Configuring Integrated Windows Authentication for Oracle WebLogic with SAS® 9.3 Web Applications
Copyright Notice
The correct bibliographic citation for this manual is as follows: SAS Institute Inc.,
*Configuring Integrated Windows Authentication for WebLogic with SAS 9.3 Web Applications*,

*Configuring Integrated Windows Authentication for WebLogic with SAS 9.3 Web Applications*
Copyright © 2012, SAS Institute Inc., Cary, NC, USA.

All rights reserved. Printed in the United States of America. No part of this publication
may be reproduced, stored in a retrieval system, or transmitted, by any form or by any
means, electronic, mechanical, photocopying, or otherwise, without the prior written
permission of the publisher, SAS Institute Inc. Limited permission is granted to store the
copyrighted material in your system and display it on terminals, print only the number
of copies required for use by those persons responsible for installing and supporting the
SAS programming and licensed programs for which this material has been provided,
and to modify the material to meet specific installation requirements. The SAS Institute
copyright notice must appear on all printed versions of this material or extracts thereof
and on the display medium when the material is displayed. Permission is not granted to
reproduce or distribute the material except as stated above.

U.S. Government Restricted Rights Notice. Use, duplication, or disclosure of the
software by the government is subject to restrictions as set forth in FAR 52.227-19
Commercial Computer Software-Restricted Rights (June 1987).

SAS and all other SAS Institute Inc. product or service names are registered trademarks
or trademarks of SAS Institute Inc. in the USA and other countries.

® indicates USA registration.

Other brand and product names are trademarks of their respective companies.
**Table of Contents**

**Integrated Windows Authentication**................................................................. 1

**Overview of Integrated Windows Authentication**.............................................. 1

**Integrated Windows Authentication for WebLogic**.......................................... 1

**Configuration Tasks on the Active Directory Domain Controller**

- **Machine** .............................................................................................................. 2
  - Create a Group in the Microsoft Active Directory .............................................. 2
  - Create a User Account in the Microsoft Active Directory .................................. 2
  - Configure Kerberos SPN for WebLogic Application Server .............................. 3
  - Create the Kerberos Keytab File Used by SPNEGO ........................................... 4

**Configuration Tasks on WebLogic** ................................................................. 5

- Copy the Keytab File to the WebLogic Application Server ................................. 5
- Create the Kerberos Configuration Files ............................................................. 5
- Verify Kerberos Authentication ........................................................................... 5

**Modifying the `webLogicLogin.config` File** ................................................... 6

**Modifying SAS Logon Manager** ...................................................................... 6

**Configuring an Active Directory Authentication Provider for LDAP** ............... 7

- Creating an Identity Asserter for SPNEGO ............................................................ 9
- Updating Start-Up Commands for WebLogic ....................................................... 9
- Restarting the Admin Server and Verifying the Active Directory Users .............. 10
- Reinstalling Node Manager .................................................................................. 10
- Adding Java Options in the WebLogic Administration Console ....................... 11

**Configuring the Client Browser to Use SPNEGO** ......................................... 11

- Configure Local Intranet Domains ...................................................................... 11
- Configure Intranet Authentication ..................................................................... 11
- Verify the Proxy Settings .................................................................................... 11
- Specify Integrated Authentication for Internet Explorer ..................................... 12

**Testing SPNEGO Support from a Domain Client PC** ....................................... 12

**Verifying IWA** ................................................................................................. 12

**Troubleshooting SPNEGO Support** .................................................................. 12

**Recommended Reading** .................................................................................. 13
Integrated Windows Authentication

Overview of Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a Microsoft technology that is used in an intranet environment where users have Windows domain accounts.

The key components of IWA include an Active Directory Controller machine (either Windows 2000 or Windows 2003 server), Kerberos Key Distribution Center (KDC) in a Domain Controller machine, a machine with a client browser, and a Web application server.

When used in conjunction with Kerberos, IWA enables the delegation of security credentials. Kerberos is an industry-standard authentication protocol that is used to verify user or host identity. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to provide their identity, they can also encrypt all of their communications to assure privacy and data integrity.

If Active Directory is installed on a Domain Controller running Windows 2000 Server or Windows Server 2003, and the client browser supports the Kerberos authentication protocol, Kerberos authentication is used. Use of the Kerberos protocol is guided by the following requirements:

- The client must have a direct connection to Active Directory.
- Both the client and the server must have a trusted connection to a Key Distribution Center (KDC) and be Active Directory-compatible.
- Service Principal Names (SPNs) are required for multiple worker processes.

