Single Sign-On Using SPNEGO

Introduction

As of Percussion CM Server version 7.0.2, build 201106R01, patch level RX-17069, Windows Single Sign-On (SSO) using SPNEGO is now supported. Through the SSO feature, a user who logs in to Windows through a domain is automatically authenticated into the Percussion CM System Content Explorer without having to enter a user name and password.

NOTE: Once the feature is turned on, a user cannot logout and login to the same system as a different user. Instead the user must log out of Windows and login as a different user.

You implement Single Sign-On in Windows environments using Simple and Protected GSS-API Negotiation (SPNEGO). Windows Single Sign-On automatically logs in users to the Percussion CM Server using their Windows network login when they connect from a Windows client with one of these supported browsers:

- Internet Explorer Version 7, Version 8, or Version 9
- Firefox Version 3.6 or Version 4.0

The client must run on one of these supported Windows client operating systems:

- Windows XP
- Windows Vista
- Windows 7

Both the CM Server and the client must be in the same Windows domain since Windows Single Sign-On is only supported for one Windows domain. The Percussion CM Server must also be running on either Windows 2003 Server or Windows 2008 Server.

IMPORTANT: You must add domain users (or user's group) to their Roles in the CM Server Administrator. Windows Single Sign-On does not include a Role provider. If you do not add users (or user's group) to their Roles in the CM Server Administrator, the users cannot login through Single Sign-On. They must login through other security providers that are configured in the CM Server, such as the backend security provider. SSO is only supported through a web browser. SSO will not work for the Percussion Developer tools or WebDAV.

Assumptions

You must have Percussion CM Server version 7.0.2, build 201106R01, patch level RX-17069 or newer installed to take advantage of Windows Single Sign-On using SPNEGO. You already have Active Directory Users or Groups assigned to their appropriate Percussion CM System Role(s). You can find all of the necessary steps in Chapter 6, Maintaining Users, of the Rhythmyx Administration Manual.

Steps to Implement Windows Single Sign-On Using SPNEGO

NOTE: Make sure that your CM System environment is not running before you perform any steps below.

Step 1: Create the Keytab

1. Create a new Active Directory domain user for creating the keytab. Make sure this is a new user (for example, spnego_user) and not an existing user account.
2. Next log into a Windows machine on your domain as the Domain Administrator. Enter the following command at a command prompt:

```
ktpass /out http-web.keytab /mapuser <username@DOMAIN> /princ HTTP/<machine-
name.domain@DOMAIN> /pass *
```

   For example, where
   - <username> is the new user you just created:

```
spnego_user@PERCUSSION.LOCAL
```

   - <machine-name.domain@DOMAIN> is the machine that will be running CM System:

```
ts-win2008.percussion.local@PERCUSSION.LOCAL
```

   the command line is

```
ktpass /out http-web.keytab /mapuser spnego_user@PERCUSSION.LOCAL /princ HTTP/ts-
win2008.percussion.local@PERCUSSION.LOCAL /pass *
```

   The system prompts you for the newly created domain user's password, as in the following example:

```
Targeting domain controller: uranus.percussion.local
Using legacy password setting method
Successfully mapped HTTP/ts-win2008.percussion.local to spnego_user.
Type the password for HTTP/ts-win2008.percussion.local:
Type the password again to confirm:
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to http-web.keytab:
Keytab version: 0x502
keysize 82 HTTP/ts-win2008.percussion.local@PERCUSSION.LOCAL ptype 0
(KRB5_NT_UNKNOWN) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x7e631beb505ed4dbdb49bbf41b5ec8e4)
```

   Enter the password twice. Upon successfully entering the password twice, the keytab file, http-web.keytab, should be in your current working directory.

