

烁维云技术文档

烁维云平台单点登录到第三方系统

V1.0



企业使用多个应用系统时，就会出现不同登录入口，需要记住每个系统的地址和对应的用户名和密码，非常的麻烦，还容易出错。烁维云平台的‘集成与单点登录’产品，解决了这个问题，只要一次登录，就可直接登录所有系统。

本文主要讲解，如何配置从烁维云平台单点登录到第三方系统，从而实现一次登录烁维云平台，就可以直接进入第三方系统。

前提条件：

1.您是企业用户

2.企业已经在自己的服务器中完成“烁维云平台”系统的部署（相关操作说明，请参考 <https://www.sygnw.com/> 中的【企业专区】）。


对于使用烁维 SaaS 平台的企业，如需实现单点登录到第三方系统，则需向烁维运维提出申请，由烁维工程师完成处理。

3.企业已经在使用的烁维云平台系统中部署了 ‘集成与单点登录’ 产品（关于如何引入和部署产品到烁维云平台，相关操作说明，请参考 <https://www.sygnw.com/> 中的【企业专区】或“个人中心”的【企业专区】相关文档）。

第一步：登录烁维云平台

- 如果企业有独立的烁维云平台登录地址，输入地址直接登录平台。
- 如果企业已经接入到烁维云生态中，请输入 <https://sso.sygnw.com> 登录平台。

登录烁维云平台的用户，需要拥有【开发中心】-【单点与外接服务】-【外接系统注册】

功能的权限。（功能权限授权，点击平台主页右上方  帮助与支持，‘入门手册’中的《公司管理员操作手册》）

第二步：申请系统的授权应用号（client_id）和授权密钥（client_secret）

1、注册外接系统。

进入平台打开【开发中心】-【单点与外接服务】-【外接系统注册】功能，进入如下界面

The screenshot shows a web form titled '外接系统注册' (External System Registration). The form includes several input fields and toggle switches. Red circles with numbers 1 through 6 point to specific elements: 1 points to the '第三方系统...' (Third-party system...) field; 2 points to another '第三方系统...' field; 3 points to the '需要单点登...' (Need single sign-on...) toggle switch; 4 points to the '需要数据集成' (Need data integration) toggle switch; 5 points to the '保存' (Save) button; and 6 points to the '提交' (Submit) button. The form also has a '回调地址' (Callback address) field and a '收起' (Collapse) button in the top right corner.