Integrated Windows Authentication for WebLogic

When IWA is configured, HTTP clients use Windows login user name to access SAS Web applications that are deployed in the WebLogic application server without any authentication challenge.

To configure IWA for WebLogic and create a single sign-on for HTTP requests using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO), the following requirements should be met:

- WebLogic Web Application Server 9.2, 10.0, or 10.3
- SAS 9.3 should be installed and configured.
- Web authentication. Complete the configuration of Web authentication. For instructions on configuring Web authentication for WebLogic, see “Configuring WebLogic Server 10.3 for Web Authentication with SAS 9.3 Web Applications”.
- Modifications to Web authentication. Complete the modifications to Web authentication.
• An Active Directory Domain Controller running Windows 2000 Server or higher
• Machine with a client browser. This is a Microsoft Windows 2000 (or higher) domain member that has a browser client and supports the SPNEGO authentication mechanism. Microsoft Internet Explorer Version 7.0 or later qualifies as the client.
• WebLogic should be running and SAS Web applications should be deployed. Users on the active directory must have access to WebLogic.
• The domain controller and the WebLogic application server should have the same local time.
• The clock on all three machines should be synchronized to within five minutes.

Configuration Tasks on the Active Directory Domain Controller Machine
To perform tasks on the Microsoft Active Directory domain controller machine, you should be familiar with Active Directory Users and Computer on a Windows server.
For instructions on how to use the Active Directory Users and Directory, refer to the product’s online Help.
Complete the following tasks on the Microsoft Active Directory domain controller machine.

Create a Group in the Microsoft Active Directory
Create an organizational unit or group for user accounts, for example, SASIWAUsers, in the Active Directory on the Windows server. Active Directory users who will be allowed to access SAS Web applications will require membership in this group. Later in the configuration, it will be mapped to a JAAS authorization role, which, in turn, is used by the Web application server for determining authorization to the SAS Web applications.

Create a User Account in the Microsoft Active Directory
1. (Optional). On the domain controller machine, run the following command to find the principals for all users:
   `dsquery user`
2. Create a user account, for example, iwauser, within the Active Directory Users and Computers window, and add this user account to the group. This user account will eventually be mapped to the Kerberos service principal name (SPN). Make sure that the following options are selected when you create the user: **User cannot change password** and **Password never expires**. Note the password you defined when creating the user account. You will need it later.
3. Configure the new user account to comply with the Kerberos protocol.
   a. Right-click the name of the user account in the Users tree in the left pane and select **Properties**.
   b. In the Properties dialog box for the user, click **Account** tab.
c. Under Account Options, select the following:

**Password never expires**

**Use DES Encryption types for this Account** *(Do NOT select this option if you are running Windows 2008.)*

**Do not require Kerberos preauthentication**

Note that selecting “Do not require Kerberos preauthentication” is optional.

4. Setting the encryption type might corrupt the password. Therefore, reset the user password by right-clicking the name of the user account, selecting **Reset Password**, and re-entering the same password specified earlier.

5. Add the user to the organizational unit or group that you created.

**Configure Kerberos SPN for WebLogic Application Server**

The Microsoft Active Directory provides support for service principal names (SPN), which are a key component in Kerberos authentication. SPNs are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. An SPN usually looks something like name@YOUR.REALM. You need to define an SPN to represent your WebLogic Server in the Kerberos realm. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos authentication is not possible.

1. On the Active Directory Controller, access the command prompt window to use the **setspn** commands.

2. Before executing the **setspn** commands, verify that there are no additional mappings already configured for the users:

   ```shell
   setspn -l HTTP|fully-qualified-host-name
   ```

   No Service Principal Names should be presented.

3. Enter the following commands for SPNs by using correct capitalization of letters and substituting the host name and user name that you created earlier:

   ```shell
   setspn -a HTTP/hostname username
   setspn -a HTTP/fully-qualified-host-name username
   ```

   Here is an example of the use of the **setspn** commands:

   ```shell
   setspn -a HTTP/redwood2.abc.sas.com iwauser
   setspn -a HTTP/redwood2.abc.sas.com iwauser
   ```

4. Run the **setspn** command to view the SPNs you created:

   ```shell
   setspn -l username
   ```
This is an important step. If the same service is linked to different accounts in the Active Directory server, the client will not send a Kerberos ticket to the server.