   NOTE: Once you create the keytab file, you will not be able to login to a Windows client machine on the domain with the newly created username (for example, spnego_user). This is not an issue because keytab enables running CM System with any other domain user. If you reset the password for the username, you must recreate the keytab (which, in effect, resets the password).
3. Confirm that the command entered above to ktpass also made your new user a Service Principal Name (SPN):
   As Domain Administrator, enter the following at a command prompt:

```
setspn -L <username> (for example, setspn -L spnego_user)
```

You should see the following ouput:

```
Registered ServicePrincipalNames for CN=SPNEGO
USER,CN=Users,DC=percussion,DC=local:

    HTTP/ts-win2008.percussion.local
```

Step 2: Enable the SPNEGO (Kerberos) Configuration File on the CM Server

A sample SPNEGO (Kerberos) configuration file is installed on the CM Server in the directory CMSystem-Home-Directory/rxconfig/Server, named krb5.conf.sample.
To enable this file:

1. Make a copy of the file, then rename the copied file krb5.conf (in other words, remove the .sample extension from the copied file.)
2. Modify the krb5.conf file by substituting these values in the sample text:
    1. The name of the Windows domain and realm that includes your CM Server and clients.
    2. The fully-qualified hostname of the domain controller for the domain and realm that includes your CM Server and clients.

    For example, if your domain is named percussion.local, and the domain controller is named ts-win2008, change the values to **PERCUSSION.LOCAL** and **ts-win2008.percussion.local** in the text as follows:
    krb5.conf:

```
[libdefaults]
        default_realm = [__PERCUSSION.LOCAL__]
        default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes256-cts aes128-cts rc4-
hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
        default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes256-cts aes128-cts rc4-
hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
        permitted_enctypes   = aes256-cts-hmac-sha1-96 aes256-cts aes128-cts rc4-
hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
        __PERCUSSION.LOCAL__  = {
                kdc = __ts-win2008.percussion.local__
                default_domain = __PERCUSSION.LOCAL__
}

[domain_r]
        __.PERCUSSION.LOCAL = PERCUSSION.LOCAL__
```

Step 3: Edit the login-conf.xml File

1. Copy the `http-web.keytab` file that you created in Step 1 to `CMSystem-Home-Directory\AppServer\server\rx\conf\`.
2. Edit the `CMSystem-Home-Directory\AppServer\server\rx\conf\login-conf.xml` file as follows:
    Depending on the version of CM System that you're working with, your `login-conf.xml` file will be a little different. For version 7.0.2, the `spnego-server` application policy node will look as follows:

```
<!-- Kerberos/Spnego SSO configuration
<application-policy name="spnego-server">
        <authentication>
```

```
                <login-module code="com.sun.security.auth.module.Krb5LoginModule"
flag="required">
                        <module-option name="storeKey">true</module-option>
                        <module-option name="isInitiator">false</module-option>
                </login-module>
        </authentication>
</application-policy>
-->
```

For version 7.0.3 or newer the `spnego-server` application policy node will look as follows:

