

CAS 单点登录对接

这页给需要把业务系统接入乐维 CAS 单点登录的开发人员或系统集成工程师使用。你可以按[这里](#)确认登录跳转、ticket 验证、用户信息返回和上线前安全项。

更新时间：2026-06-17

适用场景

- 业务系统希望接入统一身份认证，用户登录一次后访问多个受信任系统。
- 前端需要把用户引导到 CAS 登录页，并在认证后接收回调。
- 后端需要验证 CAS 返回的 ticket，再建立业务系统自己的登录态。

对接前确认

开始前，先确认下面几项，避免登录跳转成功但回调或验证失败：

- 已获取 CAS 服务地址，本文用 {server} 表示。
- 已确定业务系统回调地址，也就是 service 参数。
- service 回调地址已在 CAS 服务端允许访问。
- 业务系统后端可以访问 serviceValidate 验证接口。
- 生产环境建议全链路使用 HTTPS。

核心接口

接口	作用	调用方
GET {server}/backend_api/auth/cas/login	发起 CAS 登录，跳转至 CAS 认证页。	前端浏览器
GET {server}/backend_api/auth/cas/p3/serviceValidate	验证 CAS 返回的 ticket，获取用户信息。	业务系统后端

对接流程

1. 用户访问业务系统受保护页面。
2. 业务系统前端将用户重定向到 CAS 登录地址。
3. 用户在 CAS 认证页面完成登录。
4. CAS 服务认证成功后携带 ticket 回跳 service 地址。
5. 业务系统前端拿到 service?ticket=xxx。
6. 业务系统前端将 ticket 提交给后端。
7. 业务系统后端调用 serviceValidate 验证 ticket。
8. CAS 服务返回用户信息或认证失败。
9. 业务系统后端建立本地登录态。
10. 用户进入业务系统。

发起 CAS 登录

接口地址：

```
GET {server}/backend_api/auth/cas/login
```

请求参数：

参数	类型	必填	说明
service	String	是	登录成功后的业务系统回调地址。CAS 认证通过后，浏览器会重定向到这个地址并附带 ticket。

请求示例：

```
GET {server}/backend_api/auth/cas/login?service=https%3A%2F%2Fyour-app.example.com%2Fcallback
```

注意：service 必须先做 URL 编码。

验证 ticket

接口地址：

```
GET {server}/backend_api/auth/cas/p3/serviceValidate
```

请求参数：

参数	类型	必填	说明
ticket	String	是	CAS 认证成功后通过回调 URL 传递的一次性票据。

请求示例：

```
GET {server}/backend_api/auth/cas/p3/serviceValidate?ticket=ST-xxxxxx-xxxxxxxxxxxxx
```

验证成功返回：

```
<cas:serviceResponse xmlns:cas="http://www.yale.edu/tp/cas">
<cas:authenticationSuccess>
<cas:user>admin</cas:user>
</cas:authenticationSuccess>
</cas:serviceResponse>
```

验证失败返回：

```
<cas:serviceResponse xmlns:cas="http://www.yale.edu/tp/cas">
<cas:authenticationFailure code="INVALID_TICKET">
Ticket 无效或已过期
</cas:authenticationFailure>
</cas:serviceResponse>
```

返回字段：

字段	说明
cas:authenticationSuccess/cas:user	验证成功后返回的用户名。
cas:authenticationFailure	验证失败信息。常见失败码为 INVALID_TICKET。

后端处理建议

业务系统后端建议按下面顺序处理：

1. 从回调请求里提取 ticket。
2. 由后端调用 serviceValidate 验证 ticket。
3. 解析 XML 返回结果。
4. 验证成功后，根据 cas:user 建立业务系统自己的会话或登录令牌。
5. 验证失败时，引导用户重新登录或提示认证失败。

不要在前端直接验证 ticket。ticket 是一次性认证票据，验证动作应由业务系统后端完成。前端直接调用验证接口容易带来票据泄露、结果被篡改或跨域访问失败等风险。

常见问题

service 参数没有 URL 编码会怎样？

CAS 登录地址可能解析失败，或者回调地址中的 ?、& 等字符被错误截断。发起登录前，请先对完整 service 地址做 URL 编码。

ticket 可以重复使用吗？

不可以。ticket 通常只能验证一次。重复验证可能返回 INVALID_TICKET 或认证失败。

ticket 过期怎么办？

引导用户重新发起 CAS 登录。不要复用旧的 ticket，也不要将 ticket 长期保存在前端或日志里。

回调地址打不开或无法进入系统怎么办？

先确认 service 地址是否正确、是否已 URL 编码、是否在 CAS 服务端允许访问，并检查业务系统前后端是否都能访问对应域名。

验证成功但业务系统仍然未登录怎么办？

检查业务系统后端是否正确解析 cas:user，以及是否成功创建本地会话、Cookie 或登录令牌。

上线前检查

- service 回调地址已经 URL 编码。
- 回调地址已经在 CAS 服务端允许访问。
- 业务系统后端可以访问 serviceValidate 接口。
- ticket 只在后端验证，并且只消费一次。
- 生产环境使用 HTTPS。
- 验证成功后，业务系统会建立自己的登录态。
- 验证失败时，页面会提示用户重新登录。

接口路径和返回字段以当前部署版本为准。如果现场路径、域名或返回内容与本文不一致，请以实际环境配置为准。