HHS EWITS 2.0 AMS Integration Deployment Guide

Last updated March 11st, 2019

Taeho Lee

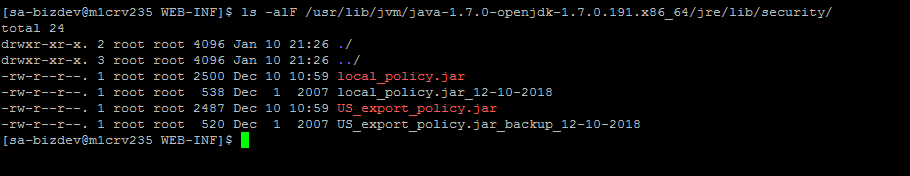
**Environment**: BizFlow 12.4.0010.0, Java 7 x64, Tomcat 8, Linux

# Deploy JCE for Policy File (by ServerAdmin)

This is a prerequisite step. You will need ROOT permission to change JRE directory. If you don’t have permission, **ask System Admin to copy the files.**

Download JCE (Java Cryptography Extension) Policy Files for your Java version from Oracle. As of today (January 16, 2019) HHS EWITS 2.0 is running JDK 7 x64bit. ***Notes****: for convenience, the JCE Policy file for JDK 7 file has been included in HHS BizFlowSSO package.*

1. Unzip **UnlimitedJCEPolicyJDK7.zip**
2. Deploy the two jar files to JRE directory
   1. **Notes:** JER directory must be the same JRE that Tomcat server is currently using. If you don’t know, you can find the path in catalina.out file.
   2. **{JRE}/lib/security/local\_policy.jar**
   3. **{JRE}/lib/security/US\_export\_policy.jar**
   4. /usr/lib/jvm/java-1.7.0-openjdk-1.7.0.191.x86\_64/jre/lib/security/local\_policy.jar
      1. /usr/lib/jvm/java-1.7.0-openjdk-1.7.0.191.x86\_64/jre/lib/security/US\_export\_policy.jar



# Configure BizFlow Server

1. Note your BizFlow Web Server IP addresses before start.
   1. **$ ifconfig**
2. Go to **{BizFlowServer}/bin** directory
   1. {BizFlowServer} is where BizFlow application server is installed.
      1. I.e. /bizflow/dev/bin, /bizflow/test/bin, /bizflow/prod/bin
3. Stop BizFlow Application server
   1. **$ ./down**
4. Open server.ini file
   1. **$ vi ./server.ini**
5. Find **[WAS]** section in the file
6. Add all Bizflow web server IPs

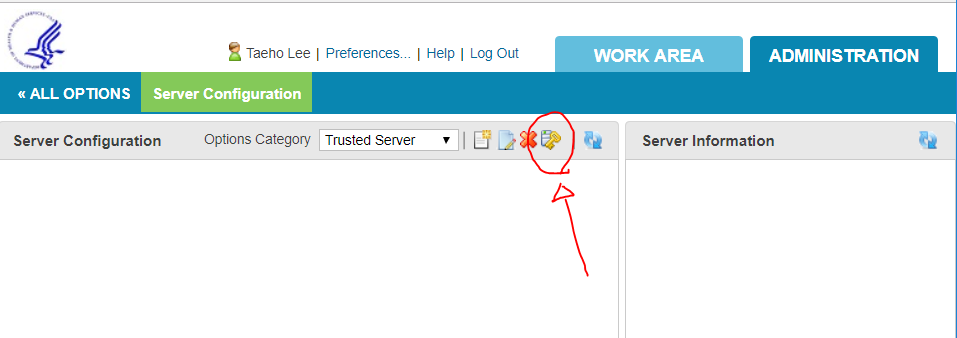
|  |
| --- |
| **[WAS]**  ; To enable trusted server feature, set the following in server.ini.  ; This applies to WebLogic or WebSphere portal customers only.  ; This server.ini setting is for the IP addresses of Portal servers that accesses BizFlow server directly.  ; See appendix B in "BizFlow Portal Bridge Deployment Guide" for other configurations.  **TrustedServer.0=127.0.0.1**  **TrustedServer.1=111.222.333.444** |

* 1. You must put 127.0.0.1 for local system access.
  2. You must change 111.222.333.444 with correct Web server IP address.