1) 输入外接系统编码：由数字、小写字母组成（下划线不能使用），编码将作为授权应用号（client_id）的一部分。

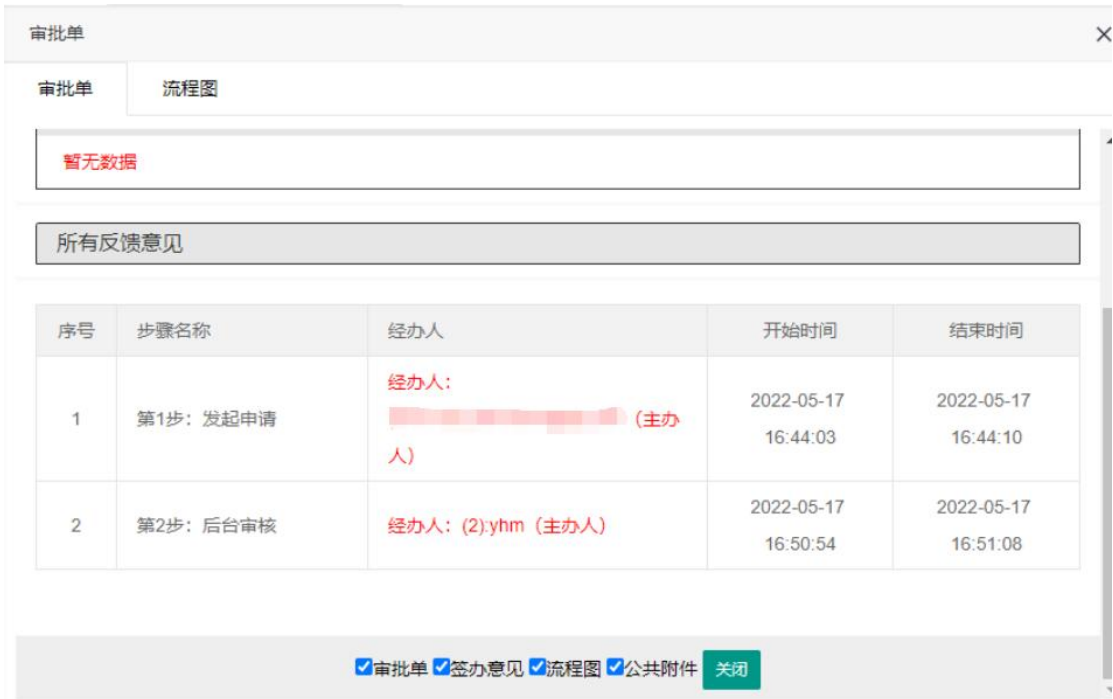
2) 输入外接系统名称

3) 如果需要进行单点登录集成，请打开开关。

4) 如果需要数据集成，请打开开关。

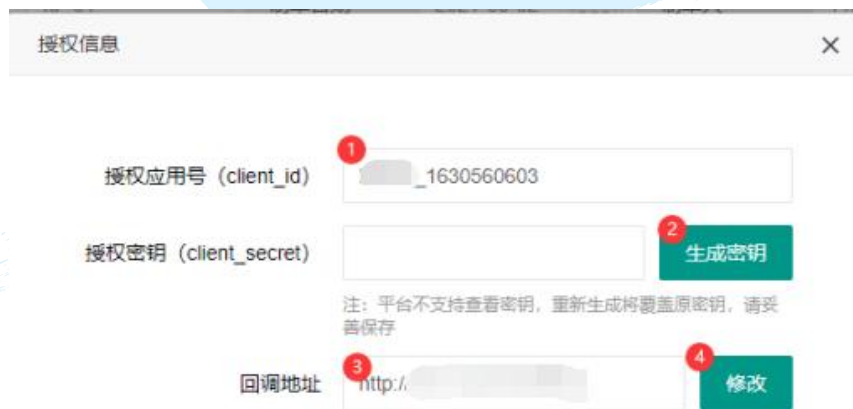
5) 回调地址，用于外接系统登录鉴权。

保存后点击‘提交’，等待平台审核，可以通过‘审批流’查看当前审批的状态。如图



2、获取授权应用号 (client_id) 和授权密钥 (client_secret)

审核通过后，点击界面下方的‘审核信息’按钮，弹出如下界面



1) 授权应用号为系统自动生成。由外接系统编码和一组随机数字组成。

2) 点击‘生成密钥’，系统自动生成授权密钥，注意平台不支持查看密钥，重新生成将覆盖原密钥，请妥善保管。

3) 回调地址，如果是单点登录集成，输入外接系统的回调地址。点击‘修改’按钮，以上设置生效。

第三步：在烁维云平台中创建单点登录功能点

1、创建第三方系统功能点。

进入平台打开【开发中心】-【单点与外接服务】-【外接功能点定义】功能，进入如下界面，增加功能节点。



- 1) 英文简缩码：由字母、数字组成。
- 2) 功能点名称：由中文、字母、数字组成。
- 3) 是否弹出：设置功能点的打开方式，弹出新的窗口还是在平台以新建页签的方式打开。
- 4) 点击‘保存’，功能点创建完成。

2、进行外接服务配置。

进入平台打开【开发中心】-【单点与外接服务】-【外接服务配置】功能，进入如下界面，增加配置服务。



- 1) 第三方系统：选择功能点对应的第三方系统
- 2) 编码：外接服务配置的编码，由字母、数字组成。
- 3) 名称：外接服务配置的名称，由中文、字母、数字组成。
- 4) 第三方系统服务器链接地址：外接系统的访问地址。
- 5) 点击‘保存’，外接服务配置完成。

3、系统管理员分配单点登录功能点的权限。

第四步：数据集成，请参考《单点登录的数据集成模式》。

第五步：调整外接系统代码，实现烁维云平台单点登录到第三方系统。

(一) 实现步骤

注：【】中的变量说明，见‘二、变量说明’中的详细说明。

步骤一:在烁维云平台中点击功能点，打开三方系统地址【url】，第三方的系统会判断当前用户是否已经登录第三方的系统，已经登录的进入第三方的系统的后续主页，没有登录进行步骤二。

