

第三方平台，接入统一登录平台说明

1) 添加配置文件信息

打开项目的 WEB-INF/web.xml

加入如下配置，**红色部分**按自己应用的实际情况修改：

```
<!-- ===== start ===== -->
<listener>

<listener-class>org.jasig.cas.client.session.SingleSignOutHttpSessionListener</listener-class>
</listener>
<filter>
    <filter-name>CAS Single Sign Out Filter</filter-name>
    <filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>
</filter>
<filter-mapping>
    <filter-name>CAS Single Sign Out Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter>
    <filter-name>CAS Filter</filter-name>
    <filter-class>org.jasig.cas.client.authentication.AuthenticationFilter</filter-class>
    <init-param>
        <param-name>casServerLoginUrl</param-name>
        <param-value>https://demo.micmiu.com:8020/cas/login</param-value>
    </init-param>
    <init-param>
        <param-name>serverName</param-name>
        <param-value>http://myApplicationIp:port/appName</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>CAS Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter>
    <filter-name>CAS Validation Filter</filter-name>
    <filter-class>
        org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter
    </filter-class>
```

```

<init-param>
    <param-name>casServerUrlPrefix</param-name>
    <param-value>https://demo.micmiu.com:8020/cas/login</param-value>
</init-param>
<init-param>
    <param-name>serverName</param-name>
    <param-value>http://myApplicationIp:port/appName</param-value>
</init-param>
</filter>
<filter-mapping>
    <filter-name>CAS Validation Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter>
    <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>
    <filter-class>
        org.jasig.cas.client.util.HttpServletRequestWrapperFilter
    </filter-class>
</filter>
<filter-mapping>
    <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter>
    <filter-name>CAS Assertion Thread Local Filter</filter-name>
    <filter-class>org.jasig.cas.client.util.AssertionThreadLocalFilter</filter-class>
</filter>
<filter-mapping>
    <filter-name>CAS Assertion Thread Local Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<!-- ===== end ===== -->

```

2) 修改项目的 pom.xml 添加一下 jar 包

```

<dependency>
    <groupId>org.jasig.cas.client</groupId>
    <artifactId>cas-client-core</artifactId>
    <version>3.2.1</version>
</dependency>

```

3) 在自己的登录方法类中添加一下内容，例子如下：

```

public ModelAndView toLogin(HttpServletRequest request,
    HttpServletResponse response) throws Exception{
    System.out.println("start sso login");
    Assertion assertion = (Assertion) request.getSession().getAttribute(

```

```
AbstractCasFilter.CONST_CAS_ASSERTION);

AttributePrincipal principal = assertion.getPrincipal();
String username = principal.getName();
System.out.println(principal.getAttributes().toString());
System.out.println("userName is : " + username);
```

注释：开发者可以通过上面的代码获得用户信息，并按照自己的需要，保存用户信息到应用中。
打印结果如下（如果还需要其他信息，请给我联系需求）：

```
{userGender=1, userId=272202,
userPassword=e10adc3949ba59abbe56e057f20f883e, userName=deane,
userEmail=deane163@163.com, userPhone=18800000000}
userName is :deane
```

注意：用户可以通过以下用户登录：

邮箱登录：deane163@163.com/123456

用户名登录：[deane/123456](#)

电话号码登录：[18800000000/123456](#)

由于我们测试服务器没有域名，请在自己的 host 文件添加
10.10.1.47 demo.micmiu.com

基于安全考虑，我们的单点登录，必须是 https 协议，需要认证证书，请把 jssecacerts 文件，放到文件夹：

%JAVA_HOME%\jre\lib\security\ 文件夹下，已通过 https 的访问验证。

测试用户登录信息：

<https://demo.micmiu.com:8020/cas/login>
deane/123456

测试用户登出信息：

<https://demo.micmiu.com:8020/cas/logout>
在 cas 中清除用户信息