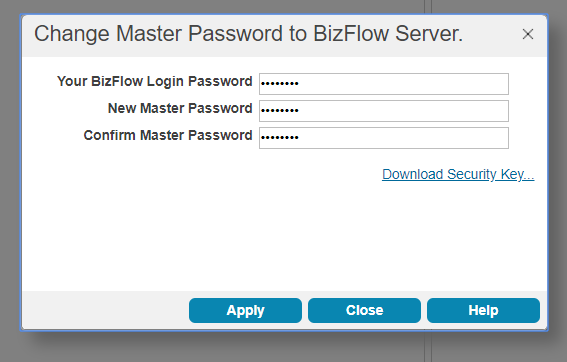
1. Start BizFlow Application server
   1. **$ ./startup**

# Setup Master Password

1. Go to Administrator > Server Configuration > Trusted Server



1. Set Up Master Password

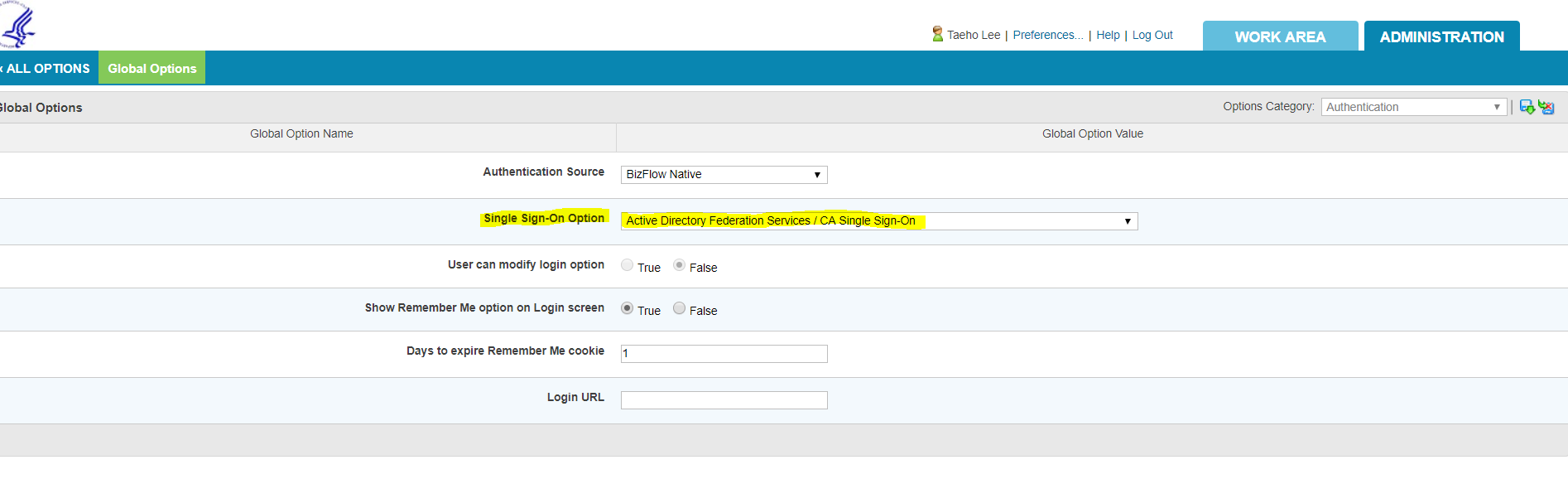


* 1. Your BizFlow Login Password:
     1. Type your BizFlow password
  2. New Master Password:
     1. Type “**changeit**”
  3. Confirm Master Password:
     1. Type “**changeit**”
  4. Click Download Security Key…
  5. Type “**changeit**”
  6. Click Download button
  7. Click Apply button to exit

1. and Download Security Key to **{TOMCAT}\webapps\bizflow\WEB-INF\bizflow.cert**

# Modify the Global Options for BizFlow Web server

1. Log into EWITS2.0 as System Administrator
2. Go to **Administrator > Global Options > Authentication**
3. Set “**Single Sign-On**” to “**Active Directory Federation Services/CA Single Sign-ON**”



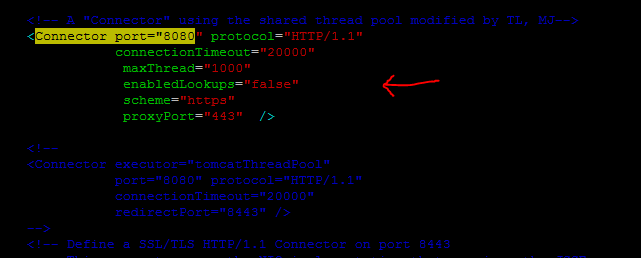
# Configure Tomcat server Connector

This step will enable Tomcat to work with a load balancer.