**Create the Kerberos Keytab File Used by SPNEGO**

A *keytab* is a file containing pairs of Kerberos principals and encrypted keys (these are derived from the Kerberos password). The keytab file contains the requisite information for the WebLogic Server to authenticate to the Key Distribution Center (KDC). Keytab files are copied to the WebLogic Server and must be readable by the user account running the WebLogic Server.

Create the Kerberos keytab file and make it available to the WebLogic application server. Use the `ktpass` command to create a user mapping and the Kerberos keytab file:

```
ktpass -out C:\hostname.host.keytab -mapuser username -crypto DES-CBC-MD5 -princ HTTP/fully-qualified-domain-name@URL address -pass password -ptype KRB5_NT_PRINCIPAL
```

The `ktpass` command creates the `hostname.host.keytab` file. Note that the input for the `-crypto` parameter depends on the type of Windows server used in your environment.

Here is an example of the use of the `ktpass` command and the options which create the `redwood2.host.keytab` file:

```
ktpass -out C:\redwood2.host.keytab -mapuser iwauser -crypto DES-CBC-MD5 -princ HTTP/redwood2.abc.sas.com@abc.sas.com -pass password -ptype KRB5_NT_PRINCIPAL
```

The following table explains the options used with the `ktpass` command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-out</td>
<td>The key is written to this output file.</td>
</tr>
<tr>
<td>-mapuser</td>
<td>The key is mapped to this user.</td>
</tr>
<tr>
<td>-crypto DES-CBC-MD5</td>
<td>This option uses the single DES encryption key.</td>
</tr>
<tr>
<td>-princ</td>
<td>Principal name.</td>
</tr>
<tr>
<td>-pass</td>
<td>This option denotes the password for the user ID.</td>
</tr>
<tr>
<td>-ptype KRB5_NT_PRINCIPAL</td>
<td>This option specifies the KRB5_NT_PRINCIPAL principal value. Specify this option to avoid warning messages.</td>
</tr>
</tbody>
</table>
**Configuration Tasks on WebLogic**

To enable the use of SPNEGO for WebLogic, the Kerberos configuration must be completed. Configuration tasks on WebLogic include copying the keytab file to the appropriate directory, and creating the Kerberos configuration files, `krb5.ini` (on Windows) and `krb5login.conf` (on UNIX).

**Copy the Keytab File to the WebLogic Application Server**

On Windows, copy the Keytab file from the Active Directory Controller machine to this directory: `C:\WINNT\keytab filename` on the WebLogic application server.

**Create the Kerberos Configuration Files**

1. On Windows, create a directory: `C:\WINNT`.
2. Create the `krb5.ini` file and save it in the `C:\WINNT` directory.

   The content in the `krb5.ini` file should resemble the following example:

   ```
   [libdefaults]
   default_realm = ABC.SAS.COM
   default_keytab_name = FILE:c:\keytab\redwood2.host.keytab
   default_tkt_enctypes = des-cbc-md5
   default_tgs_enctypes = des-cbc-md5
   kdc_default_options = 0x54800000
   ticket_lifetime = 600
   
   [realms]
   ABC.SAS.COM = {
   kdc = redwood1.abc.sas.com:88
   admin_server= redwood1.abc.sas.com
   default_domain = abc.sas.com
   }
   
   [domain_realm]
   abc.sas.com = ABC.SAS.COM
   abc.sas.com = ABC.SAS.COM
   
   [appdefaults]
   autologin = true
   forward = true
   forwardable= true
   encrypt = true
   ```

   Substitute your hostname for the `default_keytab_name` command. Make sure that the value specified for the `default_tkt_enctypes` variable matches the value specified for `-crypto` option in the `ktpass` command that you used on the Active Controller Directory machine.

**Verify Kerberos Authentication**

A Ticket Granting Ticket (TGT) could expire or get lost from the cache. To ensure that a valid TGT is available in the system, use the `kinit` command. The `kinit` command obtains and caches the Kerberos ticket-granting tickets.
1. Bring up a command prompt window, and go to the Java directory where the kinit utility resides (for example, C:\jdk1.5.0.19\bin directory).

2. On Windows, run the kinit utility to make a Kerberos request. Substitute the name of the keytab filename, URL address, and domain name:

```bash
ekinit -k -t C:\krb5.keytab\redwood2.host.keytab
HTTP/redwood2.abc.sas.com@abc.sas.com
```

It is important that the following message displays at the end of the output:

“New ticket is stored in cache file C:\Documents and settings…”

### Modifying the webLogicLogin.config File

Update the `weblogicLogin.config` file with the Java Authentication and Authorization Service (JAAS) configuration that applies to the keytab file. On Windows, this file is located in the `SAS-configuration-directory\Lev1\Web\Common\SASDomain` directory.

