



概述

Casdoor is a UI-first [Identity Access Management \(IAM\)](#) / [Single-Sign-On \(SSO\)](#) platform with web UI supporting OAuth 2.0, OIDC, SAML, CAS, LDAP, SCIM, WebAuthn, TOTP, MFA, RADIUS, Google Workspace, Active Directory and Kerberos.

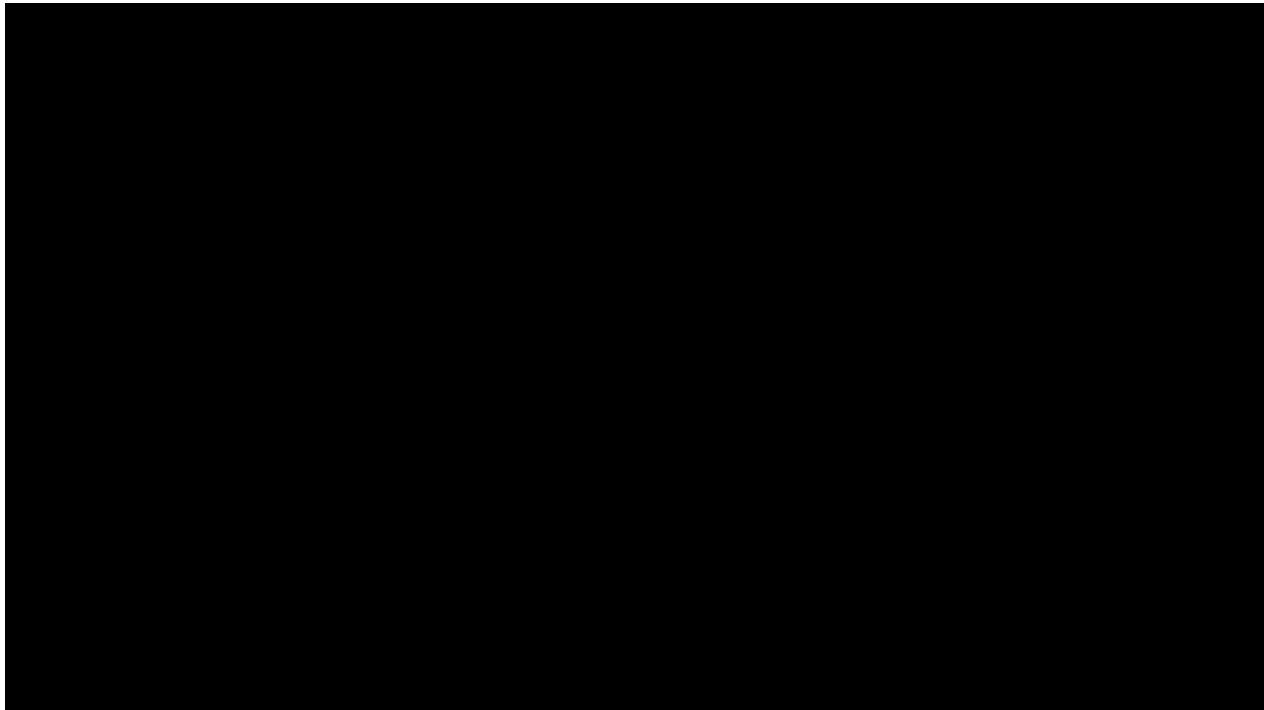
You need to enable JavaScript to run this app.

Casdoor 可为网页和应用程序用户的登录请求提供服务。

Casdoor 的特性：

1. Casdoor 遵循前后端分离架构，采用 Golang 进行开发。它支持高同步，提供基于网页的用户界面管理，并支持10多种语言的本地化。
2. Casdoor 支持第三方应用登录，如 GitHub、谷歌、QQ、微信等，并支持通过插件扩展第三方登录。
3. Casdoor 支持基于 [Cassbin](#) 的授权管理。它支持 ACL、RBAC、ABAC 和 RESTful鉴权管理模式。
4. Casdoor 提供了手机验证码、电子邮件验证码以及重置密码的功能。
5. Casdoor 支持日志的审计和记录。
6. Casdoor 可以使用阿里云、腾讯云、七牛云提供的图片CDN云存储功能。
7. Casdoor 允许自定义注册、登录以及找回密码页面。
8. 通过数据库同步支持与现有系统的集成，从而能够顺利过渡到 Casdoor。
9. Casdoor 支持主流数据库: MySQL、PostgreSQL、SQL Server 等, 并支持扩展插件以支持新的数据库。

它如何工作?



步骤0（前置知识）

1. Casdoor的授权程序基于OAuth 2.0协议。强烈建议简要了解下 OAuth 2.0 的运行原理。你可以通过此处了解 [OAuth 2.0 简介](#)。

Abstract Protocol Flow



步骤 1 (授权请求)

您的应用（或网站等）应该以 `endpoint/login/oauth/authorize?client_id=xxx&response_type=code&redirect_uri=xxx&scope=read&state=xxx` 这种格式来编写 URL。并使用你的 Casdoor 的网站 URL 替换 `endpoint`，以及使用您的信息替换 `xxx`。

ⓘ 提示

对于 `xxx` 的部分需要写上什么？

- 对于 `client_id`: 您可以在每个应用程序里找到它
- 对于 `redirect_uri`: 您应该将此设置为您自己的应用程序回调 URL。Casdoor 将使用此信息在授权后发送回响应。
- 对于 `state`: 您应该在此处填写您的应用程序名称。

应用程序将会提示用户：“嘿，我需要一些资源，且该资源需要您的许可我才能访问。您是否可以转到这个网址并为我输入您的用户名和密码？”

使用正确组合的 URL，应用就会向此 URL 发起请求，完成 授权请求。

步骤 2（授权认证）

这个步骤非常直接：用户将被重定向到在步骤1中组成的URL，用户将看到来自Casdoor的登录页面。通过在登录页面输入正确的用户名和认证信息，Casdoor现在能成功识别用户，将发送 code 和 status 返回第1步中设置的回调URL。

用户打开网址并向Casdoor提供凭据。Casdoor will say: "Looking good ~ this is the user (who is authorizing the Application to get the code and state) I know in my database, and I will send the code and state back to the Application using the callback URL (redirect_uri)".

将这两部分信息发送回您的应用程序后，应用程序将获得授权，Authorization Grant 完成。



提示

Casdoor也提供第三方登录。在这种情况下，你将看到的不是凭证输入页面，而是第三方提供商的列表。您可以使用这些提供商登录您的应用，Casdoor充当中间层（中间件）。

步骤 3（授权认证）

在这一步中，您的应用程序已经拥有了步骤2的代码，并且它将对Casdoor说：“嘿，用户同意给我 code。”你能验证这个 code 并给我 access_token 吗？”

步骤 4（访问令牌）

Casdoor对您的应用程序做出回应：“你知道吗，这段 code 看起来是合法的。”你必须是正确的应用程序。这是给你的 access_token。“有了这个 code，Casdoor确认它是一个被授权的应用程序（在步骤2中被正确的用户授权）试图获取 access_token（稍后将用于访问更多资源）。

步骤 5（访问令牌）

在这一步中，你的应用程序说：“很好！我刚刚得到了新鲜又美味的 access_token。现在我可以使用它从 Resource Server 获取更有价值的东西！”

您的应用程序然后转向 Resource Server，并说：“嘿，伙计，你能检查一下这个 access_token

吗? "我收到了来自Casdoor的它。您是否想要验证这是否是您发给Casdoor的正确令牌?"

步骤 6 (受保护资源)

Resource Server 对您的应用程序做出响应: "还不错。" 这看起来就像我发给Casdoor的那个, 而 Casdoor说, 持有这个 access_token 的人可以访问这些 Protected Resources。那就去吧, 拿起来吧! "

这基本上就是Casdoor如何与您的应用程序一起工作的。

① 提示

Casdoor可以同时充当 Authorization Server 和 Resource Server。换句话说, Casdoor 授权您的应用程序访问资源, 通常是当前登录用户的信息, 来自Casdoor的数据仓库。

在线演示

Casdoor

这里是一个由Casbin部署的在线演示。

- [Casdoor官方演示](#)

全局管理员登录:

- 用户名: `admin`
- 密码: `123`

Casbin-OA

Casbin-OA 是 Casbin 的 web 应用程序之一。它使用 Casdoor 进行身份验证。

- [Casbin-OA](#)
- 源码地址: <https://github.com/casbin/casbin-oa>

Casnnode

Casnnode 是由 Cassbin 社区开发的官方论坛。

它使用 Casdoor 作为认证平台并管理成员。

- [Casnnode](#)
- 源码地址: <https://github.com/casbin/casnnode>

结构

Casdoor 包括以下两部分:

名称	描述	语言	源代码
前端	Casdoor的前端 Web界面	JavaScript + React	https://github.com/casdoor/casdoor/tree/master/web
后端	Casdoor后端 RESTful API	Golang + Beego + SQL	https://github.com/casdoor/casdoor

核心概念

作为Casdoor的管理员，你至少应该熟悉四个核心概念：`Organization`, `User`, `Application`和`Provider`。

提示

在接下来的部分，我们将使用演示站点 <https://door.casdoor.com> 作为示例。

组织

在Casdoor中，组织是用户和应用程序的容器。例如，公司的所有员工或商业的所有客户都可以被抽象为一个组织。以下显示了`Organization`类的定义：

```
type Organization struct {
    Owner      string `xorm:"varchar(100) notnull pk" json:"owner"`
    Name       string `xorm:"varchar(100) notnull pk" json:"name"`
    CreatedTime string `xorm:"varchar(100)" json:"createdTime"`

    DisplayName     string `xorm:"varchar(100)" json:"displayName"`
    WebsiteUrl     string `xorm:"varchar(100)" json:"websiteUrl"`
    Favicon        string `xorm:"varchar(100)" json:"favicon"`
    PasswordType   string `xorm:"varchar(100)" json:"passwordType"`
    PasswordSalt   string `xorm:"varchar(100)" json:"passwordSalt"`
    PhonePrefix    string `xorm:"varchar(10)" json:"phonePrefix"`
    DefaultAvatar  string `xorm:"varchar(100)" json:"defaultAvatar"`
    Tags          []string `xorm:"mediumtext" json:"tags"`
    MasterPassword string `xorm:"varchar(100)" json:"masterPassword"`
    EnableSoftDeletion bool `json:"enableSoftDeletion"`
    IsProfilePublic bool `json:"isProfilePublic"`

    AccountItems []*AccountItem `xorm:"varchar(2000)" json:"accountItems"`
}
```

用户

在Casdoor中，用户可以登录到一个应用程序。每个用户只能属于一个组织，但可以登录该组织拥有的多个应用程序。目前，Casdoor中有两种类型的用户：

- `built-in` 组织用户，例如 `built-in/admin`：在Casdoor平台上拥有完全管理权限的全局管理员。
- 其他组织的用户，例如 `my-company/alice`：可以注册、登录、登出、更改自己的个人资料等的普通用户。

在Casdoor API中，用户通常被标识为`<organization_name>/<username>`。例如，Casdoor的默认管理员表示为`built-in/admin`。此外，`User`类定义包含一个`id`属性，这是一个像`d835a48f-2e88-4c1f-b907-60ac6b6c1b40`这样的UUID，可以被应用程序选择作为用户的ID。

提示

对于只针对一个组织的应用程序，为了简化，可以使用`<username>`代替`<organization_name>/<username>`作为应用程序中的用户ID。

这是`User`类的定义：

```
type User struct {
    Owner      string `xorm:"varchar(100) notnull pk" json:"owner"`
    Name       string `xorm:"varchar(100) notnull pk" json:"name"`
    CreatedTime string `xorm:"varchar(100)" json:"createdTime"
```



The `Properties` field is a flexible key-value map for storing custom user attributes. See the [User Properties documentation](#) for detailed usage examples and best practices.

应用程序

一个应用程序代表需要由Casdoor保护的网络服务，例如论坛网站，OA系统或CRM系统。

```
type Application struct {
    Owner          string      `xorm:"varchar(100) notnull pk" json:"owner"`
    Name           string      `xorm:"varchar(100) notnull pk" json:"name"`
    CreatedTime   string      `xorm:"varchar(100)" json:"createdTime"`
    DisplayName   string      `xorm:"varchar(100)" json:"displayName"`
    Logo           string      `xorm:"varchar(100)" json:"logo"`
    HomepageUrl  string      `xorm:"varchar(100)" json:"homepageUrl"`
    Description   string      `xorm:"varchar(100)" json:"description"`
    Organization  string      `xorm:"varchar(100)" json:"organization"`
    Cert          string      `xorm:"varchar(100)" json:"cert"`
    EnablePassword bool       `json:"enablePassword"`
    EnableSignUp  bool       `json:"enableSignUp"`
    EnableSigninSession bool     `json:"enableSigninSession"`
    EnableCodeSignin bool     `json:"enableCodeSignin"`
    Providers     []*ProviderItem `xorm:"mediumtext" json:"providers"`
    SignupItems   []*SignupItem  `xorm:"varchar(1000)" json:"signupItems"`
    OrganizationObj *Organization `xorm:"-"`
    ClientId      string      `xorm:"varchar(100)" json:"clientId"`
    ClientSecret   string      `xorm:"varchar(100)" json:"clientSecret"`
    RedirectUris  []string     `xorm:"varchar(1000)" json:"redirectUris"`
    TokenFormat   string      `xorm:"varchar(100)" json:"tokenFormat"`
    ExpireInHours int        `json:"expireInHours"`
    RefreshExpireInHours int        `json:"refreshExpireInHours"`
    SignupUrl     string      `xorm:"varchar(200)" json:"signupUrl"`
    SigninUrl     string      `xorm:"varchar(200)" json:"signinUrl"`
    ForgetUrl     string      `xorm:"varchar(200)" json:"forgetUrl"`
    AffiliationUrl string     `xorm:"varchar(100)" json:"affiliationUrl"`
    TermsOfUse     string      `xorm:"varchar(100)" json:"termsOfUse"`
    SignupHtml    string      `xorm:"mediumtext" json:"signupHtml"`
    SigninHtml    string      `xorm:"mediumtext" json:"signinHtml"`
}
```

每个应用程序都可以有自己定制的注册页面、登录页面等。根登录页面`/login`（例如，<https://door.casdoor.com/login>）是仅供Casdoor内置应用程序：`app-built-in`的登录页面。

应用程序是用户登录到Casdoor的“入口”或“界面”。用户必须通过一个应用程序的登录页面才能登录Casdoor。

应用程序	注册页面URL	登录页面URL
内置应用程序	https://door.casdoor.com/signup	https://door.casdoor.com/login
casnode 论坛系统	https://door.casdoor.com/signup/app-casnode	https://door.casdoor.com/login/oauth/authorize?client_id=014ae4bd048734ca2dea&response_type=code&redirect_uri=http://localhost:9000/callback&scope=read&state=casdoor
casbin 的OA系统	https://door.casdoor.com/signup/app-casbin-oa	https://door.casdoor.com/login/oauth/authorize?client_id=0ba528121ea87b3eb54d&response_type=code&redirect_uri=http://localhost:9000/callback&scope=read&state=casdoor

登录 URL

通过Casdoor内置的应用程序登录Casdoor非常简单；只需访问Casdoor服务器主页（例如，<https://door.casdoor.com> 用于演示站点）它将自动将您重定向到`/login`。但是你如何在前端和后端代码中获取其他应用程序的URLs呢？您可以手动连接字符串，或者调用Casdoor SDKs提供的一些实用函数来获取URL：

1. 手动连接字符串

- 注册页面URL
 - 注册指定的应用程序: `<your-casdoor-hostname>/signup/<your-application-name>`
 - 通过OAuth注册: `<your-casdoor-hostname>/signup/oauth/authorize?client_id=<client-id-for-your-application>&response_type=code&redirect_uri=<redirect-uri-for-your-application>&&scope=read&state=casdoor`
 - 自动注册: `<your-casdoor-hostname>/auto-signup/oauth/authorize?client_id=<client-id-for-your-application>&response_type=code&redirect_uri=<redirect-uri-for-your-application>&&scope=read&state=casdoor`
- 登录页面URL
 - 为指定的组织登录: `<your-casdoor-hostname>/login/<your-organization-name>`
 - 通过OAuth登录: `<your-casdoor-hostname>/login/oauth/authorize?client_id=<client-id-for-your-application>&response_type=code&redirect_uri=<redirect-uri-for-your-application>&&scope=read&state=casdoor`

2. 使用前端SDK（用于使用React, Vue或Angular的前端JavaScript代码）

`getSignupUrl()` 和 `getSigninUrl()`: [casdoor-js-sdk](#)

3. 使用后端SDK（用于Go, Java等后端代码）

`GetSignupUrl()` 和 `GetSigninUrl()`: [casdoor-go-sdk](#)

提供商

Casdoor是一个联合的单点登录系统，支持通过OIDC、OAuth和SAML的多个身份提供商。 Casdoor也可以通过电子邮件或短信向用户发送验证码或其他通知。 Casdoor 使用 `Provider` 的概念来管理所有这些第三方连接器。

可以在[provider/overview](#)找到Casdoor支持的所有提供商的列表。

```
type Provider struct {
    Owner      string `xorm:"varchar(100) notnull pk" json:"owner"`
    Name       string `xorm:"varchar(100) notnull pk" json:"name"`
    CreatedTime string `xorm:"varchar(100)" json:"createdTime"`

    DisplayName  string `xorm:"varchar(100)" json:"displayName"`
    Category    string `xorm:"varchar(100)" json:"category"`
    Type        string `xorm:"varchar(100)" json:"type"`
    Method      string `xorm:"varchar(100)" json:"method"`
    ClientId    string `xorm:"varchar(100)" json:"clientId"`
    ClientSecret string `xorm:"varchar(100)" json:"clientSecret"`
    ClientId2   string `xorm:"varchar(100)" json:"clientId2"`
    ClientSecret2 string `xorm:"varchar(100)" json:"clientSecret2"`

    Host     string `xorm:"varchar(100)" json:"host"`
    Port     int     `json:"port"`
    Title    string `xorm:"varchar(100)" json:"title"`
    Content  string `xorm:"varchar(1000)" json:"content"`

    RegionId   string `xorm:"varchar(100)" json:"regionId"`
    SignName    string `xorm:"varchar(100)" json:"signName"`
    TemplateCode string `xorm:"varchar(100)" json:"templateCode"`
    AppId      string `xorm:"varchar(100)" json:"appId"
```

Casdoor是如何自我管理的?