1. Shutdown Tomcat
2. Go to Tomcat **conf** directory
3. Open **server.xml**
4. Find **<Connector port=**
5. Change Connector setting to use https over proxy
   1. For instance

|  |
| --- |
| Before  <Connector port="*8080*" protocol="HTTP/1.1"  connectionTimeout="20000"  maxThread="1000"/> |
| After  <Connector port=“*8080*” protocol="HTTP/1.1"  connectionTimeout="20000"  maxThreads="1000"  **enableLookups="false"**  **scheme="https"**  **proxyPort="443"**/> |

* 1. Please note that port number can be different in your environment.
     1. ***enableLookups****:Set to true if you want calls to request.getRemoteHost() to perform DNS lookups in order to return the actual host name of the remote client. Set to false to skip the DNS lookup and return the IP address in String form instead (thereby improving performance). By default, DNS lookups are enabled.*
     2. ***Scheme****: set this attribute to the name of the protocol you wish to have returned by calls to request.getScheme(). For example, you would set this attribute to "https" for an SSL Connector. The default value is "http". See* [*SSL Support*](https://tomcat.apache.org/tomcat-5.5-doc/config/http.html#SSL%20Support) *for more information.*
     3. ***proxyPort****: If this Connector is being used in a proxy configuration, configure this attribute to specify the server port to be returned for calls to request.getServerPort().*
  2. Save the file



# Deploy BizFlowSSO patch to webapps/bizflow

***Notes****: for convenience, the patch has been included in HHS BizFlowSSO package.*

1. Shutdown Tomcat
2. Find webapps/bizflow directory in the package
   1. The package was built with BizFlow 12.4.0010.0 version
3. Copy webapps/bizflow/**logout.jsp** in the package to webapps/bizflow directory of Tomcat server
4. Rename webapps/bizflow/WEB-INF/lib/**hwweb.jar** to **hwweb.org** on Tomcat server
5. Copy webapps/bizflow/WEB-INF/lib/**hwweb.jar** from the package to Tomcat server

# Configure BizFlow web.xml

1. Shutdown Tomcat
2. Open web.xml by using any text editor (vi)
   1. **{TOMCAT}/webapps/bizflow/WEB-INF/web.xml**
3. Add **context-param** in red-colored below.

|  |
| --- |
| <context-param>  <!-- The definition of the Root Spring Container shared by all Servlets and Filters -->  <param-name>contextConfigLocation</param-name>  <param-value>/WEB-INF/spring/root-context.xml</param-value>  </context-param>  **<!-- BizFlowSSO logout //-->**  **<context-param>**  **<param-name>BizFlowSSOLogoutURL</param-name>**  **<param-value>/bizflowsso/saml/logout?local=true</param-value>**  **</context-param>** |

1. Set the value of “param-value” for “**redirect\_url**” in the file.
2. Set the value of “param-value” for “**TrustedServers**” in the file.
   1. You can add multiple server addresses with “,” delimiter. **Notes**: In the example below, they are all PROD server IP address.
      1. **127.0.0.1,localhost,158.74.50.211,m1crv234.hhs.gov,m1crv234,158.74.50.215,hrts.prod.hhs.gov**