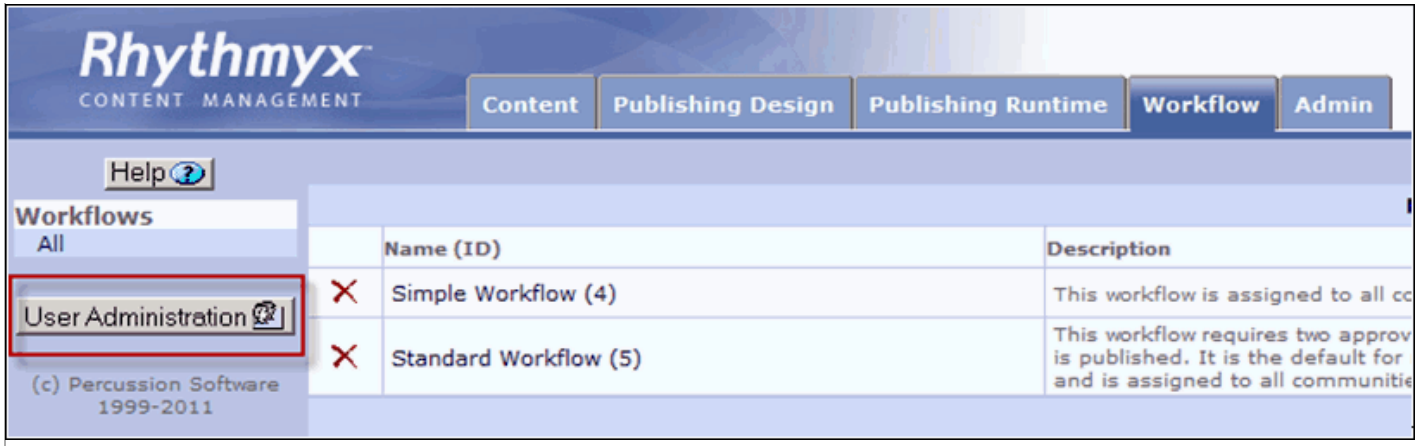
```
<!-- Kerberos/Spnego SSO configuration
<application-policy name="spnego-server">
        <authentication>
                <login-module code="com.sun.security.auth.module.Krb5LoginModule"
flag="required">
                        <module-option name="storeKey">true</module-option>
                        <module-option name="isInitiator">false</module-option>
                        <module-option name="useKeyTab">true</module-option>
                        <module-option name="keyTab">file://CMSystem-Home-
Directory/AppServer/server/rx/conf/http-web.keytab</module-option>
                        <module-option name="principal">HTTP/ts-
win2008.percussion.local</module-option>
                </login-module>
        </authentication>
</application-policy>
-->
```

If you're on CM Server version 7.0.2, build 201106R01, patch level RX-17069, you can replace the entire `spnego-server` application policy node in your `login-conf.xml` file with the above example for version 7.0.3, or you can add the three `module-option` nodes for `useKeyTab`, `keyTab` and `principal`. Either way you will need to make sure that the new `module-option` nodes are accurate for your environment.

NOTE: You must replace the principal module option with the `HTTP/<fully-qualified host name>` in lower case. You must also update the `keyTab` location from `file://CMSystem-Home-Directory/AppServer/server/rx/conf/http-web.keytab` to the correct file path to your `keytab` file.

