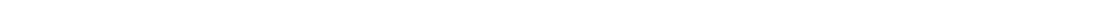


统一身份认证对接文档



目录

1 前言	1
1.1 编写目的.....	1
2 集成方式概述.....	1
3 认证接口集成.....	1
3.1 JDK 版本要求	1
3.2 客户端 Jar 包部署	1
3.3 修改原有登录入口.....	2
3.4 修改原有登出.....	3

1 前言

1.1 编写目的

本文档作为 IDS6.0 版本中应用系统的认证集成手册，旨在指导校内应用系统实现校内统一身份认证和单点登录集成。

2 集成方式概述

IDS6.0 单点登录基于 CAS (Central Authentication Service - 中心认证服务)，目的就是使分布在内部各个不同异构系统的认证工作集中在一起，通过一个公用的认证系统统一验证用户身份的合法性。通过 CAS 认证的用户将获得 CAS 颁发的一个证书，使用这个证书，用户可以在承认 CAS 证书的各个系统上自由穿梭访问，不需要再次的登录认证。

CAS 客户端在认证过程中的实现逻辑：

1) 以 filter 的形式，对 B/S 结构应用系统资源进行过滤保护，可以保护所有资源，也可以保护单一资源。

2) 获得 CAS Server 颁发的 ServiceTicket，并凭此 ST 从 CAS Server 上取得登录用户信息。

3) 为第三方应用提供开发接口，使得受保护的应用能够根据 CAS 认证信息进行正确的登录。

3 认证接口集成

3.1 JDK 版本要求

程序使用的 JDK 要求是 JDK1.4 及以下版本。

3.2 客户端 Jar 包部署

将公司提供的 casclient.jar 放在集成系统的 WEB-INF/lib 目录下。

3.3 修改原有登录入口

集成有两种方案：

1、方案一：保留原有登录入口，新增加应用访问入口，新增入口与 CAS 做集成

➤ 在 web.xml 里面上述配置的 filter 的基础上增加 filter 的过滤 pattern

```
<filter-mapping>
  <filter-name>CAS Filter</filter-name>
  <url-pattern>/caslogin.jsp</url-pattern>
</filter-mapping>
```

➤ 引入 CAS 相关

```
<% @page import="edu.yale.its.tp.cas.client.CASAttrPrincipal"%>
```

➤ 实现登录

按照上述获取用户帐号，在集成系统中判断用户在集成系统中是否存在，如果存在实现集成系统的登录（例如 session 中写入身份信息、权限信息等等），如果不存在按照集成既定的业务逻辑处理。

➤ 登录后根据原有逻辑跳转

登录成功之后，可以按照原有逻辑去处理，或者跳转到一开始访问的未授权页，或者跳转到集成系统的首页。

➤ 方案二：封闭原有入口，统一使用 CAS 登录入口

➤ 在 web.xml 里面上述配置的 filter 的基础上增加 filter 的过滤 pattern(这边是*)

```
<filter-mapping>
  <filter-name>CAS Filter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

➤ 引入 CAS 相关

```
<% @page import="edu.yale.its.tp.cas.client.CASAttrPrincipal"%>
```

➤ 修改登录验证逻辑

按照上述获取用户帐号，在集成系统中判断用户在集成系统中是否存在，如果存在实现集成系统的登录（例如 session 中写入身份信息、权限信息等等），如果不存在按照集成既定的业务逻辑处理。

3.4 修改原有登出

(可选，如果不需要单点登出，这一部分可以不做)

- ◆ 在原有登出逻辑的基础上，redirect 到统一身份认证 logout 链接，如下(跳转到哪一页由集成系统自己决定)

[https://am.wisedu.com/authserver/logout?service={encoded}\(集成系统首页 URL\)}](https://am.wisedu.com/authserver/logout?service={encoded}(集成系统首页 URL)})

统一身份认证登出 URL 可在 web.xml 里面作为全局参数配置好：

```
<context-param>
  <param-name>casServerLogoutUrl</param-name>
  <param-value>https://am.wisedu.com/authserver/logout</param-value>
</context-param>
```

上述 URL 可以通过 request.getServletContext().getInitParameter("casServerLogoutUrl")获取

或者 JSP 中通过 `application.getInitParameter("casServerLogoutUrl")` 获取

- ◆ 集成应用会话超时登出如果需要单点登录会话登出，在 `web.xml` 里面加入如下 Listener

```
<listener>
  <listener-class>
    edu.yale.its.tp.cas.client.SingleSignOutHttpSessionListener
  </listener-class>
</listener>
```