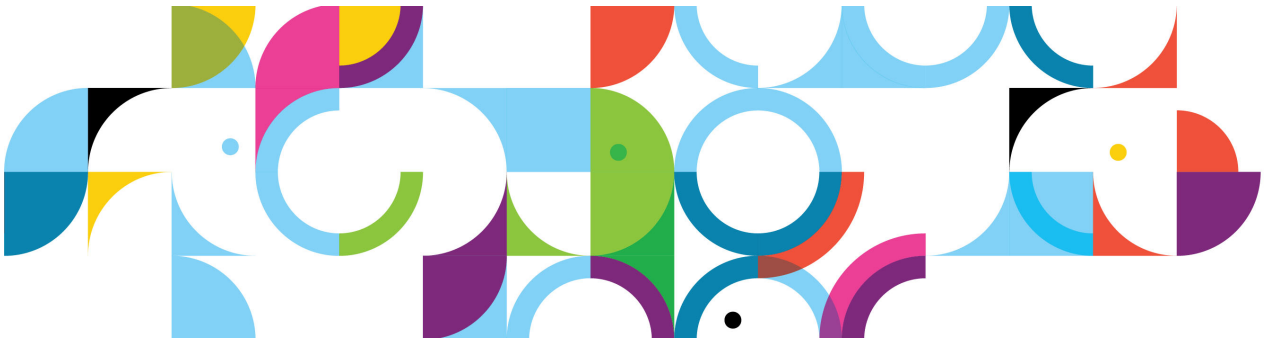

IBM Connections 4.5 Deployment Scenarios

Deployment Scenarios

ERC 1.0

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

Cognos®	DB2 Universal Database™	DB2®
Domino®	FileNet®	Lotus Notes®
Lotus®	Notes®	Rational®
Tivoli®	WebSphere®	

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

June 2013 edition

Enabling single sign-on for Tivoli Access Manager with SPNEGO

About the author

Tracy Green has worked for IBM, initially with Lotus for 17 years. She has been an Advisory Software Engineer with the Dublin System Verification Test team for the last eight years, and has worked on a range of IBM products, most recently IBM Connections. Tracy can be reached at `tracy_green@ie.ibm.com`.

Contents

Environment description

- The test environment that is described in this article is a 2-Node Medium Cluster running on Windows Server 2008 R2 Enterprise 64-bit edition that uses Microsoft SQL Server 2008 R2 database back end and Microsoft Active Directory 2008 LDAP repository.
- This article describes how to enable single sign-on for Tivoli Access Manager with SPNEGO after the IBM Connections 4.5 cluster is successfully deployed and configured.
- The Windows Domain is `.LITBG02.SWG.USMA.IBM.COM.`.

Host name	Function	RAM	Disk space
dmgrHTTPsrv	WebSphere DMGR+HTTP	8 GB 2 CPU	60 GB
wasNode1srv	WebSphere Application Server Node1	8 GB 2 CPU	60 GB
wasNode2srv	WebSphere Application Server Node2	8 GB 2 CPU	60 GB
sqlTDIsrv	SQLServer + Tivoli Directory Integrator	8 GB 2 CPU	60 GB

Host name	Function	Branch	# Users
LDAPsrv	LDAP repository	OU=SharedLDAP,OU=Lotus,OU=Software Group,DC=litbg02,DC=swg,DC=usma,DC=ibm,DC=com	300k

Host name	Function	Version
webSealsrv	WebSEAL Server	06/01/01

Connections 4.5 is fully deployed and users can log on from the remote HTTP Server host name, for example, `https://dmgrHTTPsrv.mycompany.com/homepage`.

The WebSEAL server can be accessed from `https://webSealsrv.mycompany.com`.