|  |
| --- |
| <!-- BizFlow-SSO Integration -->  <filter>  <filter-name>SessionMonitoringFilter</filter-name>  <filter-class>com.hs.bf.web.session.filter.SessionMonitoringFilterImpl</filter-class>  <init-param>  <param-name>**redirect\_url**</param-name>  <!-- Set param-value below with bizflowsso URL to use BizFlowSSO. -->  <!-- For example,  <param-value>/bizflowsso</param-value>  Or  <param-value>https://webhost:webport/bizflowsso</param-value>  -->  <param-value>**/bizflowsso/**</param-value>  </init-param>  <init-param>  <param-name>noCheck\_urls</param-name>  <param-value>/bizlogin.jsp,/bizlogin2.jsp,/bizindex.jsp,/msg.jsp,/themes/oceanblue/langs/en/bizlogo.gif,/themes/oceanblue/sessionbg.jpg</param-value>  </init-param>  <init-param>  <param-name>**TrustedServers**</param-name>  <param-value>**127.0.0.1,localhost,158.74.50.211,m1crv234.hhs.gov,m1crv234,158.74.50.215,hrts.prod.hhs.gov**</param-value>  </init-param>  </filter> |

# Deployment BizFlowSSO

## 1) Deploy BizFlowSSO.war

***Notes****: for convenience, bizflowsso.war has been included in HHS BizFlowSSO package.*

1. Find **bizflow.war** file in the package
   1. The package was built with BizFlow 12.4.0010.0 version
2. Copy the **bizflowsso.war** file to Tomcat webapps directory.
   1. I.e {TOMCAT}/webapps
3. Tomcat server will unzip the war file automatically.
4. Check if bizflowsso directory has been fully created.

## 2) Create a Keystore and Import Certificates

### 2-1) Create a Keystore

In this step, we will create bizflowsso keystore having private and public key pair, and import ADFS web server’s public certificate. If ADFS certificate has chain, we need to import parent certificate.

1. Shutdown Tomcat
2. Go to Tomcat server
3. Delete existing keystore file

|  |
| --- |
| $ ***cd {TOMCAT}/webapps/bizflowsso/WEB-INF/classes/security***  $ ***rm samlKeystore.jks*** |

1. Generating keystore

|  |
| --- |
| $ keytool -genkeypair -alias **hhsadfs** -keyalg RSA -validity 3650 -keypass **changeit** -keystore **samlKeystore.jks** -storepass changeit -dname "CN=***hrts.prod.hhs.gov***, OU=Devices, OU=OS, OU=HHS, O=U.S. Government, C=US"  $ chmod 666 **samlKeystore.jks** |

* 1. This command generates a public key/private key pair, and then imports the pair to the keystore. So, the keystore "samlKeystore.jks" will now contain additional PrivateKeyEntry with alias "**hhsadfs**".
  2. Notes that CN=hrts.prod.hhs.gov need to be changed for your environment.

### 2-2) Import ADFS Certificates

**Important:** It is very important to make sure the ADFS certificates are active. ADFS server administrator must inform EWITS 2.0 administrator when to change the certificate so that EWITS 2.0 administrator can re-import the certificate in the keystore**.**

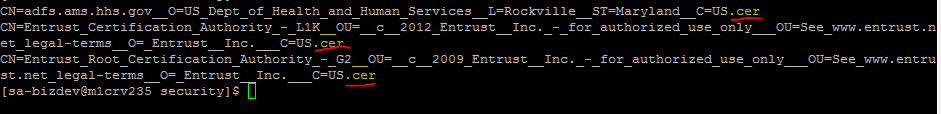
In this step, we will import public keys of ADFS server.

1. **Extracting certificates**

The SSL Extractor utility can be used to extract certificates presented by an SSL/TLS endpoint. You can find the jar file in **bizflowsso/WEB-INF/script-bin** directory. Or you can download it from github.com <https://github.com/vschafer/ssl-extractor/tree/master/release>

|  |
| --- |
| *$ cd* ***{TOMCAT}****/webapps/bizflowsso/WEB-INF/classes/security*  $ java -jar ../../script-bin/**sslextractor-0.9.jar** **adfs.ams.hhs.gov** 443  $ ls \*.cer |

You will see three cer files are generated in security directory.