首次运行Casdoor时，会创建一些内置对象以方便其管理：

- 一个内置的命名为 `built-in` 的组织。
- `built-in` 组织下用户名为 `admin` 的用户。
- 一个名为 `app-built-in` 的内置应用，由 `built-in` 组织管理，代表Casdoor本身。

`built-in` 组织下的所有用户，包括 `admin`，都将在Casdoor平台上拥有完全的管理员权限。因此，如果有多个管理员，建议在 `built-in` 组织下创建新账户。或者，应关闭 `app-built-in` 应用程序的注册通道，以防止不必要的访问。

⚠ 注意事项

无法通过网页用户界面或RESTful API重命名或删除内置对象。Casdoor在许多地方硬编码了这些保留名称；尝试通过修改数据库来重命名或删除它们可能会导致整个系统崩溃。

服务器安装

安装要求

操作系统

所有主要的操作系统，包括Windows, Linux和macOS，都得到支持。

环境

- Go 1.21+
- Node.js LTS (20)
- Yarn 1.x

① 信息

我们强烈建议使用 [Yarn 1.x](#) 来运行和构建Casdoor前端。 使用NPM可能会导致界面样式问题。 欲了解更多详情，请见：[casdoor#294](#)。

⚠ 注意事项

如果您的网络无法直接同步Go依赖包，您需要配置GOPROXY环境变量。 我们强烈建议使用：
<https://goproxy.cn/>

数据库

Casdoor使用 [XORM](#) 与数据库进行交互。 Based on [Xorm Drivers Support](#), Casdoor currently provides support for the following databases:

- [MySQL](#)
- [MariaDB](#)
- [PostgreSQL](#)
- [CockroachDB](#)
- [SQL Server](#)
- [Oracle](#)
- [SQLite 3](#)

- TiDB

下载

Casdoor 的源代码托管在 GitHub: <https://github.com/casdoor/casdoor>。 转到后端代码和 React 前端代码都包含在一个仓库中。

名称	描述	语言	源代码
前端	Casdoor的网页前端界面	JavaScript + React	https://github.com/casdoor/casdoor/tree/master/web
后端	Casdoor的ResTful API 后端	Golang + Beego + XORM	https://github.com/casdoor/casdoor

Casdoor支持 Go Modules。要下载代码，只需使用git克隆代码：

```
cd /文件夹路径/  
git clone https://github.com/casdoor/casdoor
```

配置

配置数据库

Casdoor 支持MySQL、MSSQL、SQLite3和PostgreSQL。默认情况下，Casto使用MySQL。

MySQL

Casdoor将会把users, nodes和topics信息存储在一个名为casdoor的MySQL数据库中。如果数据库不存在，则需手动创建。可以在以下位置指定数据库连接字符串 <https://github.com/casdoor/blob/master/conf/app.conf>

```
driverName = mysql  
dataSourceName = root:123456@tcp(localhost:3306)/  
dbName = casdoor
```

PostgreSQL

在运行 Cassdoor 之前，您需要手动准备PostgreSQL 数据库，因为Castor 需要在使用 xorm 打开 Postgres 时指定一个数据库。

假设你已经准备好了个名为 casdoor 的数据库，你应该像这样指定 app.conf：

```
driverName = postgres
dataSourceName = user=postgres password=postgres host=localhost port=5432
sslmode=disable dbname=casdoor
dbName = casdoor
```

❗ 对于 POSTGRESQL，请确保 dataSourceName 有一个非空的 dbName，并且也在上面的示例中为 dbname 字段复制数据库名称。:::

CockroachDB

CockroachDB也可以与PostgreSQL驱动程序一起使用，并且配置与PostgreSQL相同。

```
driverName = postgres
dataSourceName = user=postgres password=postgres host=localhost port=5432
sslmode=disable dbname=casdoor serial_normalization=virtual_sequence
dbName = casdoor
```

SQLite3

要配置SQLite3，您应该像这样指定 app.conf：

```
driverName = sqlite
dataSourceName = file:casdoor.db?cache=shared
dbName = casdoor
```

通过 Ini 文件配置

Casdoor can be configured via a single file: [conf/app.conf](#). As a beginner, you only need to modify `driverName` and `dataSourceName` based on your database (see [Configure Database](#)). Below is a complete reference of all configuration options:

Parameter	Default Value	Description
<code>appname</code>	<code>casdoor</code>	Application name (currently has no practical use)
<code>httpport</code>	<code>8000</code>	Port that the backend application listens on
<code>runmode</code>	<code>dev</code>	Running mode: <code>dev</code> or <code>prod</code>
<code>copyrequestbody</code>	<code>true</code>	Whether to copy request body for later use
<code>driverName</code>	<code>mysql</code>	Database driver (e.g., <code>mysql</code> , <code>postgres</code> , <code>sqlite</code>). See Configure Database
<code>dataSourceName</code>	<code>root:123456@tcp(localhost:3306)/</code>	Database connection string. See Configure Database
<code>dbName</code>	<code>casdoor</code>	Database name used by Casdoor
<code>tableNamePrefix</code>	(empty)	Prefix for table names when using an adapter
<code>showSql</code>	<code>false</code>	Show SQL statements in logger when log level is greater than INFO
<code>redisEndpoint</code>	(empty)	Redis endpoint for session storage (e.g., <code>localhost:6379</code>). If empty, sessions are stored locally in <code>./tmp</code> . For password: <code>host:port,db,password</code>
<code>defaultStorageProvider</code>	(empty)	Default storage provider name for file uploads (e.g., <code>avatars</code>). See storage

Parameter	Default Value	Description
<code>isCloudIntranet</code>	<code>false</code>	Whether provider endpoints use intranet addresses
<code>authState</code>	<code>"casdoor"</code>	Authorization application name checked during login
<code>socks5Proxy</code>	<code>"127.0.0.1:10808"</code>	SOCKS5 proxy address for OAuth providers (Google, GitHub, etc.) that may be blocked
<code>verificationCodeTimeout</code>	<code>10</code>	Verification code expiration time in minutes
<code>initScore</code>	<code>0</code>	Initial score assigned to new users (used by Casnode, not Casdoor)
<code>logPostOnly</code>	<code>true</code>	Whether to log only POST requests
<code>isUsernameLowered</code>	<code>false</code>	Whether to convert usernames to lowercase
<code>origin</code>	(empty)	Backend origin URL (e.g., https://door.casdoor.com)
<code>originFrontend</code>	(empty)	Frontend origin URL if different from backend
<code>staticBaseUrl</code>	<code>"https://cdn.casbin.org"</code>	CDN URL for static assets used during database initialization
<code>isDemoMode</code>	<code>false</code>	Enable demo mode restrictions
<code>batchSize</code>	<code>100</code>	Batch size for bulk

Parameter	Default Value	Description
		operations
<code>enableErrorMask</code>	<code>false</code>	Whether to mask detailed error messages
<code>enableGzip</code>	<code>true</code>	Accept and respond with gzip encoding when client supports it
<code>inactiveTimeoutMinutes</code>	(empty)	Auto-logout timeout in minutes. Empty or ≤ 0 means no timeout
<code>ldapServerPort</code>	<code>389</code>	Port for LDAP server
<code>ldapsCertId</code>	<code>" "</code>	Certificate ID for LDAPS connections
<code>ldapsServerPort</code>	<code>636</code>	Port for LDAPS (LDAP over SSL) server
<code>radiusServerPort</code>	<code>1812</code>	Port for RADIUS server
<code>radiusDefaultOrganization</code>	<code>"built-in"</code>	Default organization for RADIUS authentication
<code>radiusSecret</code>	<code>"secret"</code>	Shared secret for RADIUS authentication
<code>quota</code>	<code>{"organization": -1, "user": -1, "application": -1, "provider": -1}</code>	Resource quotas (-1 means unlimited)
<code>logConfig</code>	<code>{"adapter": "file", "filename": "logs/casdoor.log", "maxdays": 99999, "perm": "0770"}</code>	Logging configuration (adapter, file path, rotation, permissions)
<code>initDataNewOnly</code>	<code>false</code>	Whether to initialize data

Parameter	Default Value	Description
		only for new installations
<code>initDataFile</code>	<code>"./init_data.json"</code>	Path to data initialization file. See Data Initialization
<code>frontendBaseDir</code>	<code>"../cc_0"</code>	Base directory for frontend files (only for development)

通过环境变量配置

Casdoor在上述ini文件中定义的所有配置项都可以通过环境变量进行配置，以及一些beego配置项（如`httpport`, `appname`）。

例如，当你尝试启动Casdoor时，你可以使用类似这样的方式通过环境变量传递配置：

```
appname=casbin go run main.go
```

此外，`export` 衍生品也是一种可能的方法。环境变量的名称应与您想在ini文件中使用的名称完全匹配。

注意：环境变量中的配置可以覆盖ini文件中的配置。

运行

目前有两种启动方法，您可以根据自己的情况选择一种。

开发模式

后端

Casdoor的Go后端默认在8000端口运行。您可以使用以下命令启动Go后端：

```
go run main.go
```

服务器成功运行后，您可以开始进行前端部分。

前端

Casdoor的前端是一个非常经典的[Create-React-App \(CRA\)](#)项目。 它默认在端口7001上运行。 使用以下命令来运行前端：

```
cd web  
yarn install  
yarn start
```

在您的浏览器中访问 <http://localhost:7001>。 使用默认的全局管理员账户：`built-in/admin` 登录Casdoor控制面板。

```
admin  
123
```

生产模式

后端

将Casdoor Go后端代码编译成可执行文件并启动它。

对于Linux：

```
go build  
./casdoor
```

适用于Windows：

```
go build  
casdoor.exe
```

前端

将Casdoor前端代码构建成静态资源（.html, .js, .css文件）：

```
cd web  
yarn install  
yarn build
```

在您的浏览器中访问 <http://localhost:8000>。 使用默认的全局管理员账户：`built-in/admin` 登录Casdoor控制面板。

板。

```
admin  
123
```

💡 提示

要使用另一个端口，请编辑 `conf/app.conf` 并修改 `httpport`，然后重新启动 Go 后端。

❗ CASDOOR 端口详情

在 `dev` 环境中，前端由 `yarn run` 在 7001 端口运行，所以如果你想要进入 Casdoor 登录页面，你需要将 Casdoor 链接设置为 <http://localhost:7001>。

在 `prod` 环境中，前端文件首先由 `yarn build` 构建，并在 8000 端口上提供服务，因此，如果你想要进入 Casdoor 登录页面，你需要将 Casdoor 链接设置为 <https://your-casdoor-url.com:8000>（如果你正在使用反向代理，你需要将链接设置为你的域名）。

以我们的官方论坛 Casnode 为例

[Casnode](#) 使用 Casdoor 处理身份验证。

当我们在 `dev` 环境中测试 Casnode 时，我们将 `serverUrl` 设置为 <http://localhost:7001>，所以当我们使用 Casdoor 测试登录和注册功能时，它将会跳转到 `localhost 7001`，这是 Casdoor 的端口。

当我们把 Casnode 放入生产环境时，我们将 `serverUrl` 设置为 <https://door.casbin.com>，所以用户可以使用 Casdoor 登录或注册。

```
4 import * as ConfBackend from "./backend/ConfBackend.js"  
5  
6 export const authConfig = {  
7   // serverUrl: "https://door.casbin.com",  
8   serverUrl: "http://localhost:7001",  
9   clientId: "014ae4bd048734ca2dea",  
  ...
```



> 基础知识

> (可选) 使用 Docker 运行

(可选) 使用 Docker 运行

安装要求

硬件

如果你想自己构建Docker镜像，请确保你的机器至少有**2GB**的内存。Casdoor的前端是一个React的NPM项目。构建前端至少需要 **2GB** 的内存。内存少于**2GB**可能会导致前端构建失败。

如果您只需要运行预构建的镜像，请确保您的机器至少有**100MB**的内存。

操作系统

所有操作系统（Linux, Windows和macOS）都受到支持。

Docker

您可以在 Linux 中使用 Docker (docker-engine 版本 ≥ 17.05)，或在 Windows 和 macOS 中使用 Docker Desktop。

- [Docker](#)

无论操作系统如何，用户必须确保他们拥有**docker-engine**版本 ≥ 17.05 。这是因为我们在**docker-compose.yml**中使用了多阶段构建功能，该功能在**17.05**及以上版本中得到支持。有关更多信息，请参见<https://docs.docker.com/develop/develop-images/multistage-build/>。

如果您也在使用**docker-compose**，请确保您有**docker-compose**版本 ≥ 2.2 。对于

Linux用户，您还需要确保已安装docker-compose，因为它与docker-engine是分开的。

获取镜像

我们提供了两个DockerHub 镜像：

名称	描述	建议
casdoor-all-in-one	镜像中包含了Casdoor和MySQL数据库	此图像已包含一个玩具数据库，仅用于测试目的
casdoor	只有Casdoor被包含在图像中	此图像可以连接到您自己的数据库，并在生产中使用

1. [casbin/casdoor-all-in-one](#): 这个镜像包含了casdoor二进制文件，一个MySQL数据库，以及所有必要的配置。这是为了希望快速尝试Casdoor的新用户而设计的。有了这个镜像，您只需一两个命令就可以立即启动Casdoor，无需任何复杂的配置。然而，请注意，我们不建议在生产环境中使用此图像。

选项 1: 使用示例数据库

运行容器，并将8000端口暴露给主机。如果本地主机上不存在该图像，系统将会自动拉取。

```
docker run -p 8000:8000 casbin/casdoor-all-in-one
```

在您的浏览器中访问<http://localhost:8000>。使用默认的全局管理员账户：[built-in/admin](#)登录Casdoor控制面板

```
admin  
123
```

选项-2：尝试直接使用标准图像

💡 提示

如果将配置文件挂载到容器不方便，使用环境变量也是一种可能的解决方案。

example

```
docker run \  
  -e driverName=mysql \  
  -e dataSourceName='user:password@tcp(x.x.x.x:3306)/*' \  
  -p 8000:8000 \  
  casbin/casdoor:latest
```

创建 `conf/app.conf`。您可以从 Casdoor 的 `conf/app.conf` 中复制它。`
有关 `app.conf`` 的更多详细信息

然后运行

```
docker run -p 8000:8000 -v /folder/of/app.conf:/conf casbin/  
casdoor:latest
```

ⓘ 备注

The default user of Casdoor has a uid and gid of 1000. When using volume mapping with SQLite (or any storage requiring file permissions), ensure that

the path (e.g., `/folder/of/app.conf` in the example above) is accessible to uid 1000. This avoids permission errors like `permission denied` when Casdoor writes to mapped volumes.

