Business Objects

# BusinessObjects Enterprise XI Release 2

## Configuring Trusted Authentication using IIS / Tomcat Bridge

## Overview

This document will guide you in configuring Trusted Authentication with BusinessObjects XI Release 2 using the IIS to Tomcat Bridge. This guide will aim to provide an alternative Java Single Sign On (SSO) solution to using Kerberos with Vintela. Trusted Authentication provides a simple form of SSO for Java and can also allow for integrating your BusinessObjects Enterprise authentication solution with third-party authentication solutions. Trusted Authentication deployments can also be configured to pass credentials to BusinessObjects universe connections.

## Contents

# Introduction

To be able to perform Trusted Authentication you must have a web server (IIS or Apache) installed to authenticate users and pass credentials to a supported Java Application server such as Tomcat. This guide will walk through a simple IIS to Tomcat configuration. We will assume that you have at least Service Pack 2 for BusinessObjects XI Release 2 installed. We will also assume that you have a default IIS installation (BusinessObjects .NET WCA is not installed).

# Installing and Configuring the Jakarta Connector on IIS

The Jakarta connector (AJP13) is an ISAPI filter from Apache Software that allows IIS to forward specific requests to the back-end Java Application sever. There are a number of benefits gained from doing this, one most important benefit is to take advantage of IIS' ability to leverage AD authentication.

The AJP13 Jakarta connector (version 1.2.14) can be found on Apache Software's site at:

http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.14/

1. Download and install the AJP13 connector on your IIS machine. Accept the default prompts and take note of the directory in which the connector is installed to.

   By default, this directory is:

   ```
   C:\Program Files\Apache Software
   Foundation\Jakarta Isapi Redirector\
   ```

2. You must point this ISAPI filter to your Tomcat system by editing the worker.properties.minimal file in the **`\conf`** folder of the installation directory using wordpad.exe. Alter the line below replacing **`localhost`** with the hostname or IP address of your Tomcat system and save the file:

| CAUTION | Text editors such as Notepad are known to cause issues when editing configuration files. Wordpad and other commercial editors are better choices to avoid problems. |
|---|---|

```
worker.ajp13w.host=localhost
```

3. You must tell the ISAPI filter what content you want to have redirected to your Java application sever. To do this, you must edit the uriworkermap.properties file that exists in the same folder, with wordpad.exe. Immediately after the line that reads **`/servlets-examples/*=wlb`** add the following lines:

```
/businessobjects/*=wlb
/jsfadmin/*=wlb
/dswsbobje/*=wlb
/styles/*=wlb
/AnalysisHelp/*=wlb
```

4. Save the uriworkermap.properties file.

### Confirm creation of the jakarta virtual directory

Confirm that the AJP13 setup created the **`jakarta`** virtual directory within IIS Services Manager:

1. Click **Start > Settings > Control Panel > Administrative tools > Internet Information Services**.
2. Expand the **Web Sites** folder.
3. Expand the **Default Web Site**.

| NOTE | The name of the virtual directory must be **`Jakarta`**. |
|---|---|

4. Right-click the **`Jakarta`** virtual directory and choose properties.
5. Verify that the local path is the AJP13 folder's **`\bin`** directory.
6. Verify that the Execute Permissions are set to **Scripts and Executables**.

### Confirm isapi_reirect.dll was added as a filter

Confirm that the AJP13 setup added isapi_reirect.dll as a filter:

1. Repeat steps 1 and 2 from the previous section above. Right-click the **Default Web Site** and click **Properties.**
2. Click the **ISAPI Filters** tab.
3. Verify that there is a filter named **Jakarta .**

### Add a Web Service Extension for IIS version 6

For IIS version 6, you will need to add a Web Service Extension to permit IIS to run your AJP13 connector.

1. Click **Start > Settings > Control Panel > Administrative tools > Internet Information Services (IIS) Manager**.
2. Expand the computer, right-click **Web Service Extensions**, and click **Add a new Web Service Extension**.
3. Click the **Add…** button, click the **Browse** button and navigate to the isapi_redirect.dll (in the \bin folder).
4. Enter the **Extension name:** as "Jakarta mod_jk".
5. Select the **Set extension status to Allowed** check box and click **OK**.
6. Confirm that the **Status** column displays **Allowed** for **Jakarta mod_jk**.

7. Stop and restart IIS in this screen or through the command-line by typing "iisreset.exe".

# Installing and Configuring the Jakarta Connector on Tomcat

Now that you have the IIS ISAPI filter installed and configured on the IIS side, you have to configure Tomcat to accept connections from IIS. To do this, we will configure Tomcat's AJP13 listener.

1. On the Tomcat system, find the **`server.xml`** located in Tomcat's **`\conf`** directory.
2. Open the **`server.xml`** with wordpad.exe.
3. Do a search for ***`port="8009".`***
4. There are a number of changes that need to be made to this line of text:
    a. Uncomment the line by removing the **`<!--`** and **`-->`** before and after this line
    b. Put a white space between each element
    c. Add a new element: **`tomcatAuthentication="false"`**

| CAUTION | Do Not copy and paste the **`tomcatAuthentication="false"`** element. |
|---|---|

5. Save and restart Tomcat.

## Testing the Tomcat Connector

Check to see that the Tomcat system is listening on port 8009. Then we will try and pull-up some content through the connector.