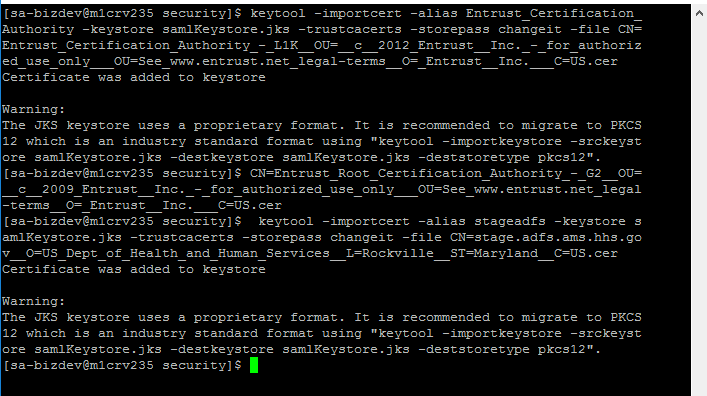


1. **Import all the extracted certificates**

This command imports additional trusted key to the keystore. You may want to change the cer files to make it shorter for easier typing.

**Notes**: the generated extracted#.cer file names can be different from command below. Change the blue-colored file names with the generated file names.

|  |
| --- |
| keytool -importcert -alias Entrust\_Root\_Certification\_Authority -keystore samlKeystore.jks -trustcacerts -storepass changeit -file CN=Entrust\_Root\_Certification\_Authority\_-\_G2\_\_OU=\_\_c\_\_2009\_Entrust\_\_Inc.\_-\_for\_authorized\_use\_only\_\_\_OU=See\_www.entrust.net\_legal-terms\_\_O=\_Entrust\_\_Inc.\_\_\_C=US.cer  keytool -importcert -alias Entrust\_Certification\_Authority -keystore samlKeystore.jks -trustcacerts -storepass changeit -file CN=Entrust\_Certification\_Authority\_-\_L1K\_\_OU=\_\_c\_\_2012\_Entrust\_\_Inc.\_-\_for\_authorized\_use\_only\_\_\_OU=See\_www.entrust.net\_legal-terms\_\_O=\_Entrust\_\_Inc.\_\_\_C=US.cer  keytool -importcert -alias stageadfs -keystore samlKeystore.jks -trustcacerts -storepass changeit -file CN=adfs.ams.hhs.gov\_\_O=US\_Dept\_of\_Health\_and\_Human\_Services\_\_L=Rockville\_\_ST=Maryland\_\_C=US.cer |



1. **Reviewing the details of certificate contained within keystore entries**

|  |
| --- |
| $ keytool -list -v -keystore samlKeystore.jks |

This command can be used to list entries in keystore "samlKeystore.jks"

## 3) Upload federationmetadata.xml

In this step, we will download **federationmeta.xml** file from ADFS site, and upload to Tomcat server directory.

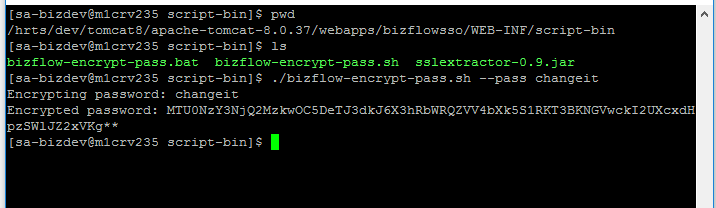
1. Open web browser
2. Visit federationmetadata.xml URL
   1. There are only two environments. Stage.adfs.mas.hhs.gov needs to be shared for DEV and TEST.
   2. DEV, TEST
      1. <https://stage.adfs.ams.hhs.gov/federationmetadata/2007-06/federationmetadata.xml>
   3. PROD
      1. <https://adfs.ams.hhs.gov/federationmetadata/2007-06/federationmetadata.xml>
3. Download the file to local
4. Upload the file to **{TOMCAT}/bizflowsso/WEB-INF/classes/security** directory

## 4) Change bizflowsso.properties

In this step, we will configure bizflowsso module to communicate with ADFS server.

