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

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

1. 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
2. Install [Eclipse IDE for Java EE Developers (Kepler SR1)](http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx)
3. 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)
4. Download the application bits which includes two projects: “waad-federation” and “sample”
5. Import Maven projects “waad-federation” and “sample” into the Eclipse workspace
6. 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” and “Register a New Application”
   2. From the “Federation Metadata Document URL”
   3. From the app configuration menu, note CLIENT ID (Properties section), REPLY URL (single sign-on section)
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=*"schneider.onmicrosoft.com"* displayName=*"schneider"*

realm=*"spn:b9f0f8cf-e160-43ba-832f-4caa93553e82"* />

</issuers>

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

#metadata URL for the Azure AD tenant obtained from the application definition

federation.metadata.url=https://login.windows.net/efaee2d0-5730-46ea-a8a7-e502fe8dbb4b/FederationMetadata/2007-06/FederationMetadata.xml

# Client ID from the Azure AD application single sign-on section of "CONFIGURE" menu

federation.realm=spn:b9f0f8cf-e160-43ba-832f-4caa93553e82

# Client ID from the Azure AD application single sign-on section of "CONFIGURE" menu

federation.audienceuris=spn:b9f0f8cf-e160-43ba-832f-4caa93553e82

# REPLY URL from the Azure AD application single sign-on section of "single sign-on" menu. The reply URL should match the servelet mapping name

federation.reply=https://localhost:8443/sample/wsfed-saml

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