Step 4: Add a SPNEGO Security Provider to the CM Server

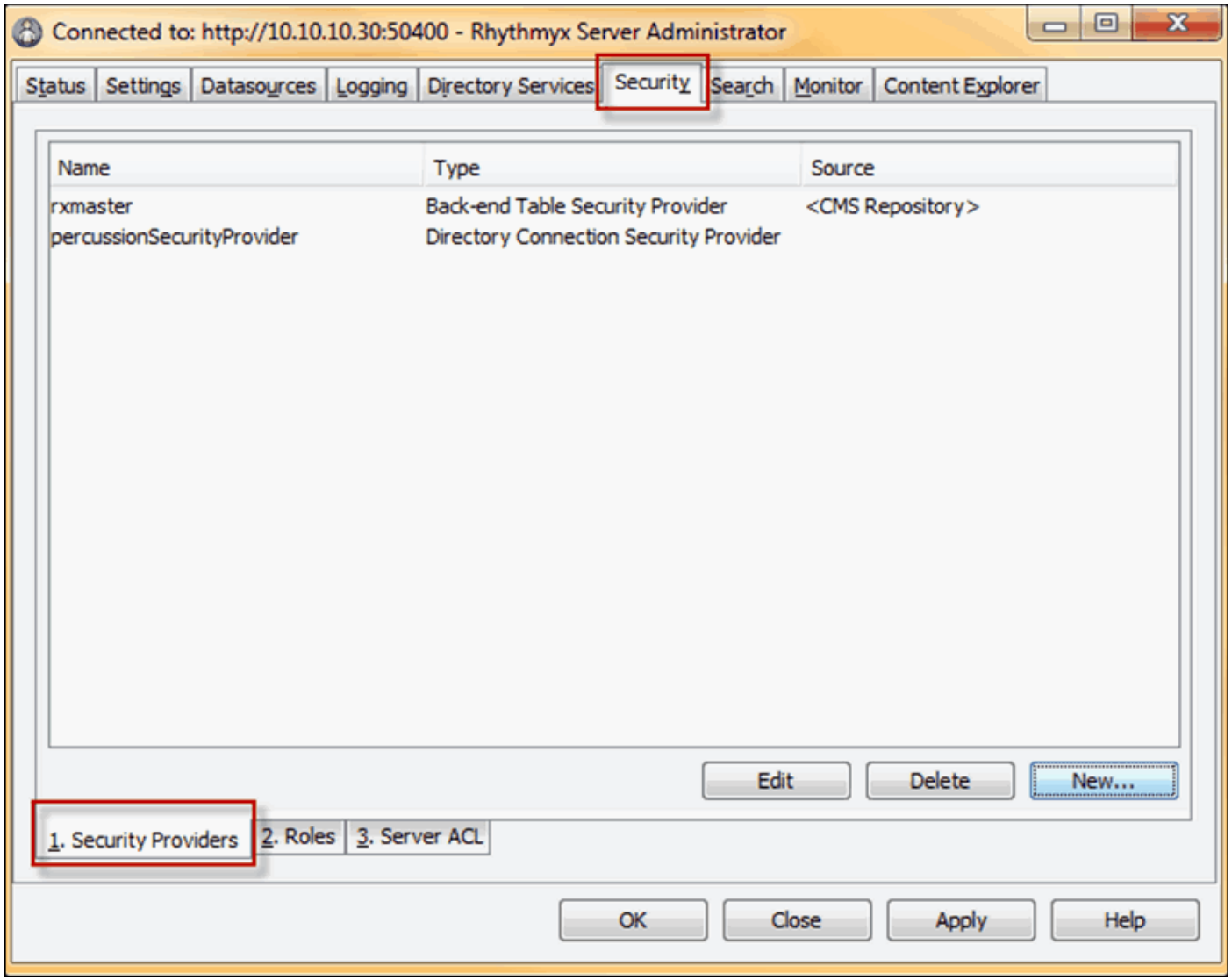
NOTE: If you are using *Percussion CM Server version 7.0.2, build 201106R01, patch level RX-17069*, you should click **User Administration** on the Workflow tab to launch the Rhythmyx Server Administrator as a Java Applet in your browser. This is necessary because patch RX-17069 will only affect the Server Administrator that's on the CM Server.



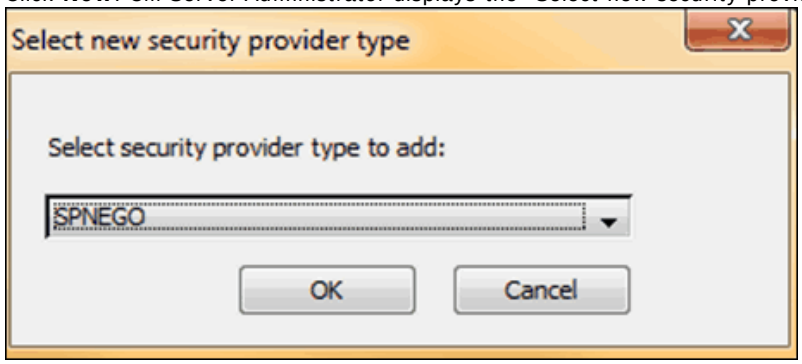
If you want to run the Server Administrator locally from you local Developer Tools, you must patch your local Developer Tools with patch RX-17069 before performing the following steps.

To add a SPNEGO security provider:

1. Login the Rhythmyx Server Administrator as either a backend or some other already established Admin user.
2. Click the Security tab at the top of the dialog, then click the Security Providers tab at the bottom.