For WebLogic 10.3, here is an example of the content in the `weblogicLogin.config` file:

```xml
com.sun.security.jgss.initiate
{
    com.sun.security.auth.module.Krb5LoginModule required
    principal="HTTP/redwood2.abc.sas.com@abc.sas.com" useKeyTab=true
    keyTab="C:\\keytab\\redwood2.host.keytab" storeKey=true debug=true;
};
com.sun.security.jgss.accept
{
    com.sun.security.auth.module.Krb5LoginModule required
    principal="HTTP/redwood2.abc.sas.com@abc.sas.com" useKeyTab=true
    keyTab="C:\\keytab\\redwood2.host.keytab" storeKey=true debug=true;
};
```

For WebLogic 10.x, the contents of the `weblogicLogin.config` file require a minor modification. Here is an example of the syntax in a `weblogicLogin.config` file for WebLogic 10.x, with the modifications shown in bold:

```xml
com.sun.security.jgss.krb5.initiate
{
    com.sun.security.auth.module.Krb5LoginModule required
    principal="HTTP/redwood2.abc.sas.com@abc.sas.com" useKeyTab=true
    keyTab="C:\\keytab\\redwood2.host.keytab" storeKey=true debug=true;
};
com.sun.security.jgss.krb5.accept
{
    com.sun.security.auth.module.Krb5LoginModule required
    principal="HTTP/redwood2.abc.sas.com@abc.sas.com" useKeyTab=true
    keyTab="C:\\keytab\\redwood2.host.keytab" storeKey=true debug=true;
};
```

### Modifying SAS Logon Manager

Edit the `web.xml` file and the `weblogic.xml` files. Both files are located in the WEB-INF application directory. For instructions on extracting and editing these files and redeploying
SAS Logon Manager, see “Configuring WebLogic Server 10.3 for Web Authentication with SAS 9.3 Web Applications.”

The file contents of the web.xml file and the weblogic.xml file should resemble the following examples. In order for Weblogic to perform the SPNEGO identity assertion that is required for Integrated Windows authentication, the auth-method parameter in the web.xml file MUST have a value of CLIENT-CERT.

Example of the web.xml file with CLIENT-CERT specified for the auth-method parameter:

```xml
<security-constraint>
<web-resource-collection>
<web-resource-name>All resources</web-resource-name>
<url-pattern>/</url-pattern>
</web-resource-collection>
<auth-constraint>
<role-name>SASWebUser</role-name>
</auth-constraint>
</security-constraint>

<login-config>
<auth-method>CLIENT-CERT</auth-method>
<realm-name>myrealm</realm-name>
</login-config>

<security-role>
<role-name>webuserRole</role-name>
</security-role>
```

Example of the weblogic.xml file with group (in this example, the group is SASIWAUsers) specified for the principal-name parameter:

```xml
<?xml version='1.0' encoding='UTF-8'?>
<session-descriptor>
<cookie-name>SASLogon.sessionID</cookie-name>
<url-rewriting-enabled>false</url-rewriting-enabled>
</session-descriptor>
<context-root>SASLogon</context-root>
<security-role-assignment>
<role-name>webuserRole</role-name>
<principal-name>SASIWAUsers</principal-name>
</security-role-assignment>
<weblogic-web-app>
```

Note that the SASIWAUsers group was previously created in the Microsoft Active Directory, and in this example, is being mapped to the JAAS authorization role webuserRole.

**Configuring an Active Directory Authentication Provider for LDAP**

Configure the WebLogic Authentication Provider. For instructions, see “Configuring WebLogic Server 10.3 for Web Authentication with SAS 9.3 Web Applications.” Then configure the Active Directory Authentication Provider for LDAP. This Authentication Provider is used primarily to facilitate JAAS role authorization based on group membership...
in an Active Directory. It ensures that access to the Web applications is limited to users within a certain Active Directory group or groups, if desired. This Authentication Provider can be omitted if the preference is to use SAS metadata group membership for this purpose instead, via the SAS TrustedAuthenticator Authentication Provider.