无论如何，只需将 `app.conf` 挂载到 `/conf/app.conf`，然后启动容器。

在您的浏览器中访问 <http://localhost:8000>。使用默认的全局管理员账户：`built-in/admin` 登录Casdoor控制面板

```
admin  
123
```

选项-3：尝试使用docker-compose

在与 `docker-compose.yml` 文件相同的目录级别中创建一个 `conf/app.conf` 目录。然后，从Casdoor复制`app.conf`。有关 `app.conf` 的更多详细信息，您可以查看[通过Ini文件](#)。

使用docker-compose创建一个单独的数据库：

```
docker-compose up
```

这样就完成了！ 

在您的浏览器中访问 <http://localhost:8000>。使用默认的全局管理员账户：`built-in/admin` 登录Casdoor控制面板

```
admin  
123
```

ⓘ 备注

如果你深入研究docker-compose.yml文件，我们创建的名为“RUNNING_IN_DOCKER”的环境变量可能会让你感到困惑。当通过docker-compose创建数据库'db'时，它在你的PC的localhost上可用，但不在Casdoor容器的localhost上可用。为了防止您因修改app.conf而遇到麻烦，这对新用户来说可能相当困难，我们提供了这个环境变量，并在docker-compose.yml中预先分配了它。当此环境变量设置为true时，localhost将被替换为host.docker.internal，以便Casdoor可以访问数据库。

(可选) 尝试使用 K8s Helm

介绍

现在我们展示如何使用 Helm 在 Kubernetes 上部署 Casdoor，以便于管理和扩展。

先决条件

- 一个正在运行的 Kubernetes 集群
- 已安装 Helm v3

安装步骤

步骤 1：安装 Casdoor 图表

Install the Casdoor chart:

```
helm install casdoor oci://registry-1.docker.io/casbin/casdoor-helm-charts --version v1.702.0
```

步骤 2：访问 Casdoor

一旦安装，您可以通过 Kubernetes 集群提供的服务 URL 访问 Casdoor。

定制和配置

通过修改 Helm 图表值来定制您的 Casdoor 安装。有关详细选项，请参考图表中的 `values.yaml` 文件。可以配置以下参数。

参数	描述	默认值
<code>replicaCount</code>	运行 Casdoor 应用的副本数量。	1
<code>image.repository</code>	Casdoor Docker 图像的仓库。	casbin

参数	描述	默认值
<code>image.name</code>	Casdoor Docker 图像的名称。	<code>casdoor</code>
<code>image.pullPolicy</code>	Casdoor Docker 图像的拉取策略。	<code>IfNotPresent</code>
<code>image.tag</code>	Casdoor Docker 图像的标签。	<code>""</code>
<code>config</code>	Casdoor 应用的配置设置。	参见 <code>config</code> 字段
<code>database.driver</code>	要使用的数据库驱动程序（支持 mysql, postgres, cockroachdb, sqlite3）。	<code>sqlite3</code>
<code>database.user</code>	数据库用户名。	<code>""</code>
<code>database.password</code>	数据库密码。	<code>""</code>
<code>database.host</code>	数据库主机。	<code>""</code>
<code>database.port</code>	数据库端口。	<code>""</code>
<code>database.databaseName</code>	Casdoor 使用的数据库名称。	<code>casdoor</code>
<code>database.sslMode</code>	数据库连接的 SSL 模式。	<code>disable</code>
<code>service.type</code>	为 Casdoor 创建的 Kubernetes 服务的类型 (ClusterIP, NodePort,	<code>ClusterIP</code>

参数	描述	默认值
	LoadBalancer 等)。	
<code>service.port</code>	Casdoor 服务的端口号。	8000
<code>ingress.enabled</code>	是否启用 Casdoor 的 Ingress。	false
<code>ingress.annotations</code>	Ingress 资源的注解。	{}
<code>ingress.hosts</code>	Ingress 资源的主机名。	[]
<code>resources</code>	Casdoor 容器的资源请求和限制。	{}
<code>autoscaling.enabled</code>	是否启用 Casdoor 的水平 Pod 自动扩展。	false
<code>autoscaling.minReplicas</code>	水平 Pod 自动扩展的最小副本数。	1
<code>autoscaling.maxReplicas</code>	水平 Pod 自动扩展的最大副本数。	100
<code>autoscaling.targetCPUUtilizationPercentage</code>	水平 Pod 自动扩展的目标 CPU 利用率百分比。	80
<code>nodeSelector</code>	Pod 分配的节点标签。	{}
<code>tolerations</code>	Pod 分配的容忍	[]

参数	描述	默认值
	标签。	
<code>affinity</code>	Pod 分配的亲和性设置。	<code>{}</code>
<code>extraContainersEnabled</code>	是否启用额外的边车容器。	<code>false</code>
<code>extraContainers</code>	额外的边车容器。	<code>[]</code>
<code>extraVolumeMounts</code>	Casdoor 容器的额外卷挂载。	<code>[]</code>
<code>extraVolumes</code>	Casdoor 容器的额外卷。	<code>[]</code>
<code>envFromSecret</code>	从 secret 提供环境变量。	<code>[{name:"", secretName:"", key:""}]</code>
<code>envFromConfigmap</code>	从 configmap 提供环境变量。	<code>[{name:"", configmapName:"", key:""}]</code>
<code>envFrom</code>	从整个 secret 或 configmap 提供环境变量。	<code>`[{name:"", type:"configmap \</code>

管理部署

升级您的 Casdoor 部署：

```
helm upgrade casdoor casdoor/casdoor-helm-charts
```

卸载 Casdoor：

```
helm delete casdoor
```

有关进一步的管理和定制，请参考 Helm 和 Kubernetes 的文档。

结论

使用 Helm 在 Kubernetes 上部署 Casdoor 简化了在 Kubernetes 环境中管理和扩展您的身份验证服务。

Casdoor 公共 API

Casdoor 前端网页用户界面是一个用 React 开发的SPA（单页应用程序）。React前端使用了Go后端代码暴露的Casdoor RESTful API。这个RESTful API被称为Casdoor Public API。换句话说，通过HTTP调用，你可以像Casdoor网页界面本身一样做任何事情。没有其他限制。以下人员可以利用该API：

- Casdoor的前端
- Casdoor 客户端 SDK（例如，casdoor-go-sdk）
- 来自应用程序一侧的任何其他自定义代码

Casdoor Public API 的完整参考可以在Swagger上找到：<https://door.casdoor.com/swagger>。这些Swagger文档是使用Beego的Bee工具自动生成的。如果你想要自己生成Swagger文档，请参见：[如何生成swagger文件](#)

API Response Language

Casdoor APIs support internationalized responses. The default response language is English. To receive error messages and other text content in your preferred language, include the `Accept-Language` header in your API requests:

```
# Example: Get error messages in French
curl -X GET https://door.casdoor.com/api/get-account \
-H "Authorization: Bearer YOUR_ACCESS_TOKEN" \
-H "Accept-Language: fr"
```

Supported language codes include `en`, `zh`, `es`, `fr`, `de`, `ja`, `ko`, and more. For a complete list and more details, see the [Internationalization](#) documentation.

Machine-to-Machine (M2M) Authentication

Machine-to-machine (M2M) authentication is designed for scenarios where services, applications, or backend systems need to authenticate and communicate with APIs **without user interaction**. This is particularly useful for:

- Backend services calling Casdoor APIs programmatically
- CLI tools that need to interact with your APIs using access tokens
- B2B enterprise scenarios where organizations need to generate tokens for API access (e.g., admin tokens for management operations, read tokens for data access)
- Automated processes such as scheduled jobs, data synchronization, or system integrations
- Microservices that need to authenticate with each other

Casdoor supports M2M authentication through the following methods:

1. **Client Credentials Grant (OAuth 2.0)**: The recommended approach for M2M scenarios. This uses the [Client Credentials Grant flow](#) where applications authenticate using their `Client ID` and `Client Secret` to obtain access tokens. See the [OAuth Client Credentials Grant](#) documentation for details on obtaining tokens via this flow.
2. **Direct API Authentication with Client ID and Secret**: Use the application's credentials directly in API calls (see method #2 below).

Use Cases for M2M Authentication

- **Organization-level API access**: In B2B scenarios, you can create a Casdoor application for each organization. The application's client credentials provide admin-level permissions for that organization, enabling them to manage their users, generate tokens, and access organizational resources independently.
- **Token generation for downstream services**: Generate access tokens programmatically (using Client Credentials Grant) that can be distributed to CLI tools, read-only services, or other applications that need scoped access to your APIs.
- **Service-to-service authentication**: Backend services can authenticate as an "application" rather than as a user, with permissions equivalent to the organization admin.

如何使用[Casdoor Public API](#)进行身份验证

1. 通过[Access token](#)

我们可以使用为经过身份验证的用户授予的访问令牌，以用户自身的身份调用[Casdoor Public API](#)。

如何获取访问令牌？

应用程序可以在OAuth登录过程结束时（也就是通过代码和状态获取令牌）获取Casdoor用户的访问令牌。API调用的权限将与用户的权限相同。

以下示例展示了如何通过casdoor-go-sdk在Go中调用[GetOAuthToken\(\)](#)函数。

```
func (c *ApiController) Signin() {
    code := c.Input().Get("code")
    state := c.Input().Get("state")

    token, err := casdoorsdk.GetOAuthToken(code, state)
    if err != nil {
        c.ResponseError(err.Error())
        return
    }
}
```

所有授予的访问令牌也可以通过管理员用户在Tokens页面上的web UI进行访问。例如，访问：<https://door.casdoor.com/tokens> 以查看演示站点。

如何进行身份验证？

1. HTTP `GET` 参数，其URL格式为：

```
/page?access_token=<访问令牌>
```

演示站点示例： https://door.casdoor.com/api/get-global-providers?access_token=eyJhbGciOiJSUzI1NiIs

2. HTTP Bearer令牌，HTTP头格式是：

```
Authorization: Bearer <访问令牌>
```

2. By `client ID` and `client secret` (Machine-to-Machine)

This method is the primary approach for machine-to-machine (M2M) authentication. It allows applications, services, or backend systems to authenticate with Casdoor APIs without any user interaction.

如何获取客户端ID和密钥？

应用程序编辑页面（例如，<https://door.casdoor.com/applications/casbin/app-vue-python-example>）将显示应用程序的客户端ID和密钥。This authentication method is useful when you want to call the API as a "machine", "application", or a "service" instead of a user. The permissions for the API calls will be the same as the application (equivalent to the admin of the organization).

Use cases

- **Service authentication:** Backend services calling Casdoor APIs programmatically
- **Organization management:** In B2B scenarios, create an application per organization to enable them to manage users and generate tokens independently
- **Token generation:** Obtain access tokens via the [OAuth Client Credentials Grant](#) flow for distribution to CLI tools or other services

如何进行身份验证？

1. HTTP `GET` 参数，其URL格式为：

```
/page?clientId=<客户端ID>&clientSecret=<客户端密钥>
```

演示站点示例： https://door.casdoor.com/api/get-global-providers?access_token=eyJhbGciOiJSUzI1NiIs

```
providers?clientId=294b09fbc17f95daf2fe&clientSecret=dd8982f7046ccba1bbd7851d5c1ece4e52bf039d
```

2. HTTP 基本认证，其HTTP头格式为：

```
Authorization: Basic <客户端ID和客户端密钥以单个冒号":"连接的Base64编码>
```

如果你不熟悉Base64编码，你可以使用一个库来完成这个任务，因为[HTTP Basic Authentication](#)是一个被许多地方支持的流行标准。

Obtaining access tokens with Client Credentials

For machine-to-machine scenarios where you need to obtain an access token (rather than using client credentials directly), use the OAuth 2.0 Client Credentials Grant flow:

1. Make a POST request to https://<CASDOOR_HOST>/api/login/oauth/access_token with:

```
{  
  "grant_type": "client_credentials",  
  "client_id": "YOUR_CLIENT_ID",  
  "client_secret": "YOUR_CLIENT_SECRET"  
}
```

2. You will receive an access token response:

```
{  
  "access_token": "eyJhb... ",  
  "token_type": "Bearer",  
  "expires_in": 10080,  
  "scope": "openid"  
}
```

3. Use the `access_token` to call Casdoor APIs (see method #1 above).

For more details, see the [Client Credentials Grant](#) documentation.

(!) 信息

For B2B Enterprises: You can create separate Casdoor applications for each of your customer organizations. Each application has its own `client_id` and `client_secret`, which your customers can use to:

- Authenticate as their organization (with admin privileges)
- Generate access tokens for their users or services

- Manage their organization's users and permissions independently
- Integrate your APIs into their systems without UI-based login flows

This approach allows you to delegate organization management to your customers while maintaining security and isolation between different organizations.

3. 通过 Access key 和 Access secret

我们可以使用Casdoor用户的访问密钥和访问秘密来调用 Casdoor Public API 作为用户本身。访问密钥和访问秘密可以由管理员或用户本人在用户设置页面中配置。 update-user API 也可以被调用来更新这些字段。API 调用的权限将与用户的权限相同。

如何进行身份验证？

1. 在账户设置页面中创建一对 accessKey 和 accessSecret。
2. HTTP GET 参数，其URL格式为：

```
/page?accessKey=<The user's access key>&accessSecret=<the user's access secret>"
```

演示站点示例：<https://door.casdoor.com/api/get-global-providers?accessKey=b86db9dc-6bd7-4997-935c-af480dd2c796/admin&accessSecret=79911517-fc36-4093-b115-65a9741f6b14>

API key ② :

Access key ② :	b86db9dc-6bd7-4997-935c-af480dd2c796
Access secret ② :	79911517-fc36-4093-b115-65a9741f6b14
:	

```
curl --location 'http://door.casdoor.com/api/user?accessKey=b86db9dc-6bd7-4997-935c-af480dd2c796&accessSecret=79911517-fc36-4093-b115-65a9741f6b14'
```

4. 通过 username 和 password

⚠ 注意事项

这种认证方法并不安全，仅为了兼容性或演示目的而保留在此。我们建议使用前三种身份验证方法。

会发生什么？

用户凭证将会以 `GET` 参数的形式在请求URL中暴露出来。此外，如果你使用的是HTTP而不是HTTPS，用户的凭证将被网络以明文形式嗅探。

我们可以使用Casdoor用户的用户名和密码来以用户自身的身份调用 `Casdoor Public API`。用户名采用的格式为 `<用户的组织名称>/<用户名>`。API调用的权限将与用户相同。

如何进行身份验证？

1. HTTP `GET` 参数，URL格式为：

```
/page?username=<用户的组织名称>/<用户名>&password=<用户的密码>"
```

演示站点示例：`https://door.casdoor.com/api/get-global-providers?username=built-in/admin&password=123`

SSO Logout

The SSO logout endpoint `/api/sso-logout` allows you to log out a user from all applications in an organization simultaneously. When called, this endpoint will:

- Delete all active sessions for the user across all applications
- Expire all access tokens issued to the user
- Clear the current session and token

This is particularly useful when you need to ensure a user is completely logged out from all services, such as during security incidents or when implementing organization-wide logout policies.

Endpoint

```
GET or POST /api/sso-logout
```

Authentication

This endpoint requires the user to be authenticated. You can use any of the authentication methods described in the [How to authenticate](#) section above.