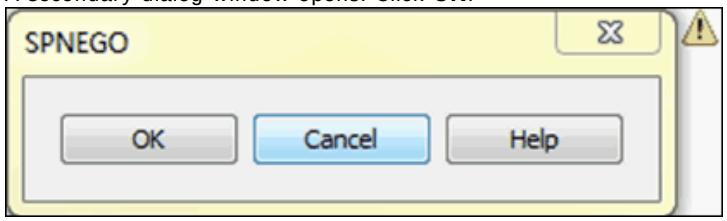


3. Click **New**. CM Server Administrator displays the “Select new security provider type” dialog.



4. In the **Select security provider type to add** drop list, choose SPNEGO. Click **OK**.

5. A secondary dialog window opens. Click **OK**.



6. Click **Apply** to save the security provider.
7. Fully reboot the computer where CM System is located. Also reboot any machines that will be connecting to CM System. Perform these reboots so that the client machines accept the new security ticket.
8. Restart CM System with any username except the SPN username (the keytab performs pre-authentication).

Step 5: Configure Clients for Windows Single Sign-On

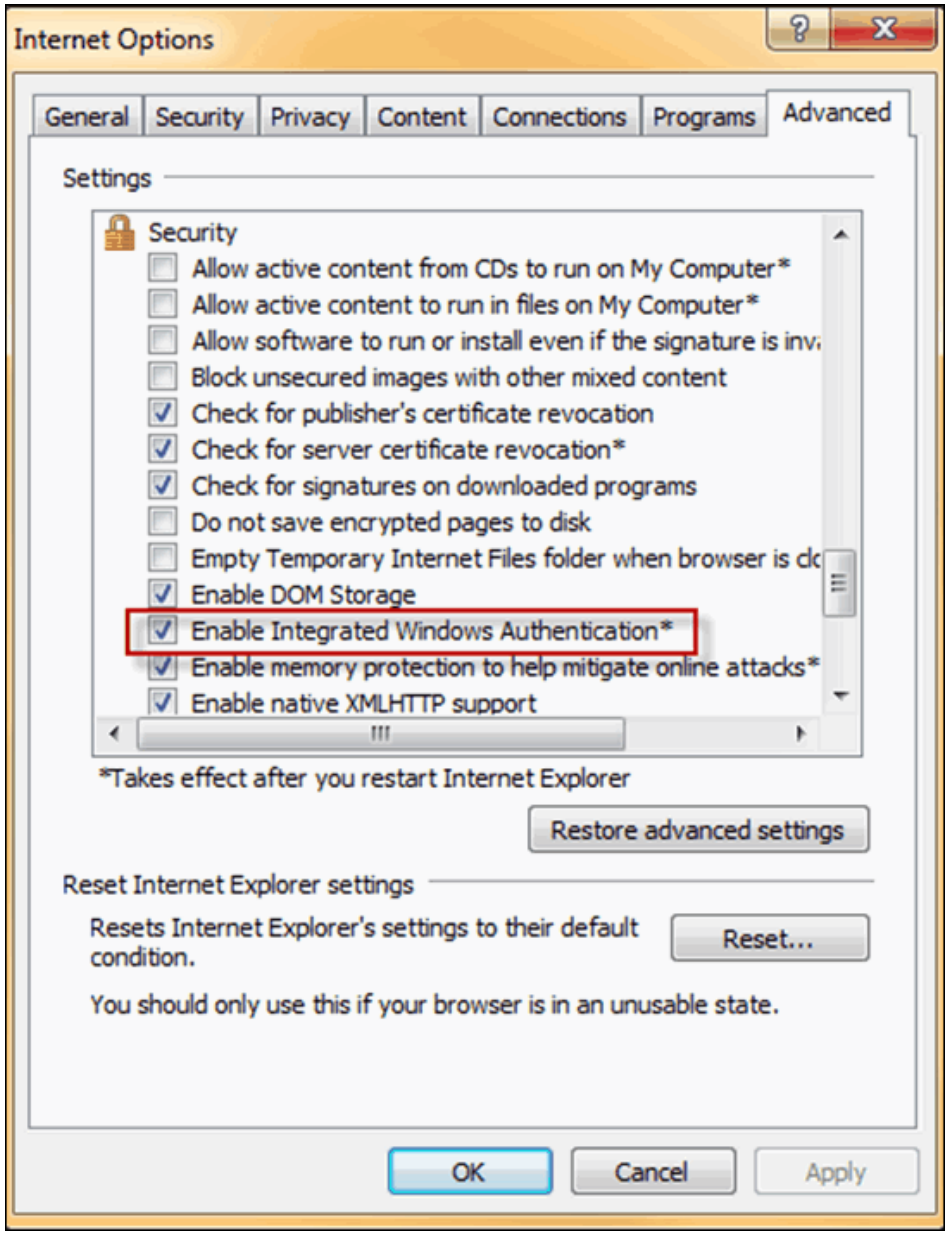
Single Sign-On is supported in the following browsers on Windows clients:

- Internet Explorer Version 7, Version 8, or Version 9
- Firefox Version 3.6 or Version 4.0

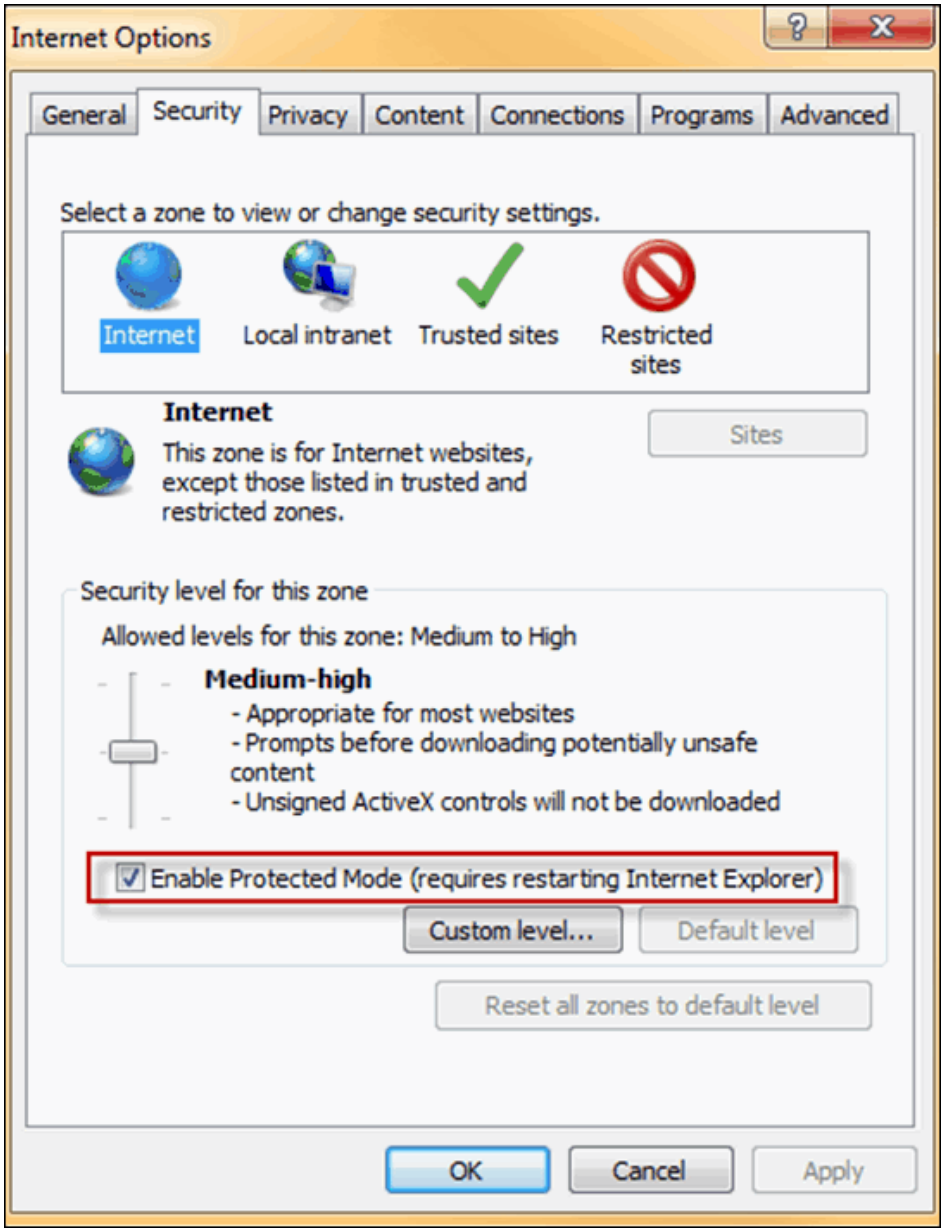
Configuring Internet Explorer to Support Windows Single Sign-On