To configure an Active Directory Authentication provider for LDAP, follow these steps:

1. Log into the WebLogic Server Administration Console.
2. In the Domain Structure panel, click Security Realms.
3. Click myrealm.
4. In the Change Center panel, click Lock & Edit.
5. In the Settings for myrealm panel, select the Providers tab.
6. In the Authentication Providers panel, click New.
7. In the Create a New Authentication Provider panel, specify the name of the Authentication Provider (for example, Active Directory Authenticator) and select Active Directory Authenticator from the choices for Type.
8. In the Configuration tab for the active directory authenticator, select Optional from the choices available for Control Flag.
9. Click Provider Specific.
10. In the Provider Specific panel, specify the values for the following fields:
    - Group Base DN:
    - User Name Attribute:
    - Host:
    - User Base DN:
    - Principal:
    - Credential:

Following is an example of values that were entered:

- **Group Base DN**: cn=Users, dc=abc, dc=sas, dc=com
- **User Name Attribute**: cn
- **Host**: redwood1.abc.sas.com
- **User Base DN**: cn=Users, dc=abc,dc=sas, dc=com
- **Principal**: ABC\admin
- **Credential**: password

Your Active Directory configuration will determine the type of entry specified in the User Name Attribute field. The following example illustrates different entries for the User Name Attribute and User From Name Filter fields. In this example, the user’s login id is used instead of the displayed name.

- **Group Base DN**: cn=Users, dc=abc, dc=sas, dc=com
- **User Name Attribute**: sAMAccountName
Host: redwood1.abc.sas.com  
User Name Filter: (&(sAMAccountName=%u)(objectclass=user))  
User Base DN: cn=Users, dc=abc,dc=sas, dc=com  
Principal: ABC\admin  
Credential: password  

11. Click Save and Activate Changes.

Creating an Identity Asserter for SPNEGO  
To enable WebLogic to use SPNEGO for identity assertion, follow these steps to create an additional provider for SPNEGO:

1. Log into the WebLogic Server Administration Console.  
2. In the Domain Structure panel, click Security Realms.  
3. Click myrealm.  
4. In the Change Center panel, click Lock & Edit.  
5. In the Settings for myrealm panel, click the Providers tab.  
6. In the Authentication Providers panel, click New.  
7. In the Create a New Authentication Provider panel, specify the name of the Authentication Provider (for example, NegotiateIdentityAsserter) and select NegotiateIdentity Asserter from the choices for Type. Click OK.  
8. Click on NegotiateIdentity Asserter.  
10. Click Save.  
11. Click Activate Changes.  
12. On the Providers tab, in the Authentication Providers panel, click Reorder.  
13. Reorder the authentication providers so they display in this order:  
   NegotiateIdentityAsserter  
   DefaultIdentityAsserter  
   DefaultAuthenticator  
   ActiveDirectoryAuthenticator  
   SASTrustedAuthenticator

The recommended settings are as follows for the applicable providers given that they are configured in the recommended order as well:

DefaultAuthenticator: SUFFICIENT  
ActiveDirectoryAuthenticator: REQUISITE  
SASTrustedAuthenticator: OPTIONAL
For more information, see the topic “Using Other Authentication Providers” in “Configuring WebLogic Server 10.3 for Web Authentication with SAS 9.3 Web Applications.”

14. Click OK to save the list of reordered authentication providers.

15. Click Activate Changes.

**Updating Start-Up Commands for WebLogic**

Shut down the Admin Server. Add the SPNEGO configuration for WebLogic by editing the `commEnvSAS.cmd` file:

**Windows:** `C:\SAS-configuration-directory\Lev1\Web\SASDomain\bin\commEnvSAS.cmd`

The content of the `commEnvSAS.cmd` file should resemble the following example:

```bash
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Djava.security.krb5.realm=abc.sas.com
-Djava.security.krb5.kdc=redwood1.abc.sas.com
-Djava.security.auth.login.config="SAS-configuration-directory\Lev1\Web\Common\SASDomain\weblogicLogin.config"
-Djavax.security.auth.useSubjectCredsOnly=false
-Dweblogic.security.enableNegotiate=true
-Dweblogic.Stdout.DEBUGEnabled=true
-Dweblogic.StdoutSeverityLevel=64
-Dsun.security.krb5.debug=true
```

Note that there must be quotes around the path and filename.

**Restarting the Admin Server and Verifying the Active Directory Users**

Restart the WebLogic Admin Server to enable the configuration changes to go into effect. To confirm that the configuration changes went into effect, verify that the users in the Active Directory are displayed. Follow these steps to verify that the Active Directory users recognized by the ActiveDirectoryAuthenticator display in WebLogic:

1. Log into the WebLogic Server Administration Console.
2. In the **Domain Structure** panel, click **Security Realms**.
3. Click **myrealm**.
4. In the **Change Center** panel, click **Lock & Edit**.
5. In the **Settings for myrealm** panel, click the **Users and Groups** tab.
6. In the **Users** panel, verify that the ActiveDirectoryAuthenticator has populated the list of users with the Active Directory users.