Example Request

```
# Using access token
curl -X POST https://door.casdoor.com/api/sso-logout \
-H "Authorization: Bearer YOUR_ACCESS_TOKEN"

# Using session cookie
curl -X POST https://door.casdoor.com/api/sso-logout \
--cookie "casdoor_session_id=abc123def456"
```

Response

```
{
  "status": "ok",
  "msg": "",
  "data": ""
}
```

CORS (Cross-Origin Resource Sharing)

Casdoor implements flexible CORS handling to allow secure cross-origin API requests. The server validates the `Origin` header and returns appropriate `Access-Control-Allow-Origin` headers based on the following rules:

Allowed origins:

- Origins matching your application's `redirect URIs` (configured in the application settings)
- Origins matching the Casdoor server's own hostname
- The configured origin in Casdoor's settings
- Special endpoint exceptions: requests to `/api/login/oauth/access_token` and `/api/userinfo` endpoints, and requests with origin `appleid.apple.com`

How it works:

When you make a cross-origin API request, Casdoor validates the origin through multiple checks: localhost/intranet addresses, matching redirect URIs in any application, matching the server's hostname, or configured origins. If any validation passes, the server includes CORS headers in the response allowing the request. For preflight `OPTIONS` requests, Casdoor returns appropriate headers including allowed methods (`POST`, `GET`, `OPTIONS`, `DELETE`) and credentials support.

Configuration:

To enable CORS for your application, add your frontend's origin to the application's `Redirect URIs` in the Casdoor admin panel. This allows your application to make authenticated API calls from the browser.

教程

产品文档

产品	技术	文档
Dashboard of PingCAP TiDB	React + TypeScript + Go + Gin	Use Casdoor for TiDB Dashboard SSO sign-in (other languages: Chinese)
GitLab	Vue + Ruby + Rails	OpenID Connect OmniAuth provider
Apache Shenyu	Java	Casdoor Plugin (other languages: Chinese)
Alist	TypeScript + SolidJS + Go + Gin	Casdoor SSO (other languages: Chinese)
BookStack	jQuery + Bootstrap + Go + Beego	Casdoor integrates registration and login

文章

技术	语言	标题
ASP.NET Core 6	英语	使用本地Casdoor Docker容器在Linux的Windows子系统上进行ASP.NET Core .NET 6演示身份验证项目
OAuth2 Proxy (Go)	中文	Use Casdoor + OAuth-Proxy to protect web applications on public networks
Casnnode (JavaScript + React + Go + Beego)	中文	使用Lighthouse设置一个像V2ex一样的论坛
Cloudreve (Go)	中文	Modify Cloudreve to support Casdoor
KodExplorer (PHP)	中文	Modify KodExplorer to support Casdoor



>

Deployment

Deployment



Deploying to Docker

Deploying Casdoor with Docker



部署到NGINX

使用Nginx反向代理您的后端Go程序，并快速启动Casdoor服务。



部署到 Kubernetes

学习如何在 Kubernetes 集群中部署 Casdoor



数据初始化

如何从文件初始化Casdoor 数据

在CDN中托管静态文件

在CDN中托管前端静态文件

在内部网络中托管静态文件

如何部署Casdoor静态资源

数据库迁移

处理Casdoor中的数据库迁移

Deploying to Docker

In this chapter, you will learn how to deploy Casdoor using Docker and Docker Compose with various reverse proxy configurations.

Prerequisites

Before starting, ensure you have:

- Docker installed on your system
- Docker Compose installed (for compose method)
- A domain name pointing to your server (for reverse proxy configurations)

Docker Deployment Methods

Choose your preferred deployment method:

[Docker Compose](#) [Docker Run](#)

Using Docker Compose

Create a `docker-compose.yml` file:

```
services:  
  casdoor:  
    image: casbin/casdoor:latest  
    container_name: casdoor  
    restart: unless-stopped
```

Start the service:

```
docker-compose up -d
```

Using Docker Run

Run Casdoor directly with Docker:

```
docker run -d \
--name casdoor \
--restart unless-stopped \
-p 8000:8000 \
-v $(pwd)/conf:/conf \
-v $(pwd)/logs:/logs \
-e GIN_MODE=release \
casbin/casdoor:latest
```

Reverse Proxy Configuration

For production deployments, it's recommended to use a reverse proxy with TLS certificates. Choose your preferred reverse proxy:

[Traefik \(Labels\)](#) [Traefik \(Dynamic\)](#) [Nginx](#) [Caddy](#)

Traefik with Docker Labels

Create a `docker-compose.yml` with Traefik labels:

```
services:
  traefik:
    image: traefik:v2.10
    container_name: traefik
```

Create the acme.json file:

```
touch traefik/acme.json
chmod 600 traefik/acme.json
```

Traefik with Dynamic Configuration

Create a `docker-compose.yml` with dynamic configuration:

```
services:
  traefik:
    image: traefik:v2.10
    container_name: traefik
    restart: unless-stopped
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock:ro
      - ./traefik/acme.json:/acme.json
      - ./traefik/traefik.yml:/etc/traefik/traefik.yml
      - ./traefik/dynamic.yml:/etc/traefik/dynamic.yml
    command:
      - --configfile=/etc/traefik/traefik.yml
  networks:
    - casdoor-network

  casdoor:
    image: casbin/casdoor:latest
    container_name: casdoor
    restart: unless-stopped
    environment:
      - GIN_MODE=release
    volumes:
      - ./conf:/conf
      - ./logs:/logs
    networks:
```

Create `traefik/traefik.yml`:

```
api:
  dashboard: true

entryPoints:
  web:
    address: ":80"
    http:
      redirections:
        entrypoint:
          to: websecure
          scheme: https
  websecure:
    address: ":443"

providers:
  docker:
    endpoint: "unix:///var/run/docker.sock"
    exposedByDefault: false
  file:
    directory: /etc/traefik
    watch: true

certificatesResolvers:
  letsencrypt:
    acme:
      email: your-email@example.com
      storage: /acme.json
      httpChallenge:
        entryPoint: web
```

Create `traefik/dynamic.yml`:

```
http:
  routers:
```

Nginx with Let's Encrypt

Create a `docker-compose.yml` with Nginx:

```
services:  
  nginx:  
    image: nginx:alpine  
    container_name: nginx  
    restart: unless-stopped  
    ports:  
      - "80:80"  
      - "443:443"  
    volumes:  
      - ./nginx/nginx.conf:/etc/nginx/nginx.conf  
      - ./nginx/conf.d:/etc/nginx/conf.d  
      - ./certbot/conf:/etc/letsencrypt  
      - ./certbot/www:/var/www/certbot  
    depends_on:  
      - casdoor  
  networks:  
    - casdoor-network  
  
  certbot:  
    image: certbot/certbot  
    container_name: certbot  
    volumes:  
      - ./certbot/conf:/etc/letsencrypt  
      - ./certbot/www:/var/www/certbot  
    command: certonly --webroot --webroot-path=/var/www/certbot  
    --email your-email@example.com --agree-tos --no-eff-email -d  
    your-domain.com  
  
  casdoor:  
    image: casbin/casdoor:latest  
    container_name: casdoor  
    restart: unless-stopped  
    environment:  
      - GIN_MODE=release
```

Create `nginx/conf.d/default.conf`:

```
server {
    listen 80;
    server_name your-domain.com;

    location /.well-known/acme-challenge/ {
        root /var/www/certbot;
    }

    location / {
        return 301 https://$host$request_uri;
    }
}

server {
    listen 443 ssl;
    server_name your-domain.com;

    ssl_certificate /etc/letsencrypt/live/your-domain.com/
fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/your-domain.com/
privkey.pem;

    location / {
        proxy_pass http://casdoor:8000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

Initialize SSL certificates:

```
# Create directories
```

Caddy with Automatic HTTPS

Create a `docker-compose.yml` with Caddy:

```
services:
  caddy:
    image: caddy:2-alpine
    container_name: caddy
    restart: unless-stopped
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - ./caddy/Caddyfile:/etc/caddy/Caddyfile
      - caddy_data:/data
      - caddy_config:/config
    depends_on:
      - casdoor
  networks:
    - casdoor-network

  casdoor:
    image: casbin/casdoor:latest
    container_name: casdoor
    restart: unless-stopped
    environment:
      - GIN_MODE=release
    volumes:
      - ./conf:/conf
      - ./logs:/logs
    networks:
      - casdoor-network

  volumes:
    caddy_data:
    caddy_config:

  networks:
```

Create `caddy/Caddyfile`:

```
your-domain.com {
    reverse_proxy casdoor:8000 {
        header_up Host {host}
        header_up X-Real-IP {remote}
        header_up X-Forwarded-For {remote}
        header_up X-Forwarded-Proto {scheme}
    }
}
```

Configuration

Create the necessary configuration directories

```
mkdir -p conf logs
```

Download the Casdoor configuration files

```
wget https://raw.githubusercontent.com/casdoor/casdoor/master/conf/
app.conf -O conf/app.conf
wget https://raw.githubusercontent.com/casdoor/casdoor/master/
init_data.json.template -O conf/init_data.json
```

Edit `conf/app.conf` to match your environment settings

ⓘ 备注

The default user of Casdoor has a uid and gid of 1000. When using volume

mapping with SQLite (or any storage requiring file permissions), ensure that the path (e.g., `/folder/of/app.conf` in the example above) is accessible to uid 1000. This avoids permission errors like `permission denied` when Casdoor writes to mapped volumes.

Testing

After deployment, visit your domain in your browser:

- Docker Run/Compose only: `http://your-server-ip:8000`
- With Reverse Proxy: `https://your-domain.com`

Troubleshooting

Check container logs

```
# For docker-compose
docker-compose logs casdoor

# For docker run
docker logs casdoor
```

Verify reverse proxy configuration

```
# Check if containers are running
docker ps

# Test connectivity
curl -I http://localhost:8000
```

SSL Certificate Issues

- Ensure your domain points to the correct server IP
- Check that ports 80 and 443 are open in your firewall
- Verify DNS propagation with `nslookup your-domain.com`

部署到NGINX

尽管Casdoor遵循前后端分离的架构，但在生产环境中，后端程序仍为前端文件提供静态文件服务。因此，您可以使用像[Nginx](#)这样的反向代理软件来代理Casdoor域的所有流量，并将其重定向到后端Go程序监视的端口。

在本章中，您将学习如何使用Nginx反向代理您的后端Go程序，并快速启动Casdoor服务。

1. 构建前端静态文件

假设您已经下载了Casdoor并完成了必要的配置（如果没有，请参考[开始部分](#)），您只需要按照以下方式构建静态文件：

[Yarn](#) [npm](#)

```
yarn install && yarn run build
```

```
npm install && npm run build
```

2. 运行后端程序

```
go run main.go
```

或者，先构建它：

```
go build && ./main
```

3. 配置并运行Nginx

```
vim /path/to/nginx/nginx.conf
```

然后，添加一个服务器：

```
server {
    listen 80;
    server_name YOUR_DOMAIN_NAME;
    location / {
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_redirect off;
        proxy_pass http://127.0.0.1:8000;
    }
}
```

接下来，重启你的Nginx进程。运行：

```
nginx -s reload
```

4. 测试

在你最喜欢的浏览器中访问 `http://YOUR_DOMAIN_NAME`。

部署到 Kubernetes

在 Kubernetes (k8s) 中部署 Casdoor

我们提供了一个在 Kubernetes 集群中部署 Casdoor 的基本示例。在 Casdoor 的根文件夹中，你会找到一个名为 "k8s.yaml" 的文件。此文件包含了在 Kubernetes 中部署 Casdoor 的示例配置，包括一个部署和一个服务。

在开始部署之前，请确保你已经修改了 `conf/app.conf` 文件，以便 Casdoor 可以成功连接到数据库，并且数据库本身正在运行。另外，请确保 Kubernetes 能够拉取必要的镜像。

要部署 Casdoor，请运行以下命令：

```
kubectl apply -f k8s.yaml
```

你可以通过运行 `kubectl get pods` 命令来检查部署状态。

这是 `k8s.yaml` 的内容：

```
# this is only an EXAMPLE of deploying casddor in kubernetes
# please modify this file according to your requirements
apiVersion: v1
kind: Service
metadata:
  #EDIT IT: if you don't want to run casdoor in default namespace,
  #please modify this field
  #namespace: casdoor
  name: casdoor-svc
```

请注意，这个文件只是一个示例。你可以根据你的需求进行各种修改，例如使用不同的命名空间、服务类型，或者使用 ConfigMap 来挂载配置文件。在 Kubernetes 中，使用 ConfigMap 挂载配置文件是生产环境中推荐的方法。

数据初始化

如果你正在将Casdoor与其他服务一起部署为一个完整的应用，你可能希望为用户提供一个开箱即用的功能。这意味着用户可以直接使用应用程序，无需任何配置。

在这种情况下，您可以使用数据初始化通过配置文件在Casdoor中注册您的服务。此文件可以预先定义，或由您自己的服务动态生成。

这里提供一个导入或导出配置数据的教程。

导入配置数据

By default, if there is a configuration file named `init_data.json` at the root directory of Casdoor, it will be used to initialize data in Casdoor. You can also specify a custom path for the initialization file by setting the `initDataFile` parameter in `conf/app.conf`:

```
initDataFile = /path/to/your/init_data.json
```

If no custom path is specified, Casdoor will look for `init_data.json` in the root directory where Casdoor runs.

如果您正在使用Casdoor的官方Docker镜像，这里有一些脚本可以帮助您将`init_data.json`挂载到容器中。

`init_data.json` 可参照模板：[init_data.json.template](#) 在使用之前将它重命名为`init_data.json`

对于 Docker

如果你使用Docker部署Casdoor，你可以使用`volume`命令将`init_data.json`挂载到容器中。

```
docker run ... -v /path/to/init_data.json:/init_data.json
```

对于 Kubernetes:

如果你使用Kubernetes部署Casdoor，你可以使用`configmap`来存储`init_data.json`。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: casdoor-init-data
data:
  init_data.json:
```

您可以通过挂载`configmap`将数据挂载到Casdoor的`pods`中。您可以按照以下方式修改您的`deployment`:

```
apiVersion: apps/v1
kind: Deployment
...
spec:
  template:
    ...
      spec:
        containers:
          ...

```

导出配置数据

You can export all Casdoor configuration data to a file for backup or migration purposes. There are two methods available:

Using the Binary (Recommended)

If you're running Casdoor from a binary, use the `-export` flag to dump the database to a JSON file:

```
# Export to default location (init_data_dump.json)
./casdoor -export

# Export to a custom path
./casdoor -export -exportPath /path/to/backup.json
```

The export runs after database initialization but before the server starts, then exits automatically. This method works with any deployment method (binary, Docker, Kubernetes) and doesn't require Go toolchain or source code access.

Using Go Test

If you have access to the source code, you can use the test method:

```
go test ./object -v -run TestDumpToFile
```

This will generate `init_data_dump.json` in the same directory.

Migrating Data

After exporting, rename `init_data_dump.json` to `init_data.json` and place it in the root directory of your target Casdoor installation. On startup, Casdoor will automatically import the data.

