

MaxKey 与 GitLab

单点登录集成指南

1. MaxKey 介绍

MaxKey 社区专注于身份安全管理(IM)、单点登录(SSO)和云身份认证(IDaaS)领域, 将为客户提供企业级的身份管理和认证, 提供全面的 4A 安全管理(指 Account, Authentication, Authorization 和 Audit)。

为企业提供社区版 IAM 产品, 减少企业建设 IAM 的成本; 同时提供企业版的 IAM 咨询和技术支持, 从而提高客户体验和降低企业内部的自开发成本。

MaxKey 单点登录认证系统, 谐音为马克思的钥匙寓意是最大钥匙, 是**业界领先的 IAM 身份管理和认证产品**; 支持 OAuth 2.x/OpenID Connect、SAML 2.0、JWT、CAS、SCIM 等标准协议; 提供简单、标准、安全和开放的用户身份管理(IDM)、身份认证(AM)、单点登录(SSO)、资源管理和权限管理等。

官方网站地址: <https://www.maxkey.top/>

2. GitLab 介绍

GitLab 是由 GitLabInc.开发, 使用 MIT 许可证的基于网络的 Git 仓库管理工具, 且具有 wiki 和 issue 跟踪功能。使用 Git 作为代码管理工具, 并在此基础上搭建起来的 web 服务。

官方网站地址: <https://about.gitlab.com/>

3. GitLab 安装配置

3.1. GitLab 安装

请参照官方文档 <https://about.gitlab.com/install/>

3.2. 配置

具体可参照 https://docs.gitlab.com/ee/integration/oauth_provider.html

编辑 `gitlab.rb`

打开配置文件:

```
vim /etc/gitlab/gitlab.rb
```

增加 OAuth 配置:

```
gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['oauth2_generic']
gitlab_rails['omniauth_block_auto_created_users'] = false
gitlab_rails['omniauth_providers'] = [
  {
    'name' => 'MaxKey',
    'app_id' => '9cdbccbe-47a0-4adb-9d3d-7e0eaceaace',
    'app_secret' => 'F3Q0MTUwMzIwMjExMTMyMTAzNDknMW',
    'args' => {
      client_options: {
        'site' => 'http://sso.maxkey.top',
        'authorize_url'=>'http://sso.maxkey.top/authz/oauth/v20/authorize',
        'token_url'=>'http://sso.maxkey.top/maxkey/authz/oauth/v20/token',
        'user_info_url' => 'http://sso.maxkey.top/maxkey/api/oauth/v20/me'
      },
      user_response_structure: {
        root_path: [],
        id_path: ['username'],
        attributes: { name: 'username', nickname: 'nickName' }
      },
      name: 'maxkey', # display name for this strategy
      strategy_class: "OmniAuth::Strategies::OAuth2Generic"
    }
  }
]
```

