V6.1, select **Servers** > **Application servers**)
5. Select your application server from the *Application servers* list (for example, select `iwa70expk`)
6. Select **Java and Process Management** > **Process Definition** under *Server Infrastructure*
7. Select **Java Virtual Machine** under *Additional Properties*

8. Select **Custom Properties** under *Additional Properties*
9. Select `com.ibm.security.krb5.Krb5Debug` in the list of properties (if the property does not exist, select **New** to create it)
10. Verify `com.ibm.security.krb5.Krb5Debug` is specified in the **Name** field
11. Specify `all` in the **Value** field
12. Select **OK**
13. Select `com.ibm.security.jgss.debug` in the list of properties (if the property does not exist, select **New** to create it)
14. Verify `com.ibm.security.jgss.debug` is specified in the **Name** field
15. Specify `all` in the **Value** field
16. Select **OK**
17. Select **Save** in the *Messages* box at the top of the page to save the changes
18. Select **Troubleshooting** > **Logs and trace** in the list of tasks
19. Select your application server from the list (for example, select `iwa70expk`)
20. Select **Diagnostic Trace** under *General Properties*
21. Select **Change Log Detail Levels** under *Additional Properties*
22. Select **Components** if it is not already selected
23. Expand *** [All Components]** > **com.ibm.ws.*** (for WAS V6.1, expand **com.ibm.ws.***)
24. Select **com.ibm.ws.security.***
25. Select **All Messages and Traces**
26. Select **OK**
27. Select **Save** in the *Messages* box at the top of the page to save the changes
28. Restart the WebSphere Application Server profile to enable the changes

---

[End of document]