引用

数据初始化支持的所有 Casdoor 对象如下：

对象	Go 结构体	文档
组织机构	struct	doc
应用	struct	doc
用户	struct	doc
证书	struct	doc
提供商	struct	doc
Idaps	struct	文档
models	struct	
permissions	struct	doc
payments	struct	文档

对象	Go 结构体	文档
products	struct	文档
resources	struct	文档
roles	struct	文档
syncers	struct	文档
tokens	struct	文档
webhooks	struct	文档
groups	struct	文档
adapters	struct	文档
enforcers	struct	
plans	struct	doc
pricings	struct	文档
invitations	struct	文档
records	struct	
sessions	struct	
subscriptions	struct	doc

对象	Go 结构体	文档
transactions	struct	

如果你对填写这个模板仍然感到困惑，你可以调用RESTful API，或者使用浏览器的调试模式来查看 `GetXXX` 对这些对象的响应。响应的格式与 `init_data.json` 相同。

在CDN中托管静态文件

前端静态资源，如.js和.css文件，位于`web/build/static/`。如果您希望在公共云的CDN服务中部署这些文件，Casdoor提供了一个简化部署过程的脚本。请按照以下步骤操作：

① 备注

我们假设您已经构建了Casdoor的前端代码。如果您还没有，请参考[文档](#)。

准备工作

首先，您需要在Casdoor UI中创建一个有效的[存储提供商](#)。您可以参考[示例](#)。

⚠ 注意事项

在填写[Domain](#)字段时，确保以'/'结束。

Domain [?](#) :

<https://cdn.casbin.com/casdoor/>

使用说明

该脚本可以在[deployment/deploy_test.go](#)找到。

在[deploy_test.go](#)中，你需要修改`GetProvider()`中的`id`参数。提供者`id`的格式是`<owner>/<name>`。

```
func TestDeployStaticFiles(t *testing.T) {
    provider := object.GetProvider("admin/
provider_storage_aliyun_oss")
    deployStaticFiles(provider)
}
```

在进行必要的修改后，使用以下命令来运行脚本：

```
cd deployment
go test
```

如果执行成功，你将会看到：

```
PASS
ok      github.com/casdoor/casdoor/deployment  2.951s
```

工作原理

脚本的功能：

- 将`css/`和`js/`文件夹中的所有文件上传到存储提供商指定的CDN服务。
- 将`web/build/index.html`中的所有`.css`和`.js`文件的URL替换为CDN中托管的URL。

你仍然需要保留`index.html`文件。在静态文件被上传到CDN后，`index.html`仍然会通过Casdoor的Go后端被用户请求，而CDN中的静态文件将通过在`index.html`中提供的URLs被请求。

在内部网络中托管静态文件

如果您在**内网**上部署Casdoor，您可能无法直接通过互联网访问静态资源。您需要部署可以访问的静态资源，然后在Casdoor中修改三处配置。

部署静态资源

Casdoor中的所有静态资源，包括图片、标志、CSS等，都存储在[casbin/static仓库](#)中。

克隆该仓库并在网页服务器上部署它。确保你可以访问这些资源。

配置Casdoor

您可以简单地修改配置文件，将静态资源地址设置为您部署的地址。前往[conf/app.conf](#)并将[staticBaseUrl](#)设置为您的部署地址。

```
staticBaseUrl = "https://cdn.casbin.org"
```

数据库迁移

在升级数据库时，存在数据丢失的风险，例如在删除旧字段时。幸运的是，Casdoor利用了[xorm](#)，它可以帮助解决许多数据库迁移问题。然而，一些模式和数据迁移仍然需要手动处理，例如在字段名称更改时。

① 备注

参考[xorm](#)文档以更好地理解xorm的模式操作。

工作原理

如前所述，xorm无法处理字段名称的更改。To address this, xorm provides a [migrate](#) package that can assist with this problem.

要处理字段重命名，你可以编写如下代码：

```
migrations := []*migrate.Migration{
{
    ID: "CasbinRule--fill ptype field with p",
    Migrate: func(tx *xorm.Engine) error {
        _, err :=
        tx.Cols("ptype").Update(&xormadapter.CasbinRule{
            Ptype: "p",
        })
        return err
    },
    Rollback: func(tx *xorm.Engine) error {
        return tx.DropTable(&xormadapter.CasbinRule{})
    },
}
```

我们的目标是将 `p_type` 重命名为 `ptype`。然而，由于 xorm 不支持字段重命名，我们必须采取更复杂的方法：将 `p_type` 的值赋给 `ptype`，然后删除 `p_type` 字段。

`ID` 字段唯一标识正在执行的迁移。在 `m.Migrate()` 运行后，`ID` 的值将被添加到数据库的迁移表中。

在再次启动项目时，数据库将检查表中是否存在任何现有的 `ID` 字段，并避免执行与相同 `ID` 相关的任何操作。



> 如何连接到Casdoor

如何连接到Casdoor

概览

将您的应用连接到Casdoor

标准OIDC 客户端

使用 OIDC 发现迁移到Casdoor

Casdoor SDKs

使用Casdoor SDKs而不是标准的OIDC协议

Casdoor Authenticator App

Store TOTP code in Casdoor

如何启用单点登录

启用单点登录

Single Sign-Out (SSO Logout)

Implement Single Sign-Out to log users out from all applications simultaneously

Vue SDK

Casdoor Vue SDK

桌面 SDK

4 个项目

移动 SDKs

1 个项目

Casdoor CLI

Using Casdoor's official command-line interface for managing users, groups, and permissions

Casdoor插件

在 Spring Boot, WordPress, Odoo 等其他框架中使用 Casdoor 插件或中间件。

Chrome Extension

Using Casdoor in Chrome extension

Next.js

在Next.js项目中使用Casdoor

Nuxt

在Nuxt项目中使用Casdoor

OAuth 2.0

使用AccessToken验证客户端

使用Casdoor作为CAS服务器

如何将Casdoor用作CAS服务器

SAML

6 个项目

面部识别

使用 Face ID 登录到Casdoor

WebAuthn

在 Casdoor 中使用webauthn

概览

在本节中，我们将向您展示如何将您的应用程序连接到Casdoor。

作为服务提供商(SP)， Casdoor 支持两项认证协议：

- OAuth 2.0 (OIDC)
- SAML

作为身份提供商 (Idp)， Casdoor 支持四项认证协议：

- OAuth 2.0
- OIDC
- SAML
- CAS 1.0, 2.0, 3.0

OAuth 2.0 (OIDC)

什么是 OAuth 2.0?

OAuth 2是一个授权框架，它使得应用程序——如Facebook, GitHub和Casdoor——能够在HTTP服务上获得对用户账户的有限访问权限。它的基本原理是将用户身份验证委托给托管用户帐户的服务，并授权第三方应用程序访问该用户帐户。 OAuth 2为网页和桌面应用程序，以及移动设备提供授权流程。

Casdoor的授权程序基于OAuth 2.0协议。 我们推荐使用 OAuth 2.0 协议，原因如下：

- 1. 该协议简单易行，能解决多种问题。
- 2. 该协议成熟度高且社区支持广泛。

如此，您的应用程序将通过 OAuth 2.0 (OIDC) 与 Casdoor 通讯。这里有三种方式连接到 Casdoor：

标准 OIDC 客户端

标准OIDC 客户端: 使用一个标准的 OIDC 客户端实现，通常在各类编程语言或框架都广泛提供。

什么是OIDC?

OpenID Connect (OIDC) 是一个在OAuth 2.0 框架顶端运行的开放身份验证协议。针对消费者，OIDC允许个人通过单点登录(SSO)访问使用OpenID提供商(OPs)的依赖方站点，如电子邮件提供商或社交网络平台，以验证其身份。它向应用程序或服务提供用户信息、认证背景，并允许访问用户个人资料。

Casdoor 完全支持 OIDC 协议。如果您的应用程序已经通过**标准的OIDC客户端库**使用了另一个OAuth 2.0 (OIDC) 身份提供商，并且您想迁移到Casdoor，使用OIDC发现将使切换到Casdoor变得非常简单。

Casdoor SDKs

Casdoor SDKs: 对于大多数编程语言，Casdoor在OIDC之上提供了易于使用的SDK库，其中包含了只在Casdoor中才有的扩展功能。

与标准的OIDC协议相比，Casdoor的SDK提供了更多的功能，如用户管理和资源上传等。通过Casdoor SDK连接到Casdoor需要的时间比使用标准的OIDC客户端库要多，但它提供了最佳的灵活性和最强大的API。

Casdoor插件

Casdoor 插件: 如果您的应用程序是基于流行平台（如 Spring Boot, WordPress 等）构建的，并且 Casdoor（或第三方）已经为其提供了插件或中间件，那么您应该使用它。使用插件比手动调用Casdoor SDK要容易得多，因为前者是专为平台制作的。

插件:

- [Jenkins 插件](#)
- [APISIX 插件](#)

中间件:

- [Spring Boot插件](#)
- [Django 插件](#)

SAML

什么是SAML?

安全鉴别标记语言(SAML)是一种开放标准，允许身份提供者(IDP)将授权证书传给服务提供者。这个术语的意思是，你可以使用一套凭证登录到许多不同的网站。管理每个用户的一个登录要比管理电子邮件、客户关系管理（CRM）软件、活动目录等的单独登录要简单得多。

SAML交易使用可扩展标记语言(XML) 在标识提供者和服务提供者之间进行标准化通信。SAML是用户身份认证和使用服务授权之间的链接。

Casdoor可以用作SAML IdP。目前，Casdoor支持SAML 2.0的主要功能。有关更多详

细信息，请参见[SAML](#)。

示例：

Casdoor作为Keycloak中的SAML IdP

建议：

1. 该协议是**强大的**，覆盖了许多场景，使其成为最全面的SSO协议之一。
2. 该协议是**大型的**，带有许多可选参数，因此在实际实施中很难100%覆盖所有应用场景。
3. 如果应用程序是**新**开发的，由于其高度的技术复杂性，不建议使用SAML。

CAS

什么是CAS？

中央认证服务（CAS）是网络的单点登录协议。它的目的是允许用户在只提供一次凭证（如用户ID和密码）的情况下访问多个应用程序。它还允许网络应用程序在不获取用户的安全凭证（如密码）的情况下对用户进行身份验证。

Casdoor已实现了CAS 1.0、2.0和3.0的功能。有关更多详细信息，请参见[CAS](#)。

建议：

1. 该协议本身相对轻量级且易于实现，但它只能解决单一场景。
2. CAS 客户端和CAS服务器之间的相互信任是通过在没有任何加密或签名机制的情况下使用接口建立的，目的是确保进一步的安全。
3. CAS协议并无优于其他协议的优点。

集成表

一些应用程序已有连接到Casdoor的示例。 您可以按照文档指示操作， 快速连接到 Casdoor。 您可以在[集成表](#)中查看所有应用程序。

标准OIDC 客户端

OIDC 发现

Casdoor已完全实现了OIDC协议。 如果您的应用程序已经使用标准的OIDC客户端库连接到另一个OAuth 2.0身份提供商，并且您想要迁移到Casdoor， 使用OIDC发现将使您非常容易切换。

Global OIDC Endpoint

Casdoor's global OIDC discovery URL is:

```
<your-casdoor-backend-host>/.well-known/openid-configuration
```

例如，演示站点的OIDC发现URL是: <https://door.casdoor.com/.well-known/openid-configuration>，它包含以下信息：

```
{
  "issuer": "https://door.casdoor.com",
  "authorization_endpoint": "https://door.casdoor.com/login/oauth/authorize",
  "token_endpoint": "https://door.casdoor.com/api/login/oauth/access_token",
  "userinfo_endpoint": "https://door.casdoor.com/api/userinfo",
  "jwks_uri": "https://door.casdoor.com/.well-known/jwks",
  "introspection_endpoint": "https://door.casdoor.com/api/login/oauth/introspect",
  "response_types_supported": [
    "code",
```

Application-Specific OIDC Endpoints

Besides the global discovery endpoint, you can use application-specific OIDC discovery endpoints. Each application gets its own isolated OIDC configuration with a unique issuer. This comes in handy when running multi-tenant deployments where applications need their own certificates or when you want to gradually migrate applications without affecting others.

The application-specific discovery URL follows this pattern:

```
<your-casdoor-backend-host>/.well-known/<application-name>/openid-configuration
```

For example, if you have an application named `app-example`:

```
https://door.casdoor.com/.well-known/app-example/openid-configuration
```

The main difference is that the `issuer` and `jwks_uri` fields in the discovery response contain the application path. The `issuer` becomes

`https://door.casdoor.com/.well-known/app-example` instead of just `https://door.casdoor.com`, and the `jwks_uri` points to `/well-known/app-example/jwks`. Everything else, including the authorization and token endpoints, stays the same.

You can also access the JWKS and WebFinger endpoints for each application:

```
<your-casdoor-backend-host>/.well-known/<application-name>/jwks  
<your-casdoor-backend-host>/.well-known/<application-name>/webfinger
```

The JWKS endpoint returns the public keys for verifying tokens. When an application has its own certificate configured, that certificate is used. Otherwise, it falls back to the global certificates.

Here's what the responses look like. The global endpoint returns:

```
{  
  "issuer": "https://door.casdoor.com",  
  "jwks_uri": "https://door.casdoor.com/.well-known/jwks",  
  "authorization_endpoint": "https://door.casdoor.com/login/oauth/authorize",  
  ...  
}
```

While the application-specific endpoint for `app-example` returns:

```
{  
  "issuer": "https://door.casdoor.com/.well-known/app-example",  
  "jwks_uri": "https://door.casdoor.com/.well-known/app-example/jwks",  
  "authorization_endpoint": "https://door.casdoor.com/login/oauth/authorize",  
  ...  
}
```

OIDC客户端库列表

以下是一些适用于Go和Java等语言的OIDC客户端库的列表：

OIDC 客户端库	语言	链接
go-oidc	Go	https://github.com/coreos/go-oidc
pac4j-oidc	Java	https://www.pac4j.org/docs/clients/openid-connect.html

请注意，上述表格并非详尽无遗。要获取完整的OIDC客户端库列表，您可以在以下位置找到更多详细信息：

1. <https://oauth.net/code/>
2. <https://openid.net/certified-open-id-developer-tools/>

OIDC UserInfo字段

以下表格说明了如何将OIDC UserInfo字段（通过</api/userinfo> API）从Casdoor的用户表的属性中映射出来：

Casdoor 用户字段	OIDC用户信息字段
Id	sub
originBackend	iss
Aud	aud
Name	preferred_username

Casdoor 用户字段	OIDC用户信息字段
DisplayName	name
Email	email
Avatar	picture
Location	address
Phone	phone

您可以在[这里](#)查看UserInfo的定义。

Casdoor SDKs

简介

与标准的OIDC协议相比，Casdoor在SDK中提供了更多的功能，如用户管理、资源上传等。通过Casdoor SDK连接到Casdoor的成本比使用OIDC标准客户端库更低，并将提供灵活性最佳和最强大的API。

Casdoor SDK可分为两类：

1. 前端SDK：用于网站的Javascript SDK和Vue SDK，用于应用的Android或iOS SDK。Casdoor支持为网站和移动应用程序提供身份验证。
2. 后端SDK：Go, Java, Node.js, Python, PHP等后端语言的SDK。

💡 提示

如果您的网站是采用后端分离的方式开发，您可以使用Javascript SDK：[casdoor-js-sdk](#) 或 Vue SDK：[casdoor-vue-sdk](#) 将Casdoor整合到前端。如果您的网页应用程序是由JSP或PHP开发的传统网站，那您就只能使用后端SDK。示例：[casdoor-Python-vue-sdk示例](#)

移动SDK	描述	SDK代码库	示例
Android SDK	适用于Android应用	casdoor-android-sdk	casdoor-android-example
iOS SDK	针对iOS应用程序	casdoor-ios-sdk	casdoor-ios-example
React Native SDK	对于React Native应用程序	casdoor-react-native-sdk	casdoor-react-native-example
Flutter SDK	适用于Flutter应用	casdoor-flutter-sdk	casdoor-flutter-example
Firebase SDK	适用于Google Firebase应用		casdoor-firebase-example
Unity游戏SDK	适用于Unity 2D/3D PC/移动游戏	casdoor-dotnet-sdk	casdoor-unity-example
uni-app SDK	对于uni-app应用程序	casdoor-uniapp-sdk	casdoor-uniapp-example

桌面版SDK	描述	SDK代码	示例
Electron SDK	对于Electron应用	casdoor-js-sdk	casdoor-electron-example
.NET 桌面 SDK	适用于.NET桌面应用	casdoor-dotnet-sdk	WPF: casdoor-dotnet-desktop-example WinForms: casdoor-dotnet-winform-example Avalonia UI: casdoor-dotnet-avalonia-example
C/C++ SDK	用于C/C++桌面应用程序	casdoor-cpp-sdk	casdoor-cpp-qt-example

Web前端SDK	描述	SDK 代码	示例代码
Javascript SDK	对于传统的非SPA网站	casdoor-js-sdk	Nodejs 后端: casdoor-raw-js-example Go 后端: casdoor-go-react-sdk-example
仅前端的SDK	仅用于前端的SPA网站	casdoor-js-sdk	casdoor-react-only-example

Web前端SDK	描述	SDK 代码	示例代码
React SDK	适用于React网站	casdoor-react-sdk	Nodejs 后端: casdoor-nodejs-react-example Java 后端: casdoor-spring-security-react-example
Next.js SDK	针对Next.js网站		nextjs-auth
Nuxt SDK	对于Nuxt网站		nuxt-auth
Vue SDK	For Vue websites	casdoor-vue-sdk	casdoor-python-vue-sdk-example
Angular SDK	For Angular websites	casdoor-angular-sdk	casdoor-nodejs-angular-example
Flutter SDK	For Flutter Web websites	casdoor-flutter-sdk	casdoor-flutter-example
ASP.NET SDK	For ASP.NET Blazor WASM websites	Blazor.BFF.OpenIDConnect.Template	casdoor-dotnet-blazorwasm-oidc-example
Firebase SDK	适用于 Google Firebase 应用		casdoor-firebase-example

接下来，根据您后端的语言，可以选择使用下面的后端SDK之一：

Web后端 SDK	描述	Sdk 代码	示例代码
Go SDK	对于Go后端	casdoor-go-sdk	casdoor-go-react-sdk-example
Java SDK	针对Java后端	casdoor-java-sdk	casdoor-spring-boot-starter , casdoor-spring-boot-example , casdoor-spring-security-react-example
Node.js SDK	针对Node.js后端	casdoor-nodejs-sdk	casdoor-nodejs-react-example
Python SDK	针对Python后端	casdoor-python-sdk	Flask: casdoor-python-vue-sdk-example Django: casdoor-django-js-sdk-example FastAPI: casdoor-fastapi-js-sdk-example
PHP SDK	针对PHP后端	casdoor-php-sdk	wordpress-casdoor-plugin
.NET SDK	针对ASP.NET 后端	casdoor-dotnet-sdk	casdoor-dotnet-sdk-example
Rust SDK	针对Rust后端	casdoor-rust-sdk	casdoor-rust-example
C/C++ SDK	针对 C/C++ 后端	casdoor-cpp-sdk	casdoor-cpp-qt-example
Dart SDK	针对Dart后端	casdoor-dart-sdk	
Ruby SDK	针对Ruby后端	casdoor-ruby-sdk	

要查看官方Casdoor SDK的完整列表, 请参阅: <https://github.com/orgs/casdoor/repositories?q=sdk&type=all&language=&sort=>

如何使用 Casdoor SDK ?