Since the default configuration for Internet Explorer supports Windows Single Sign-On, you can ignore this section if you have not altered the default configuration. Otherwise, perform the following steps to configure Internet Explorer to support Single Sign-On:

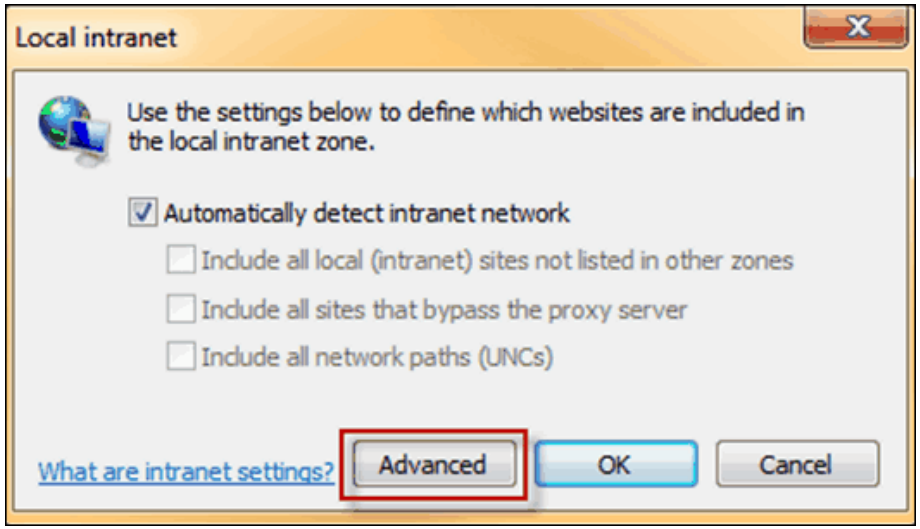
1. Under the Tools menu, open Internet Options.
2. On the Advanced tab, under Security, check **Enable Integrated Windows Authentication**.