### 4.1) Generate password

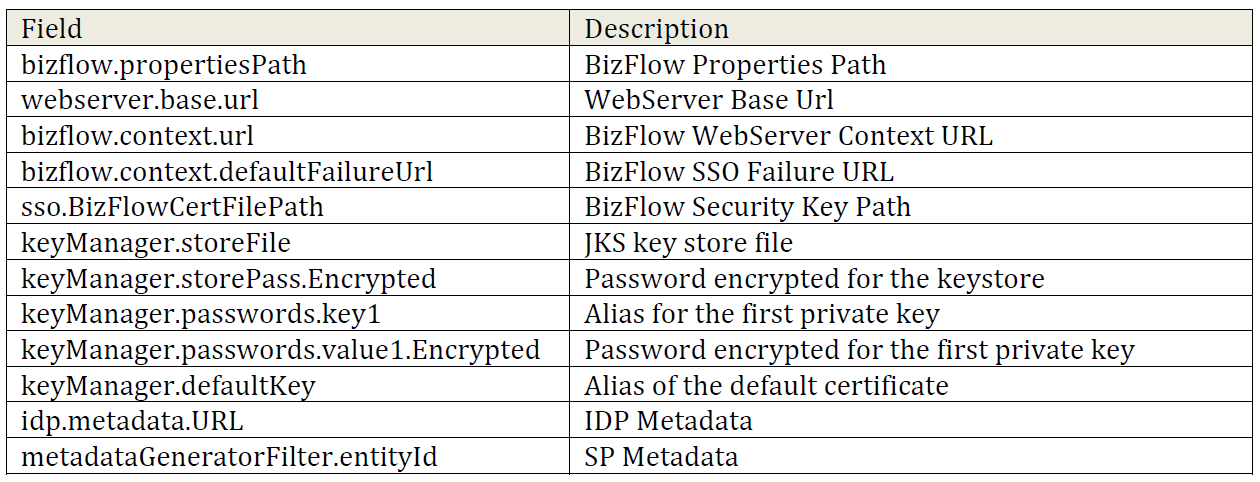
keyManager.storePass.Encrypted and keyManager.passwords.value1.Encrypted should be encrypted by bizflow-encrypt-pass tool.



1. Go to **{Tomcat}/webapps/bizflowsso/WEB-INF/script-bin**
2. Make **bizflow-encrypt-pass.sh** executable
3. Generate password
4. Note (or copy it to clipboard) the generated encrypted password

|  |
| --- |
| $ **cd {TOMCAT}/webapps/bizflowsso/WEB-INF/script-bin**  $ **chmod +x bizflow-encrypt-pass.sh**  $ **./bizflow-encrypt-pass.sh --pass changeit** |

### 4.2) Update bizflowsso.properties



1. Go to **{TOMCAT}/webapps/bizflow/WEB-INF/classes/security** directory
2. Open **bizflowsso.properties**
3. Edit properties file
4. Save the file.

|  |
| --- |
| $ **cd {TOMCAT}/webapps/bizflowsso/WEB-INF/classes**  $ **vi bizflowsso.properties** |