1. 后端 SDK 配置

当您的应用程序启动时, 您需要调用 `InitConfig()` 函数来初始化Casdoor SDK 配置。以casdoor-go-sdk为例: <https://github.com/casbin/casnode/blob/6d4c55f5c9a3c4bd8c85f2493abad3553b9c7ac0/controllers/account.go#L51-L64>

```
var CasdoorEndpoint = "https://door.casdoor.com"
var ClientId = "541738959670d221d59d"
var ClientSecret = "66863369a64a5863827cf949bab70ed560ba24bf"
var CasdoorOrganization = "casbin"
var CasdoorApplication = "app-casnode"

//go:embed token_jwt_key.pem
var JwtPublicKey string

func init() {
    auth.InitConfig(CasdoorEndpoint, ClientId, ClientSecret, JwtPublicKey, CasdoorOrganization, CasdoorApplication)
}
```

`InitConfig()` 的所有参数解释为:

参数	必须	描述
端点	是	Casdoor 服务器 URL, 例如 <code>https://door.casdoor.com</code> 或 <code>http://localhost:8000</code>
clientId	是	Casdoor 应用程序的客户端ID
clientSecret	是	Casdoor 应用程序的客户端密钥
jwtPublicKey	是	Casdoor 应用程序的证书的公钥
组织名称	是	Casdoor 组织的名称
应用程序名称	不	Casdoor 应用程序的名称



提示

`JwtPublicKey` 可以在 `Certs` 页面中进行管理。

Certs Add							
Name	Created time	Display name	Scope	Type	Crypto algorithm	Bit size	Expire in years
cert_rjeegc	2022-02-16 11:04:10	New Cert - rjeegc	JWT	x509	RSA	4096	20
cert-built-in	2022-02-15 12:31:46	Built-in Cert	JWT	x509	RSA	4096	20

您可以在证书编辑页面中找到公钥, 复制或下载它以供 sdk 使用。

Public key [Copy public key](#) [Download public key](#)

```
-----BEGIN CERTIFICATE-----
MIIEvTCzAuGgAwIBAgDAlcAMA0GCSqGSIb3dQEBcwlAMDYrHTAbBgNVBAoT
FENhc2Bvb3lgT3InW5pemf0aW9uMmRUlwIwDVQQDEiwDXNkb29yENlcnQuhNCMjEx
MDxEIMDgxMTUyWhCNDE1MDgxMTUyWjA2MR0wGwYDVQKExiRDYXnk29yE9y
Z2fXpnhGlvbJlVMWMGA1UEAxMMQ2FzG9vcBDZX10MlICjlaNBqkhkG9w0B
AQEEA0AcAGAAU1CgkAgEaslnpb5E1/yml0f1RfSDSSE8IR7y+lw+RJj74e5jr4q
b8zMY
-----END CERTIFICATE-----
```

Private key [Copy private key](#) [Download private key](#)

```
-----BEGIN PRIVATE KEY-----
MIUKQIBAAKCgAgEaslnpb5E1/yml0f1RfSDSSE8IR7y+lw+RJj74e5jr4q
b8zMY
k7HeHcYzr/hmNewEVnhxu1P0mBeQ5pp/QGo8vgEmjATNmzklNjOQjCjYwUr
sOf/m1n1Co13vx6mV1kHjZsRksMhY1YvaTEP3+vB8Hjg3MHFWrb07uvfMCj5
W8+OrkTcCKTR8+9V8janebz//zePFvh9bFZate/lhPK0G9LP1g
OvwloC1AsarHTP40mQlR0tOHqZfybdySpwAQwvNaF7e7mTSR5B0/wlNCUBDP
TSVjCo4WlISf6kz027kmPstj+btvcqsRAjGtwsB9h62Kptjs1Yn7Gau3qf4z
o
KbUrsYxQjXlvwcQsEftUuk5ew5zuPSDRl.oByQTlx0jLAFNW3g/pzDjgd/
60d6HtmvbZn45mjdyfHxCdb1Kn7N+xTojnfakwep2REV+RMcf4xGuhrRsnLsmk
mtUDey9zaBLs9j1YEQMf2IEq+RVtU+wB8y8K/d1bcY+ffG5fbpw
oq4SRsvs327bW042zx0f/1VLoRhfjPbUf0bfrr/AeZMHPkOXfz4yE+hqz6
8wfDOV9r9YcBlSAF7323osYnjEghnUrohngCpjlk/Mz2K848cbvn8CawEA
AQKCAGaHPTxhVNRuydCf2P1Ytd+MIMlJmpQH9woRi8604Upulelpbx1CpOYu
npr7x9lTzUo/u6FLDq823k6GOT7TkFyymNy4+2Wkn/5gTgw5roMqTrbwxxd
Aftxpq4ZVM8tIS3W7zMVhhabHAu50s0RvbVn-znTa7/vM5wKa6h3uLQLW
aYEltQVn3Wlk/PzA8WDF94HkaVtgSUk40EcelpAcIL6CC01fnnSb6v/BBBG
khaTdAkogVv3cEmldkR2uuax48g8s7dzIkav/JBwt+K5JrwFhmy5AYLah
bu9MrrdHhEzlxHbmDahoTwEfmc8kbU26gaEhufo4YIMk+84bEGQsnNsNR9
Msau9qkSlprYo6Mjt1Q/y1q3hfr8SuZba3XkohbYz297jk+jDtq2zakQWzDG
JLEtbGgdeYUMS2yc/C/FUVUN/YPCdn769kw/lmOR2k56wpbFrwR9jYgnQzbj3d
4AOrgs3AdevxDv0t1071c8e334WusvXNCVRuzbY/DK0/W7jxjdxdvXevHxGrh
1Gc+FkkBeinTqfDzdlkx6N80nyZuLyymRiavn9bVcrarb5h5S1CE0HOw0gH
5GdesqMuqTS0eve1RUnrF1CWWMvPeEushW9jbl3BBh4wflsQKCAQEay4x+c+F8
icbaKtsmPRMfYUJwe99tovDbxM/3x60yfEux1LsqagQz7nolJf7xJf0j+
vcG66A0qjwA6j+QdeEf8fe04t56uMac3fWPJA00vHCvrga9gCZHoC940/yn
6EqjWqg2zAU15R6A3P/XetgsixVCFCGz+Fxylbz87B1Y9h5c2zz6G3K8+PvZ
dp+DfYfHb0f1.RuWxdkXk/QglXv7fR7zFqvkGhmS7qvcKXfrWSpw+H71kQAU
TQFj8lwgqrTouVopjD6DB10Pj/1Btg59a+jsnXxcpcj9XyhgjSj1d2sMqd
ha/kY4NdHhY20KCAQEa3gkrROpdgcooamednlwplrxryk5MrhEaglBeJidp
98HhNcl0wra5xuMS6ZC7R0xOkISLp4gt22W59lq/nPQ7PN5PdN2RzOlrmHcS
-----END PRIVATE KEY-----
```

[Save](#)
[Save & Exit](#)

之后，您可以在应用编辑页面选择证书。

Edit Application [Save](#) [Save & Exit](#)

Name :	app-built-in
Display name :	Casdoor
Logo :	https://cdn.casbin.com/logo/logo_1024x256.png
Preview:	
Home :	https://casdoor.org
Description :	
Organization :	built-in
Client ID :	c2ab05e8460fd3ff9ddee
Client secret :	c9199f1025080f089d253638f1a72b4c3e926d05
Cert :	<input style="width: 100%; border: 1px solid #ccc; padding: 2px; border-radius: 4px;" type="text" value="cert-built-in"/> ←
Redirect URLs :	cert_rjeegc cert-built-in Redirect URL

Action

2. 前端配置

首先，通过 NPM 或 Yarn 安装 `casdoor-js-sdk`

```
npm install casdoor-js-sdk
```

或者：

```
yarn add casdoor-js-sdk
```

然后定义以下实用功能(在全局JS文件中更好，比如 `Setting.js`)：

```

import Sdk from "casdoor-js-sdk";

export function initCasdoorSdk(config) {
  CasdoorSdk = new Sdk(config);
}

export function getSignupUrl() {
  return CasdoorSdk.getSignupUrl();
}

export function getSigninUrl() {
  return CasdoorSdk.getSigninUrl();
}

export function getUserProfileUrl(userName, account) {
  return CasdoorSdk.getUserProfileUrl(userName, account);
}

export function getMyProfileUrl(account) {
  return CasdoorSdk.getMyProfileUrl(account);
}

export function getMyResourcesUrl(account) {
  return CasdoorSdk.getMyProfileUrl(account).replace("/account?", "/resources?");
}

export function signin() {
  return CasdoorSdk.signin(ServerUrl);
}

export function showMessage(type, text) {
  if (type === "") {
    return;
  } else if (type === "success") {
    message.success(text);
  } else if (type === "error") {
    message.error(text);
  }
}

export function goToLink(link) {
  window.location.href = link;
}

```

在您前端代码的入口文件(如 `index.js` 或 `app.js` 在React中), 您需要通过调用 `InitConfig()` 函数来初始化 `casdoor-js-sdk` 前4个参数应该使用与 Casdoor 后端SDK 相同的值。最后一个参数 `重定向路径` 是从Casdoor的登录页面返回的重定向URL的相对路径。

```

const config = {
  serverUrl: "https://door.casdoor.com",
  clientId: "014ae4bd048734ca2dea",
  organizationName: "casbin",
  appName: "app-casnnode",
  redirectPath: "/callback",
};

xxx.initCasdoorSdk(config);

```

(可选) 因为我们正在使用React作为示例, 我们的 `/callback` 路径正在撞击React路由。我们使用以下React组件接收 `/回调` 调用并发送到后端。如果您直接重定向到后端(如JSP 或 PHP), 您可以忽略此步骤。

```

import React from "react";
import {Button, Result, Spin} from "antd";
import {withRouter} from "react-router-dom";

```

3. 获取登录 URL

接下来，您可以显示“注册”和“登录”按钮或链接到您的用户。可以在前端或后端检索URL。详细信息见：[/docs/basic/core-concepts#login-urls](#)

4. 获取并验证token

步骤如下：

1. 用户点击登录URL并重定向到Casdoor的登录页面，如 `https://door.casbin.com/login/oauth/authorize?client_id=014ae4bd048734ca2dea&response_type=code&redirect_uri=https%3A%2F%2Fforum.casbin.com%2Fcallback&scope=read&state=app-casnode`
2. 用户输入用户名和密码，并点击登录（或者选择第三方登录，例如通过GitHub进行登录）
3. 该用户被重定向到您的应用，使用Casto发行的授权码(例如： `https://forum.casbin.com?code=xxx&state=yyy`)，您的应用程序的后端需要将授权码与访问令牌交换，并验证访问令牌是否有效和由Casdoor签发。函数`GetOAuthToken()` 和`ParseJwtToken()` 由Casdoor后端SDK提供。

以下代码显示如何获取并验证访问令牌。要查看一个真实的Casnode示例（一个用Go编写的论坛网站），请参见：[https://github.com/casbin/casnode/blob/6d4c55f5c9a3c4bd8c85f2493abad3553b9c7ac0/controllers/account.go#L51-L64](#)

```
// 从重定向 URL 的 GET 参数中获取代码和状态
code := c.Input().Get("code")
state := c.Input().Get("state")

// 用代码和状态交换token
token, err := auth.GetOAuthToken(code, state)
if err != nil {
    panic(err)
}

// 验证访问令牌
claims, err := auth.ParseJwtToken(token.AccessToken)
if err != nil {
    panic(err)
}
```

如果`ParseJwtToken()` 结束时没有错误，那么用户已成功登录到应用程序。返回的`claims` 可以稍后用来识别用户。

4. 用token识别用户



信息

这一部分实际上是您的应用程序本身的业务逻辑，而不是OIDC、OAuth 或Casdoor的一部分。我们只是提供正确做法，因为许多人不知道该怎么做。

在Casdoor中，访问令牌通常与ID令牌相同。他们是一样的。因此，访问令牌包含登录用户的所有信息。

由`ParseJwtToken()` 返回的变量`claims` 被定义为：

```
Type Claims struct
    User
    AccessToken string `json:"accessToken"
    jwt.RegisteredClaims
}
```

1. `User`: User 对象，包含登录用户的所有信息，请参见定义：[/docs/basic/core-concepts#user](#)
2. `AccessToken`: token信息
3. `jwt.RegisteredClaim`: JWT需要一些其他值。

这时，应用程序通常有两种方法记住用户会话： `session` and `JWT`。

Session

设置Session的方法因语言和框架而大不相同。例如，Casnode 使用 [Beego web 框架](#) 并通过调用设置会话：`c.SetSessionUser()`。

```
token, err := auth.GetOAuthToken(code, state)
if err != nil {
    panic(err)
}

claims, err := auth.ParseJwtToken(token.AccessToken)
if err != nil {
    panic(err)
}

claims.AccessToken = token.AccessToken
c.SessionUser(claims) // 设置会话
```

JWT

从 Casdoor 返回的 `accessToken` 实际上是一个 JWT。因此，如果您的应用程序使用 JWT 来保持用户 `session`，只需直接为它使用访问令牌：

1. 将访问令牌发送到前端，在本地存储浏览器等地方保存。
2. 让浏览器为每一个请求发送访问令牌到后端。
3. 调用 `ParseJwtToken()` 或使用您自己的函数来验证 `token`，通过后端提供的已登录用户信息。

5. (可选) 与用户表的互动



信息

这一部分是由 [Castor Public API](#) 提供的，而不是OIDC 或 OAuth 的一部分。

Casdoor Backend SDK 提供了许多辅助功能，不仅限于：

- `GetUser(name string)`: 通过用户名获取用户。
- `GetUsers()`: 获取所有用户。
- `AddUser()`: 添加一个用户。
- `UpdateUser()`: 更新一个用户。
- `DeleteUser()`: 删除一个用户。
- `CheckUserPassword(auth.User)`: 检查用户的密码。

这些函数是通过对 [Castor Public API](#) 调用 RESTful API 实现的。如果 Casdoor Backend SDK 中没有提供功能，您可以自己调用 RESTful API。

Casdoor Authenticator App

Overview

Casdoor-Authenticator (<https://app.casdoor.org/>) is an open-source authenticator App (source code: <https://github.com/casdoor/casdoor-authenticator>) like Google Authenticator, Microsoft Authenticator or Authy. It provides Multi-Factor Authentication (MFA) with TOTP for both iOS and Android. This app allows users to store Time-based One-Time Password (TOTP) securely in the App, which is cloud-synced with Casdoor, offering a comprehensive solution for managing Two-Factor Authentication (2FA) needs directly from mobile devices.

