

INTALIO Integrate UI-FW and CAS

Tempo

Log In 
[View](#) [Attachments \(4\)](#) [Info](#)
 [Browse Space](#)Added by [Nicolas Modrzyk](#), last edited by [Nicolas Modrzyk](#) on Oct 22, 2009

Integrate ui-fw with CAS

1. Setup CAS server properly (see previous FAQ).
2. Change the WEBAPP_ROOT/ui-fw/WEB-INF/web.xml, adding this:

```
<context-param>
  <param-name>edu.yale.its.tp.cas.proxyUrl</param-name>
  <param-value>https://cas.com:8443/cas/proxy</param-value>
</context-param>
<filter>
  <filter-name>CAS Filter</filter-name>
  <filter-class>edu.yale.its.tp.cas.client.filter.CASFilter</filter-class>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.loginUrl</param-name>
    <param-value>https://cas.com:8443/cas/login</param-value>
  </init-param>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.validateUrl</param-name>
    <param-value>https://cas.com:8443/cas/proxyValidate</param-value>
  </init-param>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.serviceUrl</param-name>
    <param-value>http://cas.com:8080/ui-fw</param-value>
  </init-param>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.proxyCallbackUrl</param-name>
    <param-value>https://cas.com:8443/ui-fw/CasProxyServlet</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>CAS Filter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<filter>
  <filter-name>CASRBAC Filter</filter-name>
  <filter-class>org.intalio.tempo.uiframework.filter.CASRBACFilter</filter-class>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.serviceUrl</param-name>
    <param-value>http://cas.com:8080/ui-fw</param-value>
  </init-param>
  <init-param>
    <param-name>edu.yale.its.tp.cas.client.filter.logoutUrl</param-name>
    <param-value>https://cas.com:8443/cas/logout</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>CASRBAC Filter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<servlet>
  <servlet-name>ProxyTicketReceptor</servlet-name>
  <servlet-class>
    edu.yale.its.tp.cas.proxy.ProxyTicketReceptor
  </servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>ProxyTicketReceptor</servlet-name>
  <url-pattern>/CasProxyServlet</url-pattern>
</servlet-mapping>
```


3. if the tempo and CAS server run on the same machine, could change both the 'cas.com' and 'tempo.com' to the same host. (eg: 'localhost')
4. you would also need to update the securityConfig.xml file with the proper host name for ticket validation:





```
<constructor-arg index="1" value="https://cas.com:8443/cas/proxyValidate" />
```



5. check the cas webapp looks for users only in the proper LDAP section (this is in deployerConfigContext.xml)

```
...
<bean class="org.jasig.cas.adaptors.ldap.BindLdapAuthenticationHandler">
  <property name="filter" value="cn=%u" />
  <property name="searchBase" value="dc=examples,dc=com" />
  <property name="contextSource" ref="contextSource" />
  <property name="ignorePartialResultException" value="yes" />
</bean>
...
```

6. check the apacheds webapp has the proper section

▼  dc=examples,dc=com (2)

- ▼  ou=People (2)
 - ▶  cn=ewilliams
 - ▶  cn=msmith
- ▼  ou=Roles (2)

- ▶  cn=employee
- ▶  cn=manager

7. check the certificate

1. tomcat uses an alias named 'tomcat' by default, and here's how it looks in server.xml, with the regular intalio keystore

```
<Connector port="8443" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS" alias="tomcat" keystoreFile="var/config/intalio-keystore.jks"/>
```

2. you can delete the existing one by using the following command

```
keytool -delete -alias tomcat -keystore intalio-keystore.jks
```

3. to generate a new certificate with the proper hostname, you can use the following command]

```
keytool -genkey -alias tomcat -keyalg RSA -keystore intalio-keystore.jks
```

4. and be sure you use the 'hostname' as first name and last name input

```
Enter keystore password:
What is your first and last name?
[Unknown]: cas.com
What is the name of your organizational unit?
[Unknown]:
```

5. Be Careful



Be Careful

Most of the SSO (with CAS but also in general) requires valid hostnames.
You can update your '/etc/hosts' file, with anything like this:
'127.0.0.1 cas.com'
to make it easy to run everything on the same machine.

Configuration on jboss

1.

1. You need to configure SSL in jboss, edit the file \$HOME/server/default/deploy/jbossweb-tomcat55.sar/server.xml

```
<Connector port="8443" address="{jboss.bind.address}"
  maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true"
  scheme="https" secure="true" clientAuth="false"
  keystoreFile="{jboss.server.home.dir}/../var/config/intalio-keystore.jks"
  keystorePass="changeit" sslProtocol = "TLS" />
```

2. Update the securityConfig.xml file as described above
3. If it is not done already, update the run.conf with the keystore file path, as described above



Note for jboss

Jboss does not support multiple hosts by default, and you need to refer to the following [document](#) if you want to have cas.com and tempo.com to be in different domains within the same jboss instance.

Comments

Site powered by a free **Open Source Project / Non-profit License** ([more](#)) of **Confluence - the Enterprise wiki**.
[Learn more](#) or [evaluate Confluence for your organisation](#).

Powered by **Atlassian Confluence**, the **Enterprise Wiki**. (Version: 1.4.1 Build:#212 Jun 02, 2005) - [Bug/feature request](#) - [Contact Administrators](#)