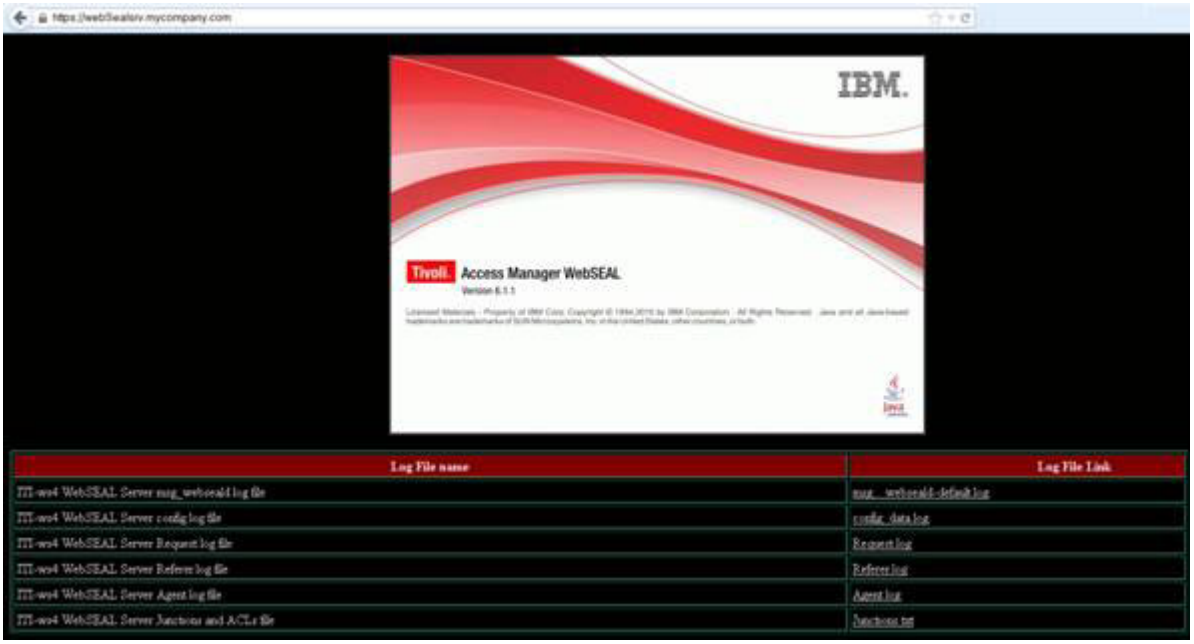

Figure 1. Tivoli Access Manager WebSEAL

After you complete the steps to enable single sign-on, you then access the Connections cluster from the WebSEAL host name, for example:

`https://webSealsrv.mycompany.com/homepage.`

Enabling single sign-on for Tivoli Access Manager with SPNEGO

Information

Refer to the IBM Connections information center for full instructions on how to apply any required changes to Tivoli Access Manager for Connections 4.5:

- Enabling single sign-on for Tivoli Access Manager, `http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_Tivoli_Access_Manager_ic45&content=pdcontent`

  Most of the previous configuration is also required when enabling single sign-on for Tivoli Access Manager with SPNEGO, except where otherwise noted. The steps for updating interService URLs, adding a Tivoli Allow Access to the Embedded Experience gadget and adding a Tivoli Access Manager authenticator property can be omitted in an SPNEGO environment.

Refer to the following information center topic for instructions on how to enable SPNEGO for WebSEAL:

- Enabling single sign-on for Tivoli Access Manager with SPNEGO, `http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_Tivoli_Access_Manager_with_SPNEGO_ic45&content=pdcontent`

  This article outlines the configuration changes required to the Connections Cluster.

WebSphere security changes

Verifying ConnectionsAdmin

__ 1. Log in to WebSphere Admin Console and go to **Security > Bus Security**.

__ 2. Click **ConnectionsBus** and select **Security > Users and groups in the bus connector role**. Ensure that your ConnectionsAdmin is listed.

Figure 2. WebSphere Admin Console

This is the user that is specified during the Connections installation and must exist in your LDAP repository.

Changing default realm

__ 1. Change the default realm name in the Federated Repositories section of the Deployment Manager to match the value of the LDAP name, including the port number (for example, `ldap.mycompany.com:389`).

__ 2. From WebSphere administration console, go to **Security > Global Security**.

__ 3. Click **Configure** beside Federated Repositories. Change the realm name to be the host name of your LDAP repository.

