# Single Sign-On with Windows Azure AD for JSP Applications

## Direct Federation

This simple sequence assumes your familiarity with Java, Apache Tomcat and Eclipse installation. Unless otherwise specified all the installations are 64-bit.

1. Log into your Azure management portal create Azure AD domain and service principal from <http://msdn.microsoft.com/library/windowsazure/dn151790.aspx>
   1. Follow steps “Create a New Directory Tenant and Add User” create WAAD tenant
   2. Follow the “Register a New Application” in creating a service principal
   3. From the “Federation Metadata Document URL” note the metadata URL
   4. From the app configuration menu, note CLIENT ID (Properties section), REPLY URL (single sign-on section)
2. Install [Java SE Development Kit 7u40](http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html) and set up JAVA\_HOME system environment variable
3. Install [Eclipse IDE for Java EE Developers (Kepler SR1)](http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx)
4. Install [Apache Tomcat 7.0.42](http://tomcat.apache.org/download-70.cgi) (download 64-bit Windows Zip)
   1. Unzip Tomcat
   2. Create keystore and [Setup SSL](http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html)
5. Download the application bits which includes two projects: “waad-federation” and “sample”
6. Import Maven projects “waad-federation” and “sample” into the Eclipse workspace
7. Edit trusted.issuers.xml with your Azure AD details. The sample is shown below:

The CLIENT ID from the previous step is used as the realm.

<issuers>

<issuer name=*"contoso.onmicrosoft.com"*

displayname=*"Contoso"*

metadataurl=*"https://login.windows.net/efaee2d0-5730-46ea-a8a7-e502fe8dbb4b/FederationMetadata/2007-06/FederationMetadata.xml"*

realm=*"spn:xxxxxxxx-e160-43ba-832f-4caa93553e82"*

audienceuri=*"spn:xxxxxxxx-e160-43ba-832f-4caa93553e82"*

replyurl=*"https://localhost:8443/sample/wsfed-saml"*

/>

</issuers>

The following is the legend for the above fields:

* name : anything that makes the issuer node unique
* displayname: this is only used to display the list of providers on the log in page
* metadataurl: WAAD metadata URL as displayed in the WAAD service management portal
* realm: Azure AD Client ID (from Azure Service Management Portal) that is synonymous with Application Principal ID (if used Powershell to display the principal details)
* audienceuri: same as the realm; only one entry is supported for now
* replyurl: the token will be sent to this URL; obtained from service management portal “CONFIGURATION” menu

1. Configure federation.properties in the “Sample” project as below [replace the values with your application details]:

#this is a pointer to the trusted issuer in trusted.issuers.xml resource

federation.trusted.issuer.to.use=contoso.onmicrosoft.com

1. Run the application in Eclipse
   1. Run the “sample” application in the eclipse workspace from the “Run As” menu
   2. Make sure to edit the keystore location in server.xml located in the Tomcat server definition inside the Eclipse workspace

## Federation through Windows Azure ACS

1. Create your ACS namespace say “contosoacs.accesscontrol.windows.net”
2. Log into your Azure management portal create Azure AD domain and service principal from <http://msdn.microsoft.com/library/windowsazure/dn151790.aspx>
   1. Follow steps “Create a New Directory Tenant and Add User”
   2. Following the step ““Register a New Application”, create an application (aka service principal) with the values below:

App URL = <https://contosoacs.accesscontrol.windows.net/>

App ID URI = <https://contosoacs.accesscontrol.windows.net/>

* 1. From the “Federation Metadata Document URL” note the metadata URL
  2. From the app configuration menu, note CLIENT ID (Properties section), REPLY URL (single sign-on section)

1. Add Azure AD as the federation identity provider using the metadata URL noted above
2. Define the default rule group and edit the rule group as needed
3. Follow steps 2 to 9 in configuring the application