**Notes:** blue-colored properties need to be changed with your environment setting.

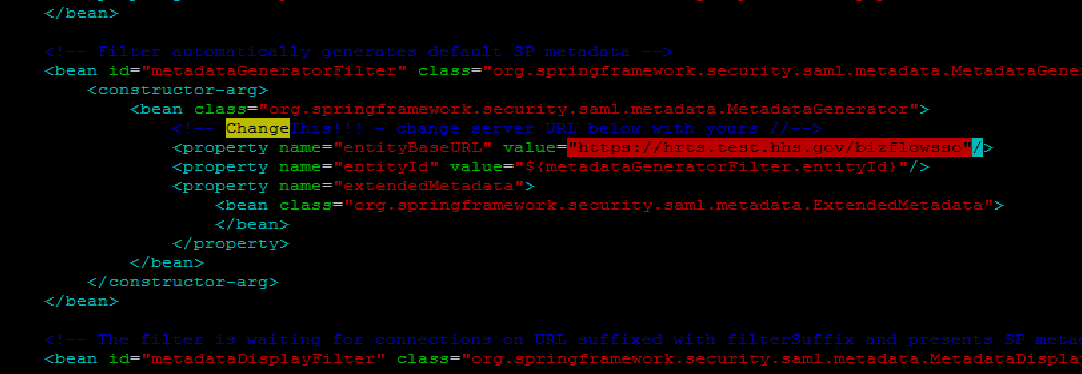
|  |
| --- |
| # BizFlow-SSO Properties File  ################################################################################  # BizFlow  ################################################################################  # BizFlow Properties Path  bizflow.propertiesPath=**/hrts/prod/tomcat8/apache-tomcat-8.0.37/**webapps/bizflow/WEB-INF/bf.properties-auto  # WebServer Base Url  webserver.base.url=***https://hrts.prod.hhs.gov***  # BizFlow WebServer Context Url  bizflow.context.url=${webserver.base.url}/bizflow  #BizFlow SSO Failure URL  bizflow.context.defaultFailureUrl=${bizflow.context.url}/msg.jsp?resid=MSG\_SSO\_FAIL  # BizFlow Security Key Path  sso.BizFlowCertFilePath=**/hrts/prod/tomcat8/apache-tomcat-8.0.37/**webapps/bizflow/WEB-INF/bizflow.cert  ################################################################################  # Active Directory Federation Services (AD FS) 2.0  ################################################################################  # Central storage of cryptographic keys for SAML  keyManager.storeFile=classpath:security/samlKeystore.jks  # storePasswd encrypted  keyManager.storePass.Encrypted=***MTU0Njk5MDc0NDc0NC5HN0xnTk9yYmpLcFBzYVdiSGxXeEhocV9LWFhaQlE5T1BJNUdVNVJ6T0tZKg\*\****  keyManager.passwords.key1=hhsadfs  # password encrypted for key  keyManager.passwords.value1.Encrypted=***MTU0Njk5MDc0NDc0NC5HN0xnTk9yYmpLcFBzYVdiSGxXeEhocV9LWFhaQlE5T1BJNUdVNVJ6T0tZKg\*\****  keyManager.defaultKey=hhsadfs  # IDP Metadata for SAML  idp.metadata.URL=***https://adfs.ams.hhs.gov/federationmetadata/2007-06/federationmetadata.xml***  # Unique identifier of the service provider for SAML  metadataGeneratorFilter.entityId=${webserver.base.url}/bizflowsso/saml/metadata  ################################################################################  # CA Single Sign-On  ################################################################################  siteminderFilter.principalRequestHeader=SM\_USER  #When principal has domain name with @, set "siteminderFilter.principal.cutOffCharacters" to "@" to remove it.  #siteminderFilter.principal.cutOffCharacters=@  siteminderFilter.principal.cutOffCharacters= |

### 4.3) Update securityContext.xml

1. Open **bizflow-sso.properties** in **{TOMCAT}/webapps/bizflowsso/WEB-INF/classes** directory
2. Edit entries below in the file
3. Save
4. Restart Tomcat

|  |
| --- |
| $ **cd {TOMCAT}/webapps/bizflowsso/WEB-INF/classes**  $ **vi securityContext.xml** |

|  |
| --- |
| <!-- ChangeThis!!! - change server URL below with yours //-->  <property name="**entityBaseURL**" value="**https://hrts.prod.hhs.gov/bizflowsso**"/> |



### 

### 4.4) Generate metadata.xml

1. Open web browser
2. Visit {EWITS2\_URL}[/bizflowsso/saml/metadata](https://hrts.prod.hhs.gov/bizflowsso/saml/metadata) and download metadata.xml
   1. Prod: ***https://hrts.prod.hhs.gov/bizflowsso/saml/metadata***
   2. Test: https://hrts.test.hhs.gov/bizflowsso/saml/metadata
   3. Dev: https://hrts.dev.hhs.gov/bizflowsso/saml/metadata
   4. OldDev: https://hrts.olddev.hhs.gov/bizflowsso/saml/metadata
3. Open the metadata.xml
4. Check all EWITS2 URLs use not http:// but https://
   1. If not, change [**http**://hrts.prod.hhs.gov](http://hrts.prod.hhs.gov) to [**https**://hrts.prod.hhs.gov](https://hrts.prod.hhs.gov) to use https instead.
5. Save the file
6. Send the metadata.xml file to AMS team