配置文件修改完成后，重设配置：

```
gitlab-ctl reconfigure
```

重设完毕，等待约 30 秒。

重新启动 gitlab

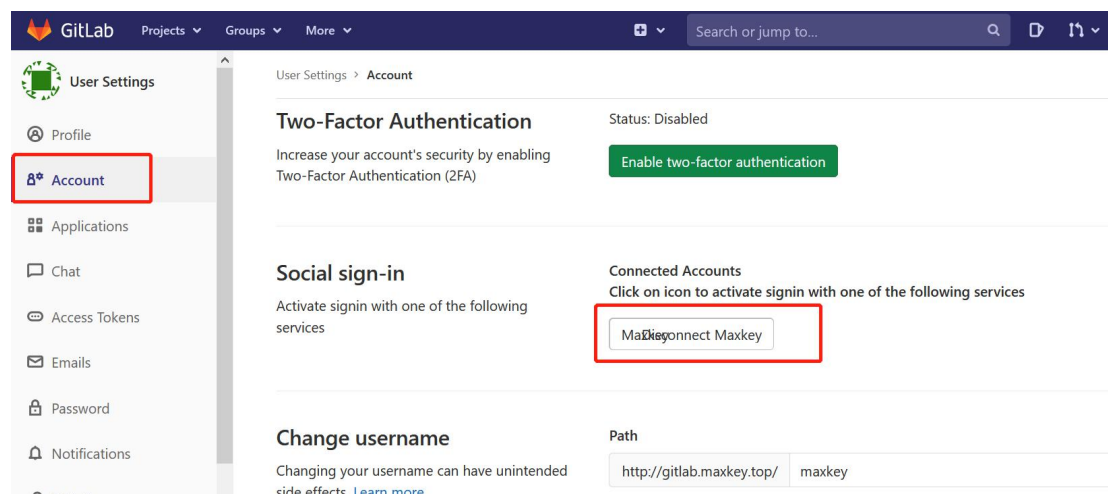
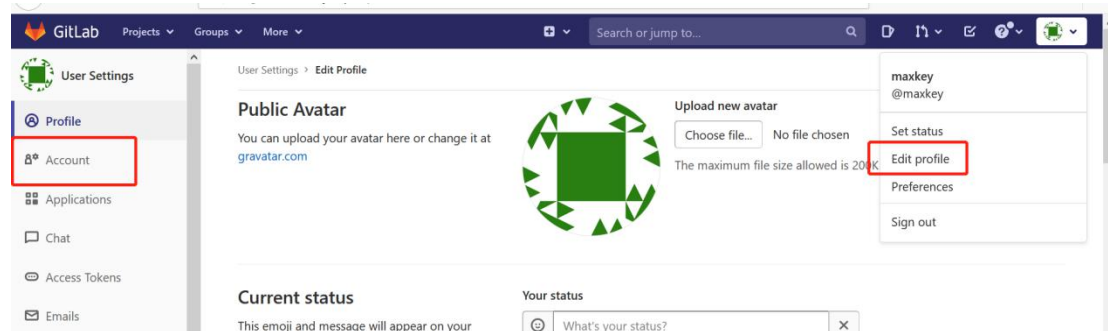
```
gitlab-ctl restart
```

3.3. 创建账号

3.4. 创建一个账号 maxkey

3.5. 关联 Gitlab 账号

用户登录 gitlab 之后，在 setting-Account 中点击 Connect 进行账户关联。



关联成功后，即可使用登录页的 Oauth2 登录。

3.6. 注意事项

Gitlab 必须要手动关联后，才可单点登录。

https 需要配置 omiauth 的 provider_ignores_state:true，同时需要把 maxkey 的证书放到 gitlab 的 trusted-certs 下，然后重新配置 gitlab-ctl reconfigure 就好了。


4. MaxKey 配置及登录验证

4.1. 应用配置

进入后台“应用管理”，编辑应用



配置主要明细入下

登录地址:	http://gitlab.maxkey.top/		
注销地址:		注销方式:	无
访问协议:	OAuth_v2.0	类型:	DEV
图标:		排序:	3
供应商:	GitLab	供应商网址:	https://about.gitlab.com/
权限范围:	所有用户	扩展属性:	请选择
适配:	禁用	适配器:	OAuth 2.0默认适配器 请选择
描述:			
OAuth 2.0 认证配置			
Client Id:	9cdbccbe-47a0-4adb-9d3d-7e0eceaacaace	Client Secret:	F3QOMTUwMzlwMjExMTMyMTAzNDknMW
作用域:	read <input checked="" type="checkbox"/> write <input type="checkbox"/> trust <input type="checkbox"/> openid <input type="checkbox"/> profile <input type="checkbox"/> email <input type="checkbox"/> phone <input type="checkbox"/> address <input type="checkbox"/> all <input type="checkbox"/>		
授权方式:	authorization_code code <input checked="" type="checkbox"/> password <input type="checkbox"/> implicit <input type="checkbox"/> refresh_token <input type="checkbox"/> id_token <input type="checkbox"/> token <input type="checkbox"/>		
认证地址:	http://gitlab.maxkey.top/users/auth/maxkey/callback		

配置对应关系

序号	MaxKey	参数	备注
----	--------	----	----

1	登录地址	http://gitlab.maxkey.top/	
2	访问协议	OAuth_v2.0	
3	适配	启用	
4	适配器	OAuth 2.0 默认适配器	
5	认证地址	http://gitlab.maxkey.top/users/auth/maxkey/callback	
6	授权方式	authorization_code	

4.2. 应用访问赋权



如果不在该列表内，可以“新增成员”

4.3. 单点登录验证

重新登录 <https://sso.maxkey.top/maxkey>，点击“GitLab”图标单点登录