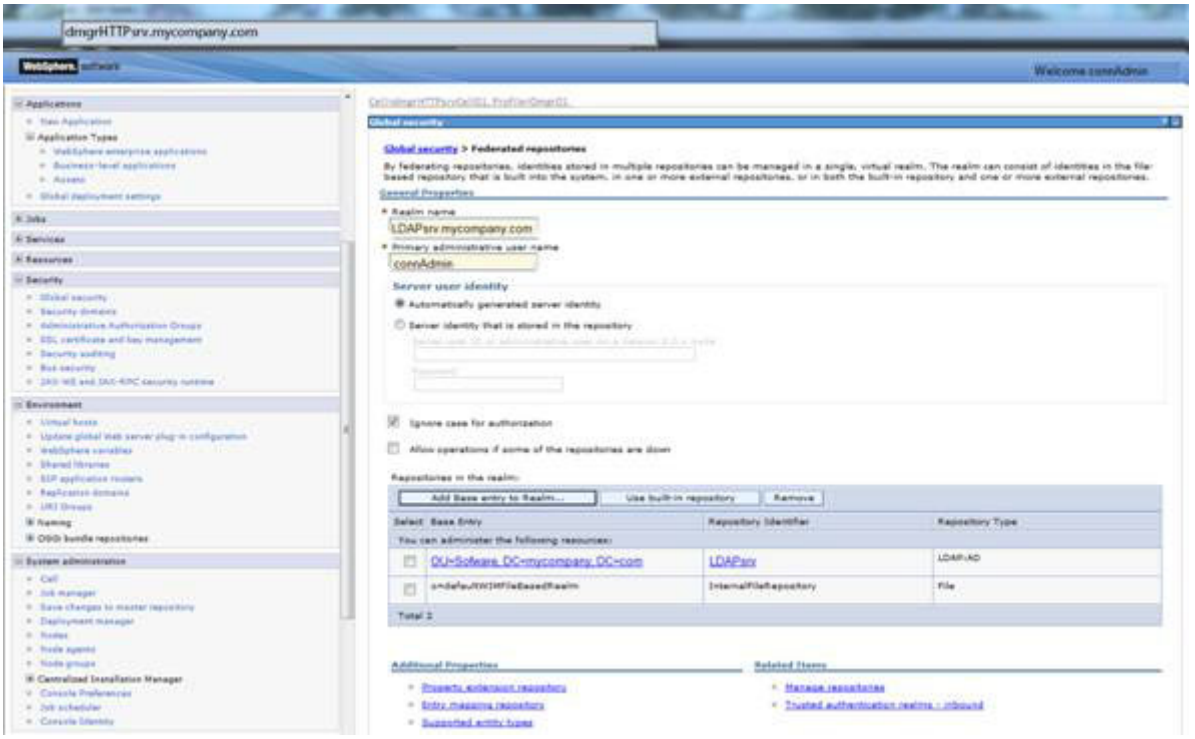

Figure 3. WebSphere Administration Console - Global Security

Setting the single sign-on domain name to match the Tivoli Access Manager server domain name

__ 1. From the WebSphere Administration Console, go to **Security > Global Security > Web and SIP security > Single sign-on (SSO)**.

__ 2. Ensure that the following check boxes are selected:

- Enabled
- Interoperability mode
- Web inbound security attribute propagation
- Set security cookies to HTTPOnly to help prevent cross-site scripting attacks

__ 3. Set the domain name, for example, `mycompany.com`, and click **Apply**, **OK**, and **Save**.

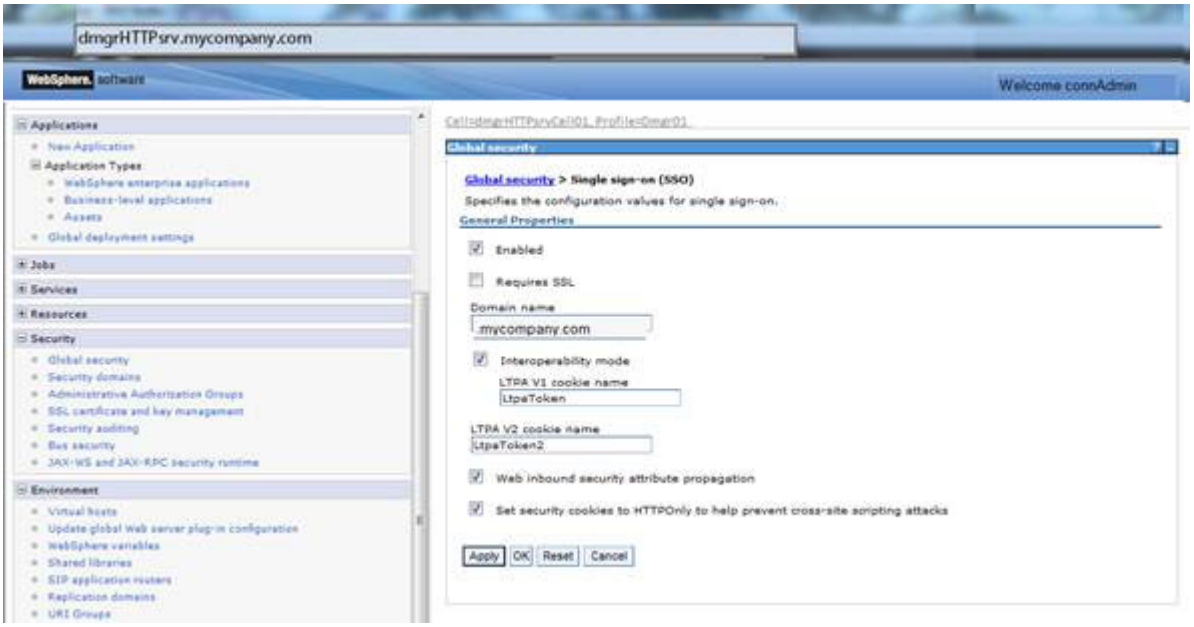

Figure 4. WebSphere Admin Console - Global Security - Web and SIP security - Single sign-on (SSO)

__ 4. You must now go to **Security > Global Security > Web Security - General Settings**.

__ 5. Click **Authenticate only when the URI is protected** and select **Use available authentication data when an unprotected URI is accessed**.