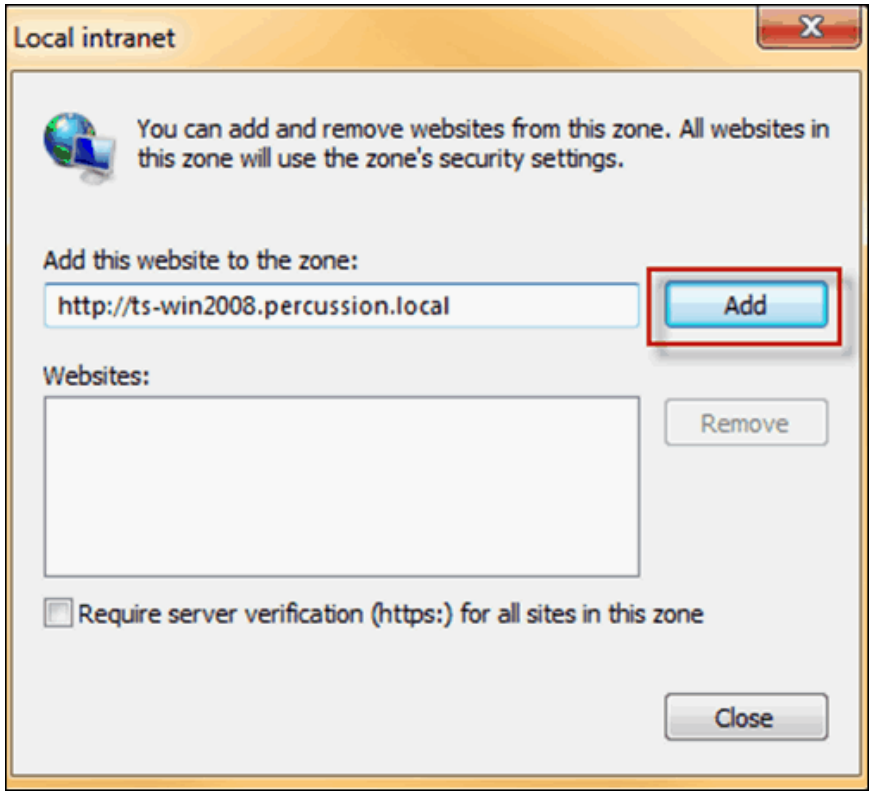
3. On the Security tab, check **Enable Protected Mode**.



4. Perform the following substeps if you need to access the server using a fully qualified name of the machine, where the name is appended with the domain name (for example, `http://ts-win2008.percussion.local`). Otherwise, proceed to Step 5.
    1. On the Security tab, check the **Local intranet** icon.
    2. Click the **Sites** button to display the **Local intranet** dialog box.
    3. Click the **Advanced** button.



4. At **Add this website to the zone**, enter the host name (for example, `http://ts-win2008.percussion.local`).
5. Click **Add** to add the URL to the **Websites**: list.



6. Click **Close**.
5. Click **OK** on all open dialog boxes to save your changes.
6. Restart Internet Explorer.

Configuring Firefox to Support Windows Single Sign-On

To configure Firefox to support Single Sign-On, add the Windows domain to the network.negotiate-auth.trusted.uris property:

1. In the Firefox address field, enter *about:config*. Read the pop-up message and click **I'll be careful...**. Firefox displays the *about:config* page with a list of configurable preferences.
2. Right-click on the `network.negotiate-auth.trusted.uris` property and from the popup menu, choose *Modify*. Firefox displays the Enter String Value dialog.
3. Enter the name of the Windows domain and hostname. For example, `.percussion.local,ts-win2008`
4. Click **OK** to save the new configuration.

Step 6: Test the Windows Single Sign-On Implementation

To test the implementation, login to a Windows client on the domain of the CM Server as a user in a CM System Role. Start a browser configured to support Single Sign-On and connect to the CM Server. You should be logged in automatically; the browser will take you to Content Explorer.

Troubleshooting

You cannot have multiple users mapped to the same machine. If you do, authentication will fail, so you must delete the old mappings. In the following steps, replace `machine-name.domain.name` with your fully-qualified machine name. Replace `username` with the user you would like to use for SPN. It's important to note that for keytab, the user will no longer be able to log in with their password once a keytab is generated, so do not use a normal username.
Perform the following steps to delete all old SPN Registrations before configuring keytab:

1. As Domain Administrator, enter the following at a command prompt to see if the user is mapped. Perform this step for any user that you suspect is mapped:

   ```
   setspn -L <username>
   ```

   Example Output:

   ```
   HTTP/<machine-name.domain.name>
   HTTP/<machine-name>
   ```

2. As Domain Administrator, delete the old mappings by entering the following at a command prompt:

   ```
   setspn -D HTTP/<machine-name.domain.name> <username>
   setspn -D HTTP/<machine-name> <username>
   ```

   Make sure no other users are mapped to the machine.

Questions?

Refer to information about contacting Percussion at the following URL:
http://www.percussion.com/about/company-information/contact/