IBM Connections V4.5: How to configure IBM Tivoli Access Manager (TAM) V6.1.1.

Before you begin

- Install IBM Tivoli Access Manager (TAM) for e-business, version 6.1.1.
- Ensure that you can access the installed IBM Connections applications from a web browser.
- Set the IBM WebSphere® Application Server single sign-on domain to the same value as that of the Tivoli Access Manager server.

Notes:

- If you are enabling SSO between IBM Connections and a product that is deployed with a stand-alone LDAP configuration on WebSphere Application Server, or if the product is using IBM Lotus® Domino®, you must first complete the steps described in the Enabling SSO with stand-alone LDAP topic.
- The connectionsAdmin J2C alias that you specified during installation must correspond to a valid account that can authenticate with Tivoli Access Manager. It may map to a back-end administrative user account but is not intended to be used as a user account for IBM Connections. This account must be capable of authenticating for single sign-on against Tivoli Access Manager. If you need to update the userid or credentials for this alias, see the Changing references to administrative credentials topic
- IBM Connections supports the WebSphere cookie-based lightweight third-party authentication (LTPA) mechanism as an SSO solution for Tivoli Access Manager. IBM Connections does not support other SSO solutions that WebSEAL supports such as WebSphere Trust Association Interceptor (TAI), Forms SSO, Cross-domain SSO, or E-community SSO.
- IBM Connections supports the use of SSL Transparent Path junctions with Tivoli Access Manager. IBM Connections does not support TCP type junctions or Tivoli Access Manager Standard junctions.
- For more information about IBM Tivoli Access Manager, go to the Tivoli Access Manager information center.

About this task

Single sign-on (SSO) enables users to log in to one application of IBM Connections and switch to other applications and resources without having to authenticate again.

There are several different ways to configure SSO. This procedure describes one approach. It uses a WebSphere Application Server LTPA key and WebSEAL Transparent Junctions. To set up SSO using Tivoli Access Manager, complete the following steps:

Procedure

Refer to this topic in the information center: Enabling single sign-on for Tivoli Access Manager

- **Steps 1 to 14** should be carried out by the TAM administrator and is beyond the scope of this document.
- **Steps 15** onwards are specific to the IBM Connections administrator and are covered here.

Once the TAM administrator has created the TAM junctions and completed the configuration steps we can now begin to configure Connections and the HTTP Server for TAM integration.

Step 15: Update the values for the dynamicHosts and interService URL attributes in the LotusConnections-config.xml configuration file:

a. Check out the **LotusConnections-config.xml** and using a text editor make the following changes:

b. Find the dynamicHosts element and set the enabled flag to **true**.

c. Set the dynamicHost href and ssl_href to that of the TAM servers hostname e.g.

```
<dynamicHosts enabled="true">
   <host href="http://tamserver.mycompany.com" ssl_href="https://tamserver.mycompany.com"/>
</dynamicHosts>
```

d. Update the interservice URLs for **all** applications with the TAM server hostname. For example the entry for dogear becomes:

```
<sloc:href>
    <sloc:hrefPathPrefix>/dogear</sloc:hrefPathPrefix>
    <sloc:static href="http://dmgr.mycompnay.com" ssl_href="https://dmgr.mycompnay.com"/>
    <sloc:interService href="https://tamserver.mycompany.com"/>
</sloc:href>
</sloc:serviceReference>
```

e. Save the file and check it back in**.**

Step 16: Configure the HTTP server for TAM

To correctly configure the web server to handle the user clicking the log out button in a TAM environment some changes are required to the **httpd.conf** to implement this post log out behaviour. This ensures the user is correctly and securely logged out. Open this file in a text editor and add the following rules:

a. Un-comment the line containing "LoadModule rewrite_module modules/mod_rewrite.so" if not already done so, so that the rewrite module is enabled.

b. 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]
```

c. The following example illustrates how this 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
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"
```

17. Add an ErrorDocument 500 statement to the httpd.conf file. This statement appears in the user's browser if an IBM Connections application becomes unavailable.

18. Save and close the *httpd.conf* file.

19. Restart IBM HTTP Server.

20/21/22. (Do not complete this step for Tivoli Access Manager with SPNEGO) Add a Tivoli Access Manager authenticator property by editing the **LotusConnections-config.xml** file.

a. Find the default **customAuthenticator** setting and change it as follows:

```
<customAuthenticator name="DefaultAuthenticator"/>
```

to:

```
<customAuthenticator name="TAMAuthenticator">
  <attribute key="CookieTimeout" value="10" />
</customAuthenticator>
```

Note: also add the attribute “CookieTimeout” and set to 10 (as shown)

Save these changes.

b. Check in the file **LotusConnections-config.xml;** then stop/restart the Deployment manger and then a Full resynchronise of the Nodes.

23. Import the Tivoli Access Manager certificate into the WebSphere Application Server trust store. For more information, see the Adding certificates to the WebSphere trust store topic.

24. Configure files-config.xml

The files-config.xml must be updated so that the reauthenticateAndSaveSupported property is set to false. This ensures that when an application detects a session timeout, users must log in again through the SSO authentication mechanism.

This change will look like the following :

```
<security reauthenticateAndSaveSupported="false">
<logout href="/files/ibm_security_logout" />
<inlineDownload enabled="false" />
</security>
```

Save the change and resynchronise nodes and restart Connections for these change to take effect.

25. Stop then Restart Connections
Stop all Connections' Clusters, then the Deployment manager; Restart the Deployment manager, then all Connections' clusters.

26. Verify you can access Connections via the TAM URL

Enter ***https://tamserver.mycompany.com/profiles***
You are presented with the TAM login screen:

Enter a valid username and password and you will be logged into Connections.