__ 6. Click **OK** and save the changes.

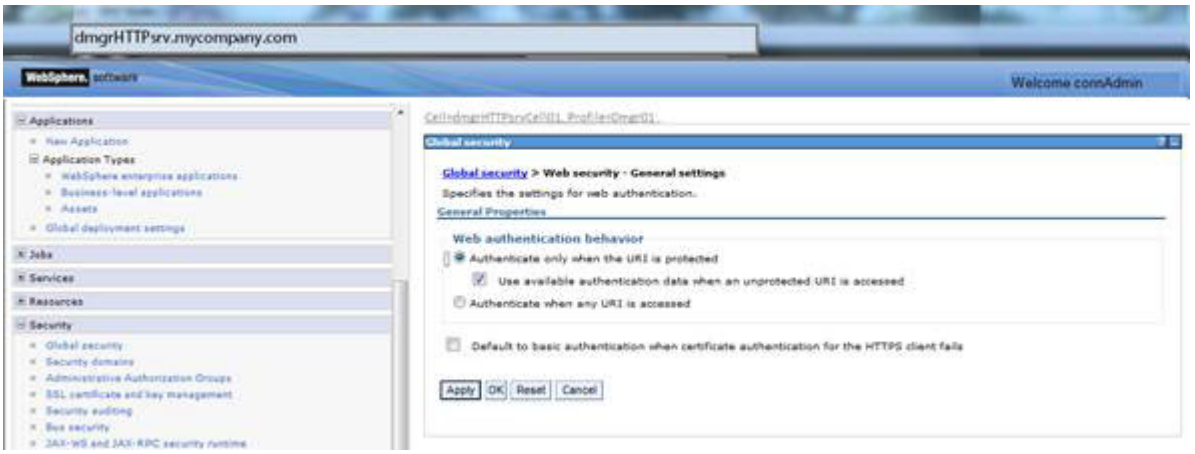

Figure 5. WebSphere Admin Console - Global Security - Web Security - General Settings

Extracting the LTPA token

__ 1. From the WebSphere administration console, go to **Security > Global Security** and click the **LTPA** link.

__ 2. Go to the **Cross-cell single sign-on** section and enter a password for your LTPA key and set the path and key file name.