**Reinstalling Node Manager**

If the node manager is installed as a Windows service, then uninstall it, reinstall it, and restart it. For more information, see the instructions for the `commEnvSAS.cmd` in “Configuring WebLogic Server 10.3 for Web Authentication with SAS 9.3 Web Applications.”
Adding Java Options in the WebLogic Administration Console
Add the Java options for each SAS server definition in the WebLogic Administration Console:

1. Log into the WebLogic Server Administration Console.
2. In the Domain Structure panel, click Environment.
3. Click Servers.
4. In the Servers panel, click SASServer1.
5. In the Settings for SASServer 1 panel, click Server Start.
6. Click Lock & Edit.
7. In the Arguments field, add the following Java options by substituting the values shown in this example:
   -Djava.security.krb5.realm=abc.sas.com
   -Djava.security.krb5.kdc=redwood1.abc.sas.com
   -Djavax.security.auth.useSubjectCredsOnly=false
   -Dweblogic.security.enableNegotiate=true

Configuring the Client Browser to Use SPNEGO
Complete the following steps on the machine with the client browser application to ensure that your Microsoft Internet Explorer browser is enabled to perform SPNEGO authentication.

Configure Local Intranet Domains
1. In the Internet Explorer window, select Tools ► Internet Options ► Security.
2. Under Local Intranet, click Sites.
3. Verify that the checkboxes are selected for the following options:
   - Include all local (Intranet) sites not listed in other zones
   - Include all sites that bypass the proxy server
4. Add your domain name to the list of Web sites to ensure that Internet Explorer recognizes any site with your domain name as the intranet.

Configure Intranet Authentication
1. In the Internet Explorer window, select Tools ► Internet Options ► Security.
2. Under Local Intranet, click Sites.
3. On the Security tab, select Local Intranet and click Custom Level.
4. In the Security Settings – Local Intranet Zone, under User Authentication, select Automatic Logon only in Intranet Zone and click OK.

Verify the Proxy Settings
1. In the Internet Explorer window, select Tools ► Internet Options ► Connections.
2. Click LAN Settings.
3. Verify that the proxy server address and port number are correct.
4. Click Advanced.
5. In the Proxy Settings dialog box, ensure that all desired domain names are entered in the Exceptions field.
6. Click OK to close the Proxy Settings dialog box.

**Specify Integrated Authentication for Internet Explorer**

1. On the Internet Options window, click the Advanced tab and scroll to Security settings. Verify that the checkbox is selected for Enable Integrated Windows Authentication.
2. Click OK. Restart your Microsoft Internet Explorer to activate this configuration.

**Testing SPNEGO Support from a Domain Client PC**

SPNEGO testing can be done with the sec_con tool, if it is available on the WebLogic machine. You can access the sec_con tool from a domain client PC by specifying the URL address in the browser application. To obtain the sec_con tool along with customized instructions, contact SAS Technical Support.

Following is an example of a URL address used to access the sec_con tool:

http://redwood2.abc.sas.com:7501/sec_con/sec_con_03wls.jsp

**Verifying IWA**

Log on to SAS Web applications to confirm that no prompt is presented for logon credentials, and that the applications load with the current Windows user logged into the application.

Do NOT test from a browser on the middle-tier machine itself (that is, the machine where the application server is installed). This will not work. Testing must be performed on a separate client machine within the Windows domain.

**Troubleshooting SPNEGO Support**

To troubleshoot SPNEGO support within WebLogic, you can add command-line arguments to the server startup and produce DEBUG logs for the Kerberos process. When you complete troubleshooting, these debug logs should disabled. To enable the DEBUG logs, add the following start-up arguments in the WebLogic Administration Console:

-Dsun.security.krb5.debug=true
-Dweblogic.StdoutDebugEnabled=true

These arguments produce server logs that you can review for troubleshooting purposes.
Recommended Reading


SAS is the world leader in providing software and services that enable customers to transform data from all areas of their business into intelligence. SAS solutions help organizations make better, more informed decisions and maximize customer, supplier, and organizational relationships. For more than 30 years, SAS has been giving customers around the world The Power to Know®. Visit us at www.sas.com.