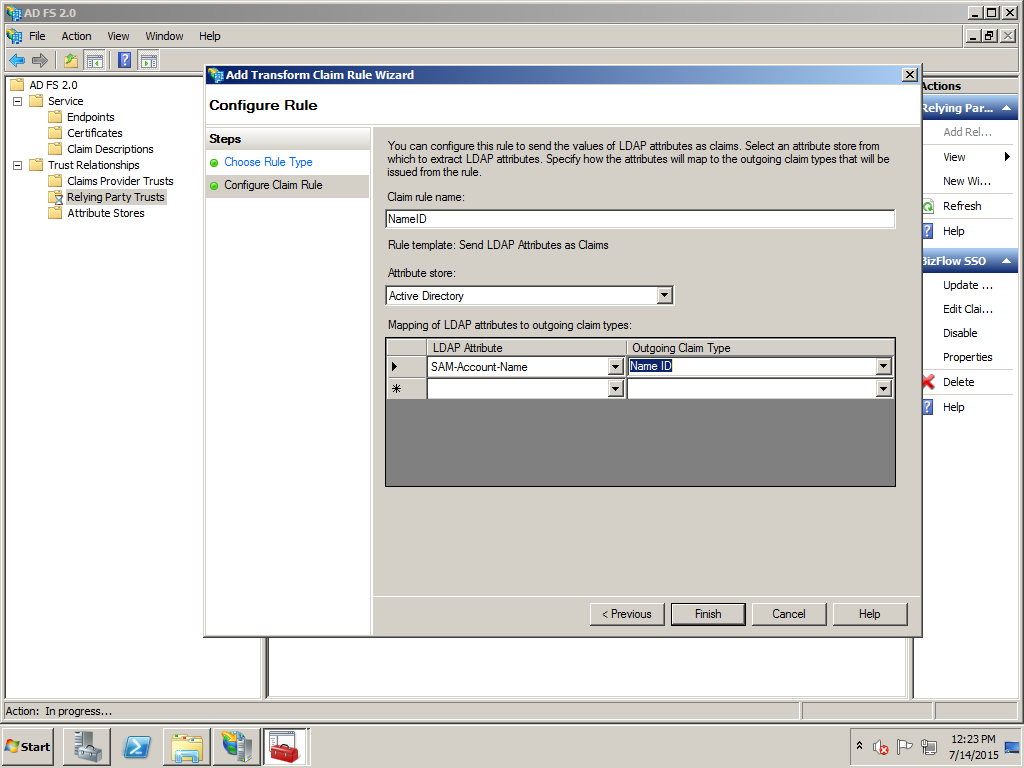
# Deploy logout.jsp to webapps/bizflow

1. Find logout.jsp file in the HHS AMS SSO package
2. Upload logout.jsp to {TOMCAT}/webapps/bizflow
3. Restart Tomcat server

# 

# Deployment Guide in ADFS Side (by ADFS Admin)

1. Open up the ADFS Management Console and navigate to the Relying Party Trusts section
2. Click “Add Relying Party Trust…” and click Start.
3. Choose “Import data about the replying party from a file”
4. Select the metadata.xml file that was generated at the previous step.
5. Enter a name for trust and click Next
6. Choose “Permit all users to access this replying party”, and click Next.
7. Choose “Send LDAP Attributes as Claims” Then, click Next.
8. Add “NameID” as “Claim rule name”, Choose “Active Directory” as attribute store, choose “SAM-Account-Name” as LDAP Attribute and “Name ID” as “Outgoing claim type”, finish the wizard and confirm the claim rules window. Cick Apply and OK.



Appendix

# How to enable / disable BizFlowSSO

## Modify the Global Options for BizFlow Web server

1. Log into EWITS2.0 as System Administrator
2. Go to **Administrator > Global Options > Authentication**
3. Set “**Single Sign-On**” to “**Active Directory Federation Services/NONE**”

## Change web.xml

1. Go to {Tomcat}/webapps/bizflow/WEF-INF
2. Open web.xml
3. Remove value of **param-value** of **redirect\_url**
   1. From
      1. <param-value>/bizflowsso/<param-value>
   2. To
      1. <param-value><param-value>

|  |
| --- |
| <init-param>  <param-name>**redirect\_url**</param-name>  <!-- Set param-value below with bizflowsso URL to use BizFlowSSO. -->  <!-- For example,  <param-value>/bizflowsso</param-value>  Or  <param-value>https://webhost:webport/bizflowsso</param-value>  -->  **<param-value></param-value>**  </init-param> |

1. Save the file
2. Restart Tomcat