__ 3. Then, click **Export**, followed by **Apply**, **OK**, and **Save**.

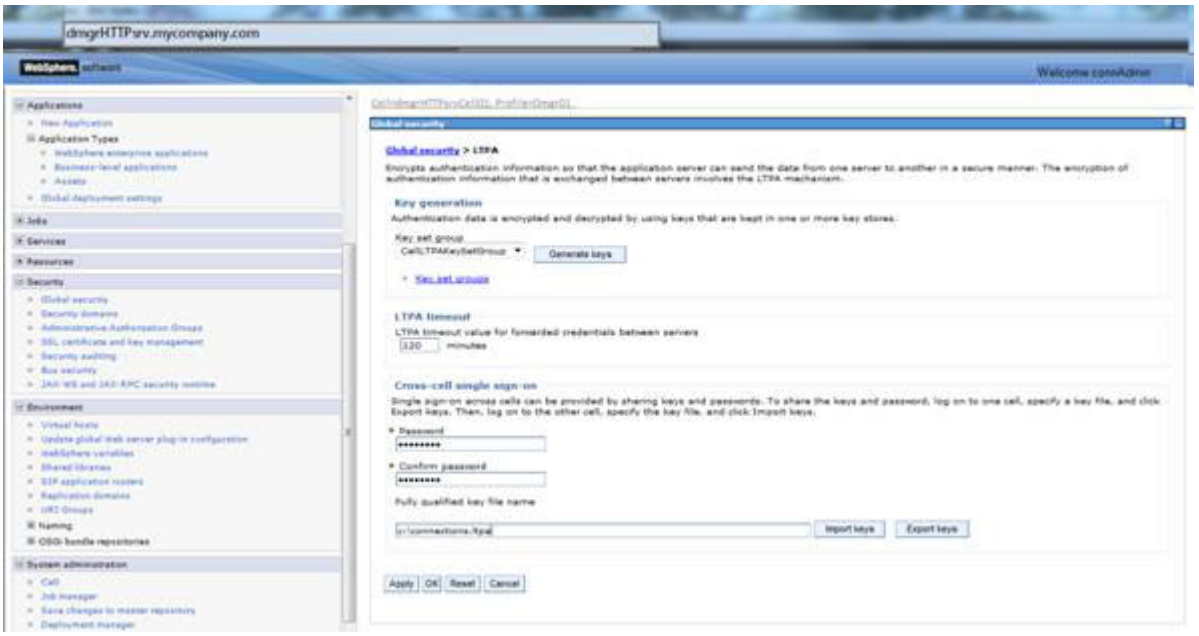

Figure 6. WebSphere Admin Console - Security - Global Security - LTPA

The LTPA key is used for configuring the transparent path junctions in Tivoli Access Manager as described in the information center.

Extracting the IBM HTTP Server SSL certificate

__ 1. From the HTTP server, choose **IBM HTTP Server v8.0 > Start Key Management Utility** from the Start menu.

__ 2. Select **Key Database File > Open**.

__ 3. Open the `plugin-key.kdb`, which contains the IBM HTTP Server WebSphere Application Server keys and extracts the Personal Certificate.

Note

The default password, if not changed, is `WebAS`.

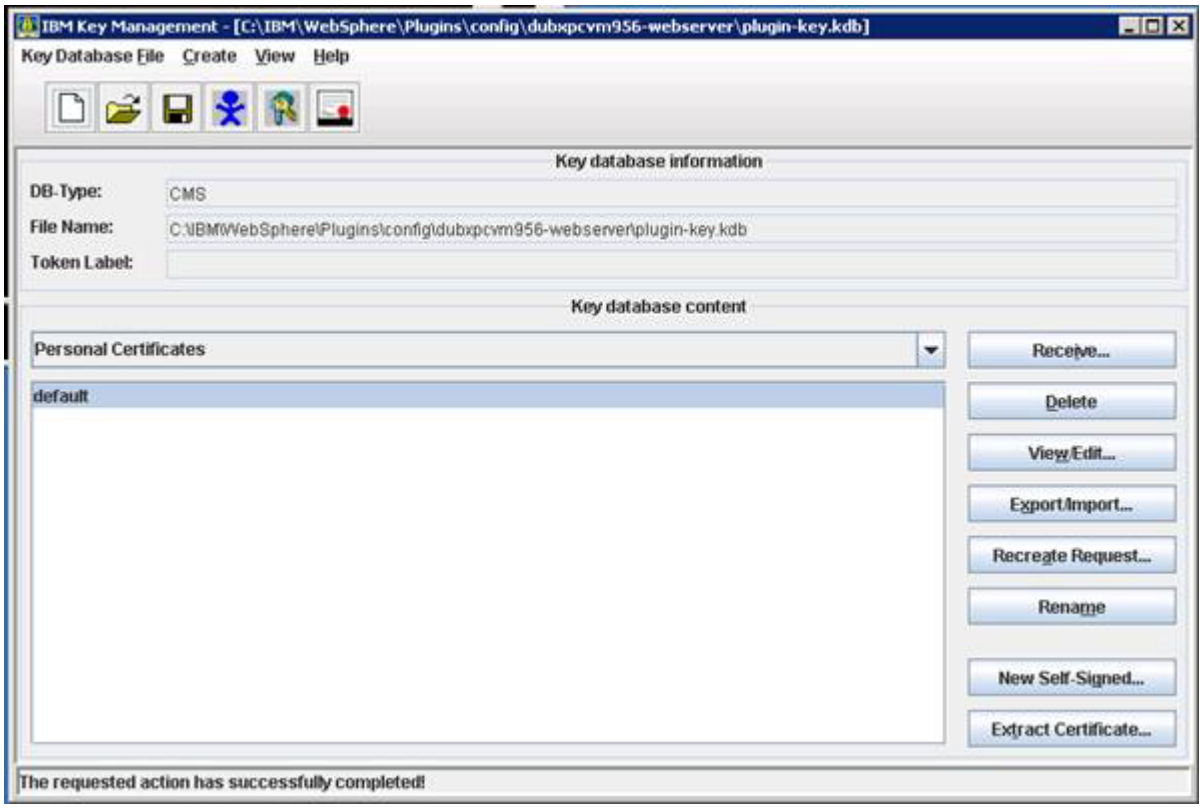

Figure 7. IBM Key Management

__ 4. Click **Extract Certificate** and provide a path and name for the extracted file, leaving the `.arm` extension, and click **OK**.