Key Features

- **Multi-Factor Authentication (MFA):** Generate secure TOTP-based codes for enhanced account protection.
- **Offline mode:** Generate TOTP codes without an internet connection.
- **Account synchronization:** Securely sync your accounts across multiple devices.
- **Privacy-focused:** All data is encrypted and stored securely.
- **Friendly UI:** Simple and intuitive design for easy navigation.

Android

22:21



Casdoor

admin



Search



Google:test/admin

192 592

7s



Github:test/admin

472 889

7s



Amazon:test/admin

124 416

7s



slack:test

835 125

7s

What is TOTP?

TOTP stands for Time-based One-Time Passwords and is a common form of two-factor authentication (2FA). Unique numeric passwords are generated with a standardized [algorithm](#) that uses the current time as an input. These time-based passwords:

- Change every 30 seconds for enhanced security
- Are available offline
- Are widely supported by many services and apps
- Provide user-friendly, increased account security as a second factor

How to use the Casdoor Authenticator App?

Step 0: Install the Casdoor Authenticator App

Casdoor-Authenticator is currently available for Android devices. You can download the app from the following sources:

1. Homepage: <https://app.casdoor.org>
2. Source code: <https://github.com/casdoor/casdoor-authenticator>
3. Binary release: <https://github.com/casdoor/casdoor-authenticator/releases>

For developers interested in building the app from source, you can find the source code and build instructions in the [Casdoor Authenticator GitHub Repository](#).

Step 1: Enable Totp Account storage in Casdoor Server

(Optional)

This setup is optional for users who want to store their TOTP codes in the Casdoor server. Before using the Casdoor Authenticator App, you need to make sure that the MFA accounts setting is enabled in the Casdoor server.

Account items		Visible	Regex	View rule	Modify rule	Action
Name	Organization	<input checked="" type="checkbox"/>		Public	Admin	<input type="button"/> <input type="button"/> <input type="button"/>
ID		<input checked="" type="checkbox"/>		Public	Immutable	<input type="button"/> <input type="button"/> <input type="button"/>
Name		<input checked="" type="checkbox"/>		Public	Admin	<input type="button"/> <input type="button"/> <input type="button"/>
Display name		<input checked="" type="checkbox"/>		Public	Self	<input type="button"/> <input type="button"/> <input type="button"/>
Avatar		<input checked="" type="checkbox"/>		Public	Self	<input type="button"/> <input type="button"/> <input type="button"/>
Face ID		<input checked="" type="checkbox"/>		Public	Self	<input type="button"/> <input type="button"/> <input type="button"/>
Managed accounts		<input checked="" type="checkbox"/>		Self	Self	<input type="button"/> <input type="button"/> <input type="button"/>
MFA accounts		<input checked="" type="checkbox"/>		Public	Self	<input type="button"/> <input type="button"/> <input type="button"/>

Step 2: Log in to the Casdoor Authenticator App

After installing the Casdoor Authenticator App and enabling the MFA accounts setting in the Casdoor server, you have three convenient ways to connect to your Casdoor server:

1. Manual Configuration

- Tap "Enter Server Manually"
- Enter your server URL, client ID, and organization name
- Log in with your Casdoor account credentials

2. QR Code Scan

- Tap "Scan QR Code"
- Use your device's camera to scan the QR code from your Casdoor server
- The QR code can be found in "My Account" → "MFA accounts" section

- The app will automatically configure the connection

3. Demo Server

- Tap "Try Demo Server" to connect to a pre-configured demo instance
- Useful for testing the app's functionality without setting up your own server

Casdoor server

X

Endpoint

<https://door.casdoor.com>

Client ID

b800a86702dd4d29ec4d

App Name

app-example

Organization Name

casbin

Confirm

Scan to Login

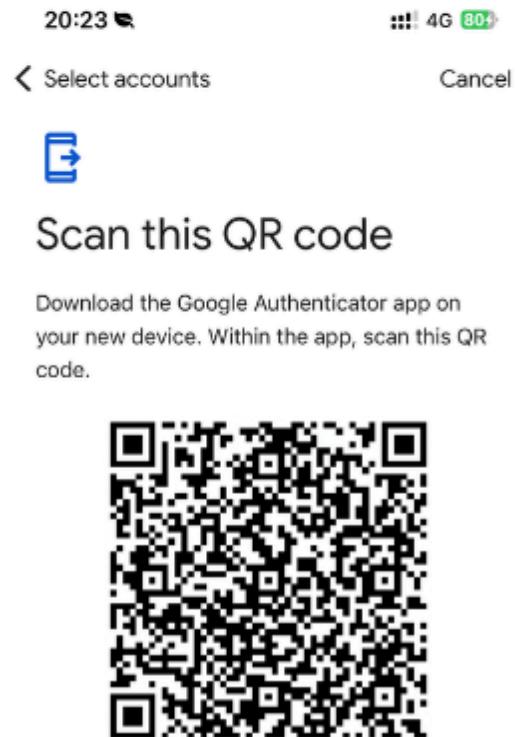
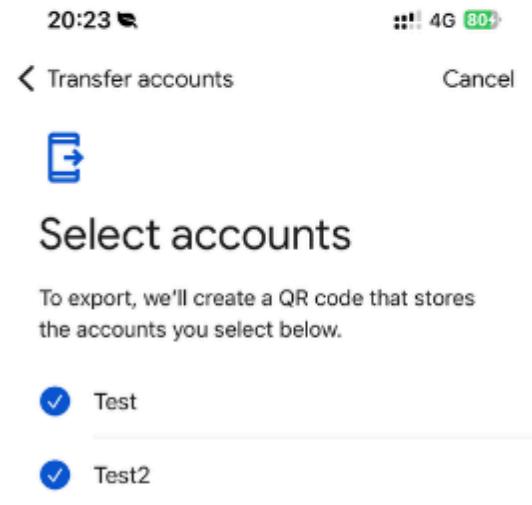
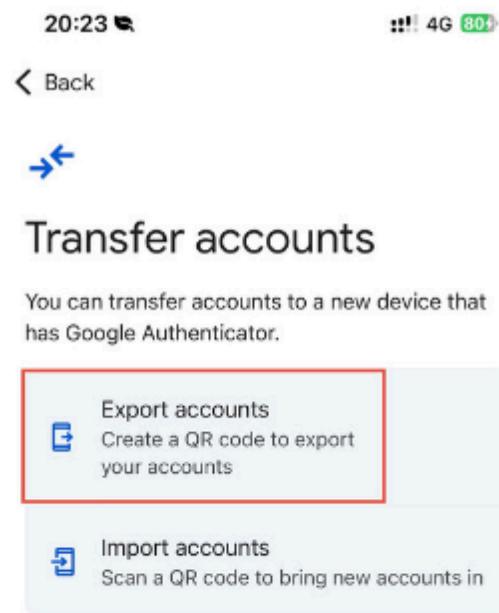
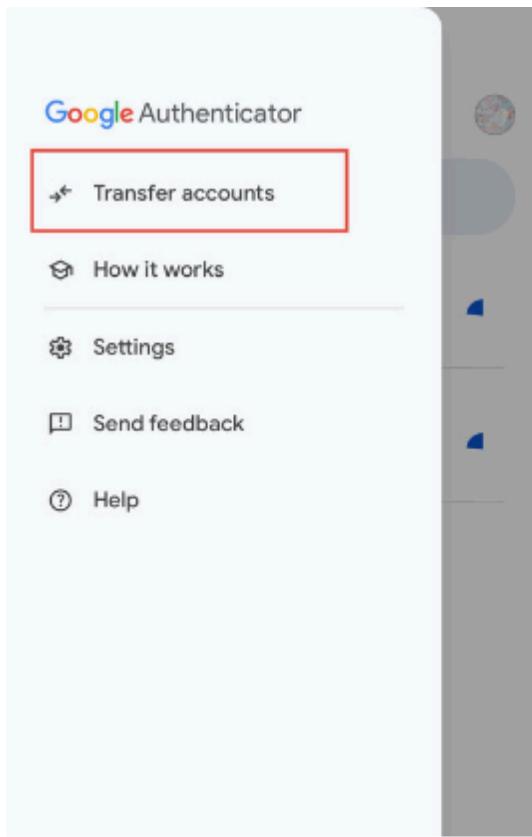
Use Casdoor Demo Site

Once connected, you can view your TOTP codes and manage your 2FA settings directly from the Casdoor Authenticator App like other authenticator apps.

Migration from Other Authenticator Apps

Migration from Google Authenticator

Select the "Transfer Accounts" option in the menu of Google Authenticator and choose the accounts you want to transfer. Then, click the "Export" button to generate a QR code.



In the Casdoor Authenticator App, scan the QR code generated by Google Authenticator to import your TOTP data. The app will automatically add the accounts to your Casdoor Authenticator App, allowing you to manage your TOTP codes securely.

22:12



Casdoor

Login



Search



Test

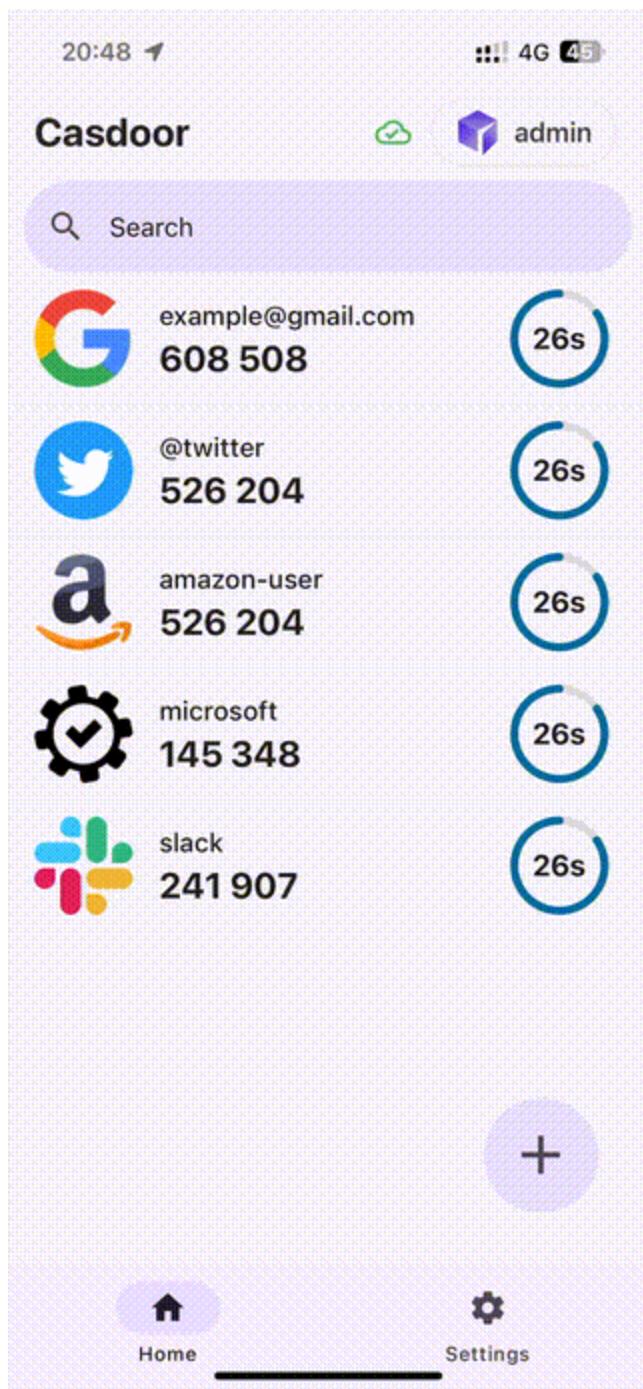
145 112



Migration from Microsoft Authenticator (requires root access)

If you are using Microsoft Authenticator, you can migrate your TOTP data to the Casdoor Authenticator App using the Microsoft Authenticator's database backup. Here's how:

1. On your Android device with Microsoft Authenticator installed, locate the app's data directory: `/data/data/com.azure.authenticator/databases/`
2. You will need root access to extract the `PhoneFactor` database file.
3. In the Casdoor Authenticator App, go to the import section
4. Select "Import from Microsoft Authenticator"
5. Choose the extracted `PhoneFactor` database file
6. The app will automatically import all your TOTP accounts from Microsoft Authenticator



如何启用单点登录

简介

您已连接了 Casdoor，并在组织中配置了多个应用程序。你希望用户只需在组织中的任何一个应用中登录一次，然后在转到另一个应用时就能够登录，无需任何额外的点击。

我们提供了这个单点登录功能。要启用它，你只需要：

- 启用自动登录按钮。
- 填写主页的URL。
- 在应用主页添加一个**静默登录**功能。

① 备注

Casdoor提供的基本登录过程允许用户通过选择当前登录的用户或使用另一个账户登录到组织中的其他应用。

启用自动登录后，将不会显示选择框，已登录的用户将直接登录。

配置

1. 填写“主页”字段。它可以是应用程序的主页或登录页面。

Casdoor Home Organizations Users Roles Permissions Models Adapters Providers Applications

Edit Application Save Save & Exit

Name : app-casbin-oa

Display name : Casbin OA

Logo : URL : https://cdn.casbin.org/img/casbin_logo_1024x256.png

Preview: 

Home : https://oa.casbin.com

Description : OA system for Casbin

2. 启用自动登录按钮。

Password ON :

Enable signup :

Signin session :

Auto signin :

Enable code signin :

Enable WebAuthn signin :

添加静默登录

实际上，我们通过在URL中携带参数来实现自动登录。因此，你的应用需要有一种方法在跳转到URL后触发登录。我们提供了[casdoor-react-sdk](#)来帮助你快速实现这个功能。你可以在[use-in-react](#)中看到详细信息。

① 信息

工作原理

1. 在应用程序主页的 URL 中，我们将携带 `silentSignin` 参数。
2. 在你的主页中，通过检查 `silentSignin` 参数来确定是否需要静默（自动）登录。如果 `silentSignin === 1`，函数应返回 `SilentSignin` 组件，该组件将帮助你发起登录请求。由于你已启用自动登录，用户将在不点击的情况下自动登录。

添加弹出登录

“弹出登录”功能将打开一个小窗口。在子窗口中登录Casdoor后，它将向主窗口发送身份验证信息，然后自动关闭。我们通过在URL中携带参数来实现这个功能。

① 信息

如何使用

使用[casdoor-js-sdk](#)中的 `popupSignin()` 方法来快速实现这个功能。你可以在[casdoor-nodejs-react-example](#)中看到一个演示。

工作原理

1. 在到应用主页的URL中，我们将携带 `popup` 参数。
2. 当 `popup=1` 在登录参数中时，Casdoor 将把 `code` 和 `state` 作为消息发送到主窗口，并在主窗口中使用SDK完成 `token` 的获取。