步骤二:跳转到烁维平台 sso 进行鉴权 参数用 get 方式传递

302 Location:

https://sso.sygnw.com/oauth/authorize?response_type=code&client_id= 【 client_id 】

&scope=*;corp:last&state=【state】&redirect_uri=【redirect_uri】

步骤三：

1、跳转到烁维的认证服务器登录界面，登录成功后回调第三方系统的回调地址【redirect_uri】，回调地址调用示例参数如下：

302 Location: 【redirect_uri】?code=2339a784a7f747b79d93befd8f264e0b&state=【state】

2、第三方系统从 get 的参数中得到 code 后在第三方系统的服务器上用 POST 方式访问 https://sso.sygnew.com/oauth/token 得到 token

3、获取 token 模拟调用命令

1) .【code】从 get 参数中得到,因为 code 只能使用 1 次，再次使用这个 code 获取 token 会报错，错误信息如下: {"message": "An authorization code must be supplied.", "status": 0}

2) .模拟的【redirect_uri】

=http%3A%2F%2Fclient.sygnew.com%2Flogin%2Foauth%2Fcode%2Fsso-login

```
curl -X POST "https://sso.sygnew.com/oauth/token" -H "Content-Type: application/x-www-form-urlencoded; charset=UTF-8" -d "grant_type=authorization_code&code=2339a784a7f747b79d93befd8f264e0b&redirect_uri=http%3A%2F%2Fclient.sygnew.com%2Flogin%2Foauth%2Fcode%2Fsso-login&client_id=demo_12345678&client_secret=00885c609f391979be009dedf722c000"
```

成功返回

```
{"access_token": "c12v5vCKUjCWJIdoiM0UwpTb6-01PQHzuXg5nDA9iGfmbd-JUBuvPCuQpUW aR79xD7R-0hoBxyGikrviBxhzr0USuP4iJOS89ahIqa3F90100ym-8JpC2E0AI751wKezRigeSUGmdraQ9a4kSogag iT7fsFP7dogkefbr5LSUtvPA", "opencode": "SampleClientId", "scope": "*,corp:last", "urlfile": "https://xxx/group1/upload", "urlapi": "https://xxx/yyy", "token_type": "bearer", "expires_in": 7199, "jti": "12905bd7-fc64-4cce-837e-1fdad12dc935", "status": 1}
```

步骤四：第三方系统根据得到的 token，处理好自己的 session 和 cookie，标志为登录状态，并跳转回【url】。

可以从 token 的第二段（用.分割）做 base64 解码，得到 email,roles 等不同的属性例如：

```
{"iss": "http://sso.sygnew.com", "sub": "791293669@qq.com", "aud": "dangan_1629283276
```

```

", "roles": "all", "agt": "60c17578262aec7dccf40bf13352d86b", "cid": "@ubhirH2Ina_ENJbIjZc_fh2A
YNDBiDag@", "pid": "@e9hKudVqxGmmRXn8Lck87Q..@", "uid": "@ubhirH2Ina_9tzbkiJzCh0UtgemMb7CB@",
"rmt": "103.100.65.242", "usr": "791293669@qq.com", "lan": "zh_cn", "ltm": "2021-09-17", "exp": 163
1863806, "nbf": 1631856606, "iat": 1631856606, "jti": "12905bd7-fc64-4cce-837e-1fdad12dc935"}
    
```

roles 中的权限是烁维系统中的此操作员拥有角色的编码，第三方系统可以用这个参数控制自己系统的权限范围。

步骤五：验证 token 的正确性

用返回的 access_token 作为参数请求平台提供的‘获取当前操作员的信息’接口，地址 [https://develop.sygnew.com/docs/contract.sign/#/?id= 207](https://develop.sygnew.com/docs/contract.sign/#/?id=207) 获取当前操作员的信息，在得到当前用户信息的同时完成公钥的验证。

二、变量说明：

【client_id】 : 烁维平台提供的 client_id

【client_secret】 : 烁维平台提供的 client_secret

【url】 : 第三方系统提供的的访问地址，用于浏览器访问烁维平台中功能点的地址

【redirect_uri】 : 第三方系统提供的回调地址，用于烁维单点服务器访问，第三方在这个地址的程序中处理鉴权

【state】 : 是由客户自己定义的锁定此次登录的 id，可以忽略。