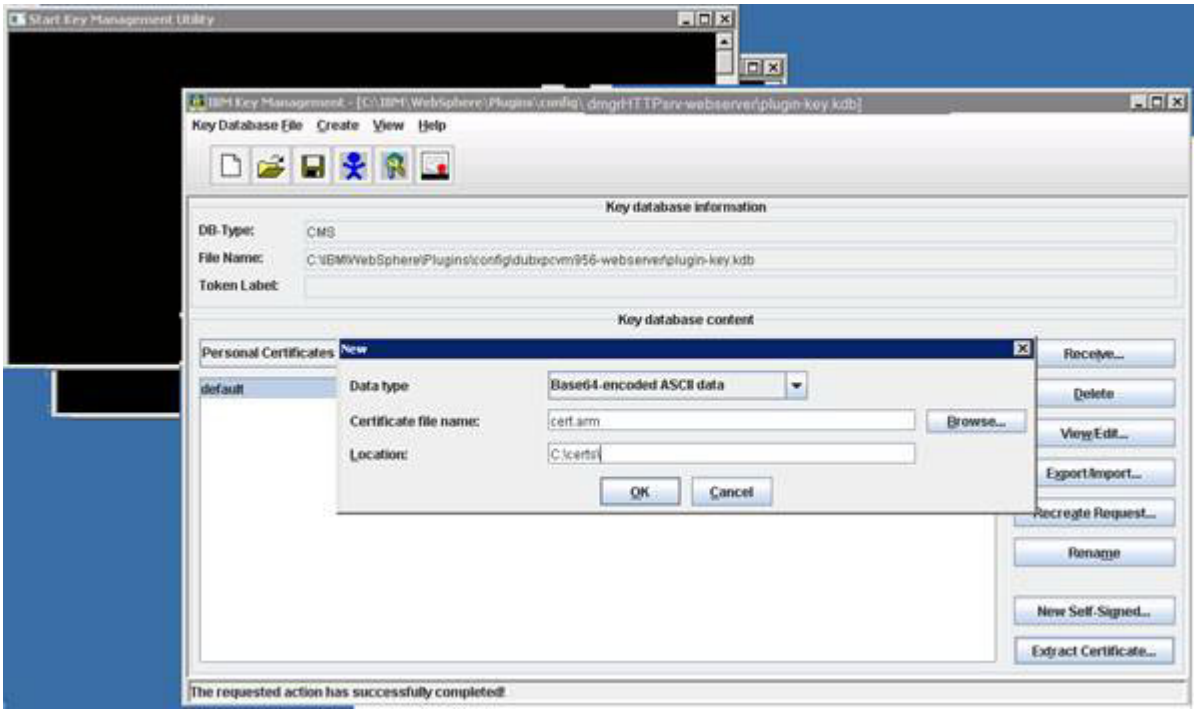

Figure 8. Start Key Management Utility

The SSL certificate is copied to the WebSEAL server when applying the Connections changes to Tivoli Access Manager as described in the information center.

Information

Review the information center to complete the Tivoli Access Manager configuration:

- Enabling single sign-on for Tivoli Access Manager, `http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_Tivoli_Access_Manager_ic45&content=pdcontent`
- Enabling single sign-on for Tivoli Access Manager with SPNEGO, `https://idoc2.swg.usma.ibm.com/connections/topic/com.ibm.lotus.connections.doc/secure/t_secure_with_tam-spnego.html`

Configuring the LotusConnections-config.xml

__ 1. On your Deployment Manager computer where Connections is installed, go to:

`C:\WebSphere\AppServer\profiles\Dmgr01\config\cells\dmgrHTTPsrvCell01\LotusConnections-config`

__ 2. Back up the `LotusConnections-config.xml` file and move the backup to another location, because leaving multiple versions of the `.xml` files in the `LotusConnections-config` folder causes functional problems.