1. On the Tomcat system open a command-prompt and type:

    netstat –an |grep "8009"

| NOTE | You should find port in LISTENING state. The Tomcat system may take some time to open this port for listening. |
|---|---|

2. Test the connector through a browser by navigating to a URL on the webserver. For example:

    **`http://<iiswebserver>/jsp-examples/`**

3. At this point, try the InfoView URL:

    **`http://<iiswebsever>/businessobjects/enterprise115/desktoplaunch/`**

# Configuring IIS to perform Authentication

This step is required to allow IIS to silently populate the username within the HTTP header and logon the user to BusinessObjects using Trusted Authentication.

1. Click **Start > Settings > Control Panel > Administrative tools > Internet Information Services**.
2. Expand the **Web Sites** folder and right-click the **Default Web Site**
3. Select **Properties > Directory Security** tab > click the **Edit** button under **Authentication and Access Control**.
4. Verify that **Anonymous Access** is unchecked.
5. Verify that **Integrated Windows Authentication** is checked.
6. Click the **OK** button in the next two dialogue boxes. If you are presented with an **Inheritance Override** prompt, select the child node 'jakarta' and click **OK**.
7. Stop and restart IIS in this screen or through the command-line by typing "iisreset.exe".

| NOTES | |
|---|---|
| | • You should be able to still access IIS web content from a client machine without being prompted for your domain credentials. If you are prompted then you are not already logged into a Windows Desktop as a domain user<br>• Another reason could be your IIS server is not a member of the list of **Local Intranet Sites** in IE (This IIS site can not also exist in IE's **Trusted Sites**).<br>• If you are using a Windows 2003 client, **Internet Explorer Enhanced Security Configuration** could be enabled and interfering. |

## Configure IE settings for Local Intranet Sites

To add your IIS site to your client machine's IE settings, follow these steps:

1. Logon to the Windows Desktop as your domain user.
2. Open IE and click **Tools > Internet Options > Security** tab.
3. Click the **Local intranet** Icon **> Sites** button **> Advanced** button.
4. Type your IIS server URL in the **Add this web site to the zone** text box:

   http://<iiswebserver>/
5. Click the **Add** button **> OK** button **> OK** button **> OK** button.

Now when you try to access the IIS web server again, you should not be prompted.

# Configuring Trusted Authentication

Trusted Authentication will work with any authentication method available in BusinessObjects XI Release 2 (Enterprise, LDAP, Active Directory or Windows NT). Before proceeding, make sure that your users are created in the system either by creating Enterprise accounts manually, or mapping a group through one of the 3rd party plug-ins and selecting **New aliases will be added and new users will be created** as your update option.

There are a number of ways to configure Trusted Authentication. These alternate configurations are fully documented in our BusinessObjects XI Release 2 Deployment and Configuration guide located on our documentation site:

http://support.businessobjects.com/documentation/product_guides/default.asp

## Using the REMOTE_USER method

The next steps will guide you though configuring trusted authentication using the REMOTE_USER method.

1. Find the web.xml for InfoView. By default, this is located here:

   \Tomcat\webapps\businessobjects\enterprise115\desktoplaunch\WEB-INF\web.xml

2. Create a backup copy of this **`web.xml`** so we can revert back to a working system if we make mistakes.
3. Edit the **`web.xml`** using wordpad.exe
4. Make the following changes:

| <param-name> | Default value | New value |
|---|---|---|
| cms.default | Hostname:port of your CMS | Hostname:port of your CMS |
| siteminder.enabled | true | false |
| sso.enabled | false | true |
| trusted.auth.user.retrieval | (blank) | REMOTE_USER (see below) |
| trusted.auth.user.param | (blank) | (blank) |

| | | |
|---|---|---|
| trusted.auth.shared.secret | (blank) | (blank) |

The parameter **`trusted.auth.user.retrieval`** should look like the following:

```
<context-param>
<param-name>trusted.auth.user.retrieval</param-name>
<param-value>REMOTE_USER</param-value>
</context-param>
```

| NOTE | Take note that **`<param-value>`** had to be added and the "/" had to be moved to the correct side of **`</param-value>`**. **Do not copy and paste from this document**. |
|---|---|

## Creating the TrustedPrincipal.conf file

Create the **`TrustedPrincipal.conf`** file by doing the following:

1. Navigate to the following folder:

\BusinessObjects Enterprise 11.5\win32_x86\plugins\auth\secEnterprise

2. Create a file named "TrustedPrincipal.conf".
3. In this file enter the following line:

   **SharedSecret=your_shared_secret**

4. Save the file.

## Setting the same shared secret in the Central Management Console

Set the same shared secret in the Central Management Console (CMC) by doing the following:

1. Logon to the CMC as Administrator.
2. Click **Authentication** under the **Manage** section and the **Enterprise** tab.
3. Select the **Trusted Authentication is enabled** check box.
4. Enter your shared secret into the **Shared secret** text box.
5. Click the **Update** button.

### Testing the Trusted Authentication

At this point, we can restart Tomcat and test to see that SSO using Trusted Authentication is working. Please ensure that you have a valid BusinessObjects Enterprise user account created.

http://<iiswebserver>/businessobjects/enterprise115/desktoplaunch/

### Using Multiple Domains in Active Directory

Be aware that with Trusted Authentication, Active Directory usernames are stripped of their domain pre-fix. Because of this, if 2 users have the same username, but come from different domains such as **`AMER\jsmith`** and **`INT\jsmith`**) they will both be logged in as a BusinessObjects Enterprise account named **`jsmith.`**

## Finding more information

Read the Business Objects XI Release 2 Deployment and Configuration guide.

To find out how to define an exit page for Trusted Authentication, read KB 4085978.

For more information and resources, refer to the product documentation and visit the support area of the web site at

http://support.businessobjects.com/

▶ www.businessobjects.com