__ 3. Now, edit `LotusConnections-config.xml` with a text editor and scroll to the bottom of the file. Locate `dynamicHosts` and set it to "Enabled" and set the `href` and `ssl-href` values to the host name of your WebSEAL server, for example, `webSealsrv.mycompany.com`.

```
350    <languageSelector cookieDomain="" cookieName="" defaultLanguage="" enabled="false" usePermanentCookie="false">
351        <language lang="en">English</language>                                    <!--English-->
352        <language lang="zh">\u4e2d\u6587 (\u200f\u7b80\u4f53)</language>          <!--Chinese, Simplified-->
353        <language lang="fr">Fran\u00e7ais</language>                              <!--French-->
354        <language lang="ar">\u200f\u0627\u0644\u0639\u0631\u0628\u064a\u0629\u200f</language>  <!--Arabic-->
355    </languageSelector>
356
357    <!-- Search settings -->
358    <languageSensitive enabled="false"/>
359    <ignorePunctuation enabled="false"/>
360    <transactionSetting>
361        <attribute key="Transaction_Max" value="20"/>
362        <attribute key="Queue_Max" value="10"/>
363    </transactionSetting>
364    <seedlistSettings allowUnsecuredTransfer="false">
365        <attribute key="maximumPageSize" value="1000"/>
366        <attribute key="maximumIncrementalQuerySpanInDays" value="30"/>
367    </seedlistSettings>
368
369    <useRichTextEditorInBookmarklet enabled="false"/>
370
371    <!-- Support for 1 to 2 mapping. This is a search config setting that controls composition of unicode characters
372         from decomposed forms like the base character and its accents or other modifiers. -->
373    <oneToTwoMapping enabled="false"/>
374
375    <dynamicHosts enabled="true">
376        <host href="http://webSealsrv.mycompany.com" ssl_href="https://webSealsrv.mycompany.com"/>
377    </dynamicHosts>
378
379    <resources>
380    </resources>
381
382    <sessionCookies>
383        <cookieName key="JSESSIONID"/>
384    </sessionCookies>
385
386    <versionStamp value="20130306.234007"/>
387 </config>
```

Figure 9. Editing LotusConnections-config.xml

__ 4. Save the file and restart your cluster. Stop all application servers and all nodes, and then restart the deployment manager, all the nodes, and all the application servers.

Configuring HTTP server for logout

Optional

This section is optional.

Determine how you want the system to behave when users log out of IBM Connections. In an SPNEGO environment when users click **Log out**, they are not logged out of IBM Connections. However, you can redirect the user by using the IBM HTTP Server HTTP configuration file, at `C:\IBM\HTTPServer\conf`.

__ 1. Back up and then edit `httpd.conf`.

__ 2. Uncomment the line that contains `LoadModule rewrite_module modules/mod_rewrite.so` if not already done, so that the rewrite module is enabled.

__ 3. To capture requests to `/ibm_security_logout` and redirect them to `/pkmslogout`, add the following rewrite rules to the http and https sections of the file:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
   RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
```

The following example illustrates how it would look in the `httpd.conf` file after the changes are implemented:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName dmgr.mycompany.com
```

__ 4. Uncomment the line that contains `LoadModule rewrite_module modules/mod_rewrite.so` if not already done, so that the rewrite module is enabled:

```
SSLEnable
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "C:\IBM\HTTPServer\Keys\webserver-key.kdb"
   SSLStashFile "C:\IBM\HTTPServer\Keys\webserver-key.sth"
```

__ 5. Save and close the `httpd.conf` file.

__ 6. Restart IBM HTTP Server.

Accessing IBM Connections within the SPNEGO domain

You now access IBM Connections from the WebSEAL server host name.

__ 1. From a client computer within the SPNEGO domain, in this case .MYCOMPANY.COM, open the following URL from your web browser: `https://webSealsrv.mycompany.com/homepage`

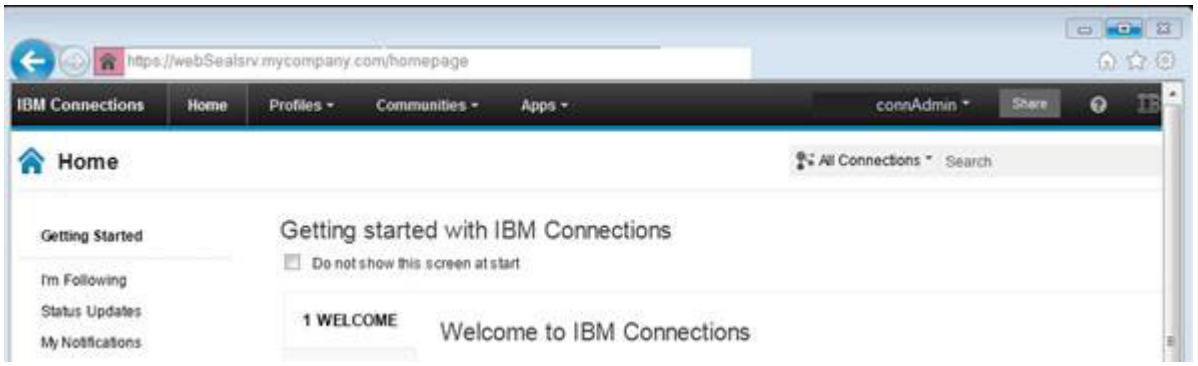

Figure 10. IBM Connections - home page

The authenticated windows user is automatically logged in to Connections.

You must ensure that your web browser includes the WebSEAL server as a trusted host to work properly.

Example for Internet Explorer:

a. Select **Tools > Internet Options**.

b. Click the **Security** tab and select **Local intranet**.

c. Click **Advanced** and add the WebSEAL host name to “Add this website to the zone” and click **Add**.

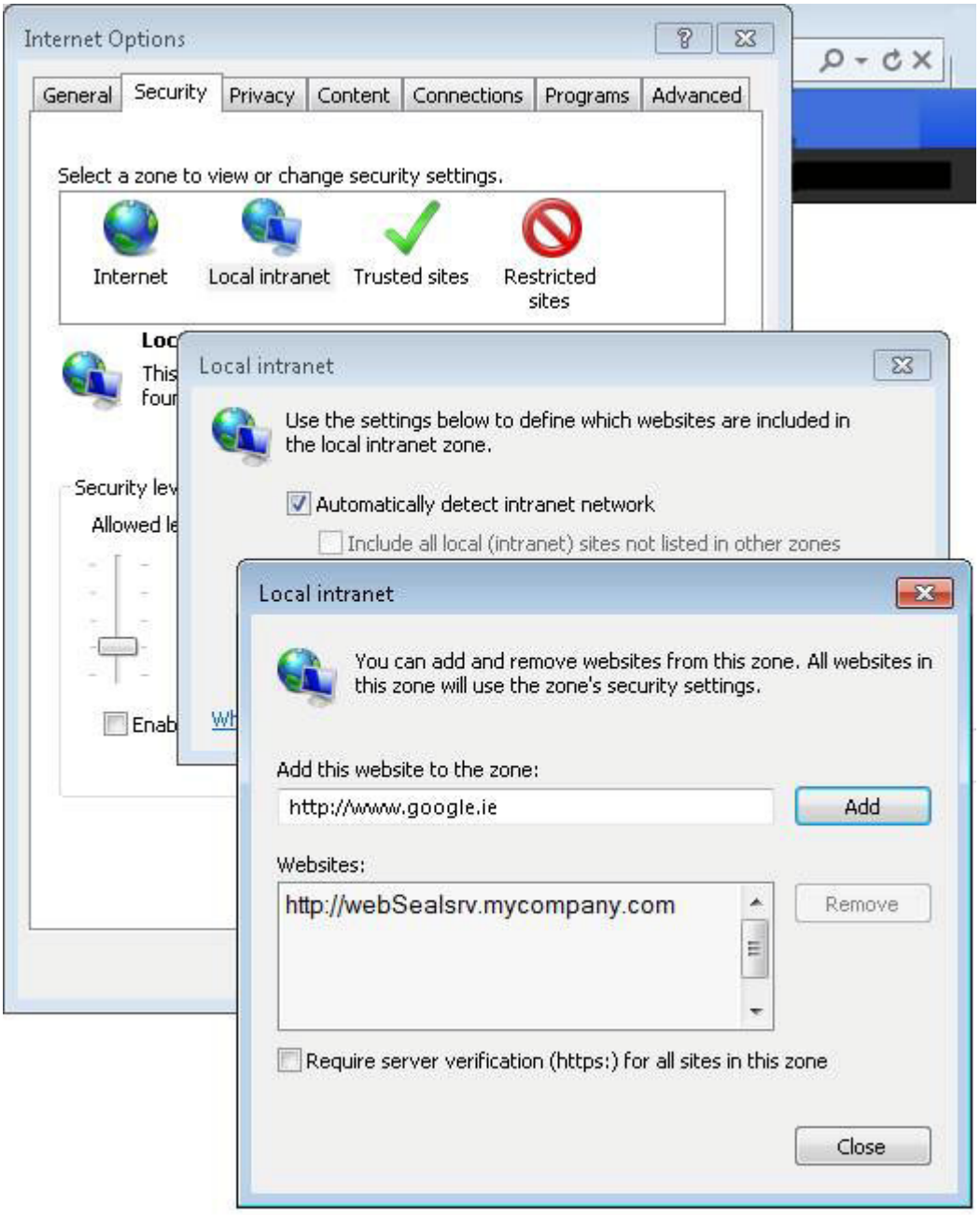

Figure 11. Adding a website to a zone by using Internet Explorer