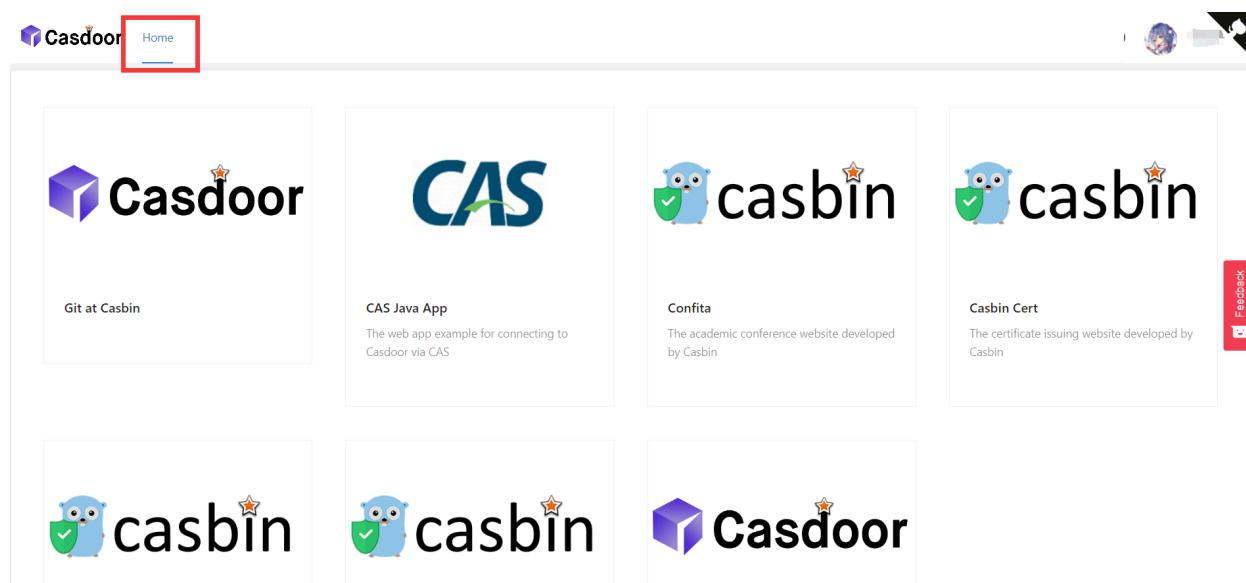
使用 SSO

配置已完成。下面，我们将向你展示如何使用自动登录。

① 信息

确保你的应用可以重定向到用户的个人资料页面。我们在每种语言的SDK中都提供了 `getMyProfileUrl(account, returnUrl)` API。

打开个人资料页面，然后转到“主页”页面（/ URL路径）。你将看到由组织提供的应用列表。值得注意的是，只有“内置”以外的组织中的用户才能在“主页”上看到应用列表。所有全局管理员（在“内置”组织中的人）都看不到它。



点击应用列表中的一个图块，它将跳转到带有GET参数`?silentSignin=1`的该应用的主页URL。如果应用已经与Casdoor SSO集成（因此它会识别`?silentSignin=1`参数并在后台执行静默登录），它将自动登录到应用。

SSO Logout

When using SSO, you might need to log a user out from all applications simultaneously. Casdoor provides an SSO logout endpoint that terminates all active sessions and expires all tokens for a user across all applications in the organization.

To implement SSO logout in your application, make a request to the `/api/sso-logout` endpoint. This endpoint will ensure the user is completely logged out from all integrated applications. For detailed information about the SSO logout API, including authentication methods and request examples, see the [SSO Logout](#) section in the Public API documentation.

Single Sign-Out (SSO Logout)

Introduction

Single Sign-Out (SSO Logout) is a feature that allows you to log a user out from all applications in an organization simultaneously. When a user logs out from one application, they are automatically logged out from all other applications that are part of the same SSO ecosystem.

This is particularly useful in scenarios such as:

- **Security incidents:** Immediately terminate all active sessions when a security breach is detected
- **Organization-wide logout policies:** Enforce logout across all services when users leave the organization or change roles
- **Compliance requirements:** Ensure users are completely logged out from all systems when required by regulations
- **User-initiated logout:** Allow users to log out from all applications with a single action

How SSO Logout Works

When the SSO logout endpoint is called, Casdoor performs the following actions:

1. **Delete all active sessions:** All active sessions for the user across all applications in the organization are terminated

2. **Expire all access tokens:** All access tokens that were issued to the user are immediately invalidated
3. **Clear the current session:** The user's current session and authentication state are cleared

This ensures that the user is completely logged out from all integrated applications and cannot access any resources without re-authenticating.

SSO Logout API

Endpoint

GET or POST /api/sso-logout

The SSO logout endpoint accepts both `GET` and `POST` requests, making it flexible for different integration scenarios.

Authentication

This endpoint requires the user to be authenticated. You can use any of the authentication methods supported by Casdoor:

- **Access token:** Include the access token in the `Authorization` header
- **Session cookie:** Use the session cookie that was set during login
- **Client credentials:** Use the application's client ID and secret for machine-to-machine scenarios

For more details on authentication methods, see the [Casdoor Public API](#) documentation.

Request Examples

Using Access Token

```
curl -X POST https://door.casdoor.com/api/sso-logout \
-H "Authorization: Bearer YOUR_ACCESS_TOKEN"
```

Using Session Cookie

```
curl -X POST https://door.casdoor.com/api/sso-logout \
--cookie "casdoor_session_id=abc123def456"
```

Using JavaScript Fetch API

```
fetch('https://door.casdoor.com/api/sso-logout', {
  method: 'POST',
  headers: {
    'Authorization': `Bearer ${accessToken}`
  },
  credentials: 'include'
})
.then(response => response.json())
.then(data => {
  console.log('Logout successful:', data);
  // Redirect to login page or home page
  window.location.href = '/login';
})
.catch(error => {
  console.error('Logout failed:', error);
});
```

Response

The API returns a standard Casdoor response:

```
{  
  "status": "ok",  
  "msg": "",  
  "data": ""  
}
```

Response Fields:

- `status`: Indicates whether the operation was successful ("ok") or failed ("error")
- `msg`: Contains an error message if the operation failed, otherwise empty
- `data`: Additional data returned by the API, typically empty for logout operations

Implementing SSO Logout in Your Application

Using Casdoor SDKs

Most Casdoor SDKs provide built-in support for SSO logout. Here are examples for different platforms:

Go SDK

```
import "github.com/casdoor/casdoor-go-sdk/casdoorsdk"

func logout(w http.ResponseWriter, r *http.Request) {
    // Get the access token from the session or request
    token := getAccessTokenFromSession(r)

    // Call the SSO logout endpoint
    err := casdoorsdk.Logout(token)
    if err != nil {
        http.Error(w, "Logout failed",
            http.StatusInternalServerError)
        return
    }

    // Clear local session
    clearSession(w, r)

    // Redirect to login page
    http.Redirect(w, r, "/login", http.StatusFound)
}
```

JavaScript SDK

```
import Sdk from "casdoor-js-sdk";

const CasdoorSDK = new Sdk({
    serverUrl: "https://door.casdoor.com",
    clientId: "YOUR_CLIENT_ID",
    appName: "YOUR_APP_NAME",
    organizationName: "YOUR_ORG_NAME",
});

async function handleLogout() {
```

Python SDK

```
from casdoor import CasdoorSDK

sdk = CasdoorSDK(
    endpoint="https://door.casdoor.com",
    client_id="YOUR_CLIENT_ID",
    client_secret="YOUR_CLIENT_SECRET",
    certificate="YOUR_CERT",
    org_name="YOUR_ORG_NAME",
    app_name="YOUR_APP_NAME",
)

def logout(access_token):
    try:
        # Call the SSO logout endpoint
        result = sdk.logout(access_token)

        if result['status'] == 'ok':
            # Clear local session
            clear_session()
            return True
        else:
            print(f"Logout failed: {result['msg']}")
            return False
    except Exception as e:
        print(f"Logout error: {e}")
        return False
```

Manual Implementation

If you're not using a Casdoor SDK, you can implement SSO logout manually by making an HTTP request to the logout endpoint:

```
async function logout() {
  const accessToken = localStorage.getItem('access_token');

  try {
    // Use the full Casdoor server URL in your application
    const response = await fetch('https://door.casdoor.com/api/sso-logout', {
      method: 'POST',
      headers: {
        'Authorization': `Bearer ${accessToken}`,
        'Content-Type': 'application/json'
      },
      credentials: 'include'
    });

    const result = await response.json();

    if (result.status === 'ok') {
      // Clear local storage
      localStorage.removeItem('access_token');
      localStorage.removeItem('user_info');
      sessionStorage.clear();

      // Redirect to login page
      window.location.href = '/login';
    } else {
      console.error('Logout failed:', result.msg);
    }
  } catch (error) {
    console.error('Logout error:', error);
  }
}
```

Best Practices

1. Clear Local State

After calling the SSO logout endpoint, make sure to clear all local authentication state:

- Remove access tokens from local storage or session storage
- Clear any cached user information
- Invalidate any local session cookies
- Reset application state to the logged-out state

2. Handle Logout Errors Gracefully

Even if the SSO logout endpoint fails, you should still clear local authentication state to ensure the user appears logged out from your application:

```
async function logout() {
  try {
    await callSSOLogout();
  } catch (error) {
    console.error('SSO logout failed, clearing local state
anyway:', error);
  } finally {
    // Always clear local state
    clearLocalAuthenticationState();
    redirectToLogin();
  }
}
```

3. Provide User Feedback

Give users clear feedback about the logout process:

```
async function logout() {
  // Show loading indicator
  showLoadingIndicator('Logging out...');

  try {
    await callSSOLogout();
    showSuccessMessage('Logged out successfully');
  } catch (error) {
    showErrorMessage('Logout failed, but you have been logged out
locally');
  } finally {
    clearLocalAuthenticationState();
    // Redirect after a short delay to allow users to see the
message
    setTimeout(() => redirectToLogin(), 1000);
  }
}
```

4. Implement Logout Timeout

Set a reasonable timeout for the logout request to prevent users from waiting indefinitely:

```
async function logout() {
  const timeout = 5000; // 5 seconds

  try {
    await Promise.race([
      callSSOLogout(),
```

Security Considerations

1. Secure Communication

Always use HTTPS when calling the SSO logout endpoint to prevent token interception:

```
// ✓ Good: Uses HTTPS
const logoutUrl = 'https://door.casdoor.com/api/sso-logout';

// ✗ Bad: Uses HTTP (insecure)
const logoutUrl = 'http://door.casdoor.com/api/sso-logout';
```

2. Token Validation

Casdoor validates the access token before processing the logout request. Ensure your token is valid and has not expired before making the logout call.

3. CSRF Protection

When using session cookies for authentication, ensure CSRF protection is enabled to prevent unauthorized logout requests:

```
// Include CSRF token in the request headers
// Replace with your actual Casdoor server URL
fetch('https://door.casdoor.com/api/sso-logout', {
  method: 'POST',
  headers: {
    'X-CSRF-Token': getToken()
  },
});
```

4. Audit Logging

Consider logging logout events for security auditing and compliance:

```
func logout(userID string, token string) error {
    // Call SSO logout
    err := casdoorsdk.Logout(token)

    // Log the logout event
    auditLog.Info(map[string]interface{}{
        "event": "sso_logout",
        "user_id": userID,
        "timestamp": time.Now(),
        "success": err == nil,
    })

    return err
}
```

Troubleshooting

Logout Not Working Across All Applications

If users remain logged in to some applications after SSO logout:

1. Verify application integration: Ensure all applications are properly integrated with Casdoor and use the same organization
2. Check token validation: Make sure all applications validate tokens on each request
3. Review session management: Applications should not rely solely on local sessions; they must validate tokens with Casdoor

Token Still Valid After Logout

If access tokens remain valid after logout:

1. Verify the logout endpoint: Ensure you're calling the correct endpoint (`/api/sso-logout`)
2. Check authentication: Make sure you're sending valid authentication credentials with the logout request
3. Review token caching: Ensure applications don't cache token validation results

Logout Endpoint Returns Error

Common error scenarios:

- 401 Unauthorized: The access token is invalid or expired. Clear local state and redirect to login.
- 403 Forbidden: The user doesn't have permission to logout. This is rare and may indicate a configuration issue.
- 500 Internal Server Error: Server-side error. Log the error and clear local state anyway.

```
async function logout() {
  try {
    // Replace with your actual Casdoor server URL
    const response = await fetch('https://door.casdoor.com/api/sso-logout', {
      method: 'POST',
      headers: { 'Authorization': `Bearer ${token}` }
    });
  }
}
```

Related Documentation

- [Single Sign-On \(SSO\)](#): Learn how to enable SSO for your applications
- [Casdoor Public API](#): Complete API reference including authentication methods
- [Tokens](#): Understand how Casdoor manages access tokens and sessions
- [OAuth 2.0](#): Learn about OAuth 2.0 flows supported by Casdoor

Vue SDK

Casdoor Vue SDK是为Vue 2和Vue 3设计的，使其使用起来非常方便。

Vue SDK基于casdoor-js-sdk。您也可以直接使用casdoor-js-sdk，这将允许更多的自定义。

请注意，这个插件仍在开发中。如果您有任何问题或建议，请随时通过打开一个[问题](#)与我们联系。

我们现在将向您展示下面的必要步骤。

如果你在阅读README.md后仍然不确定如何使用它，你可以参考这个例子：
[casdoor-python-vue-sdk-example](#)以获取更多详情。

该示例的前端使用casdoor-vue-sdk构建，而后端使用casdoor-python-sdk构建。您可以在示例中查看源代码。

安装

```
# NPM
npm install casdoor-vue-sdk

# Yarn
yarn add casdoor-vue-sdk
```

初始化SDK

要初始化SDK，您需要按照以下顺序提供5个字符串参数：

名称	必需的	描述信息
服务器Url	是	您的Casdoor服务器的URL。
客户端Id:	是	您的Casdoor应用程序的客户端ID。
应用程序名称	是	您的Casdoor应用程序的名称。
组织名称	是	与您的Casdoor应用程序关联的Casdoor组织的名称。
重定向路径	否	您的Casdoor应用程序的重定向URL路径。如果未提供，它将默认为 /callback。

对于 Vue 3：

```
// 在 main.js 中
import Casdoor from 'casdoor-vue-sdk'

const config = {
  serverUrl: "http://localhost:8000",
```

对于 Vue 2:

```
// 在 main.js 中
import Casdoor from 'casdoor-vue-sdk'
import VueCompositionAPI from '@vue/composition-api'

const config = {
  serverUrl: "http://localhost:8000",
  clientId: "4262bea2b293539fe45e",
  organizationName: "casbin",
  appName: "app-casnnode",
  redirectPath: "/callback",
};

Vue.use(VueCompositionAPI)
Vue.use(Casdoor, config)

new Vue({
  render: h => h(App),
}).$mount('#app')
```

示例

```
// in app.vue
<script>
export default {
  name: 'App',
  methods: {
    login() {
      window.location.href = this.getSigninUrl();
    },
    signup() {
      window.location.href = this.getSignupUrl();
    }
}
```

自动修复

如果 `postinstall` 钩子没有被触发，或者你已经更新了Vue版本，尝试运行以下命令来解决重定向问题：

```
npx vue-demi-fix
```

有关切换Vue版本的更多信息，请参考[vue-demi文档](#)。

桌面 SDK

Casdoor的Electron应用示例

这是一个Electron应用程序示例，演示了Casdoor的集成能力。

dotNET 桌面应用

一个用于Casdoor的dotNET桌面应用示例

移动SDKs .NET MAUI应用

Casdoor的.NET MAUI应用示例

Qt 桌面应用程序

一个用于Casdoor的Qt桌面应用示例

Casdoor的Electron应用示例

一个Electron应用示例，演示了Casdoor的集成能力。

如何运行示例

初始化

您需要初始化6个参数，所有这些参数都是字符串类型：

名称	描述	路径
serverUrl	您的Casdoor服务器URL	src/App.js
clientId	您的Casdoor应用程序的客户端ID	src/App.js
appName	您的Casdoor应用程序的名称	src/App.js
redirectPath	如果未提供，您的Casdoor应用程序的重定向URL路径将为 /callback	src/App.js
clientSecret	您的Casdoor应用程序的客户端密钥	src/App.js
casdoorServiceDomain	您的Casdoor服务器URL	public/electron.js

如果您没有设置这些参数，此项目将使用 [Casdoor 在线演示](#) 作为默认的Casdoor 服务器，并使用 [Casnode](#) 作为默认的 Casdoor 应用程序。

可用命令

在项目目录中，您可以运行：

`npm run dev` 或者 `yarn dev`

构建电子应用并运行此应用。

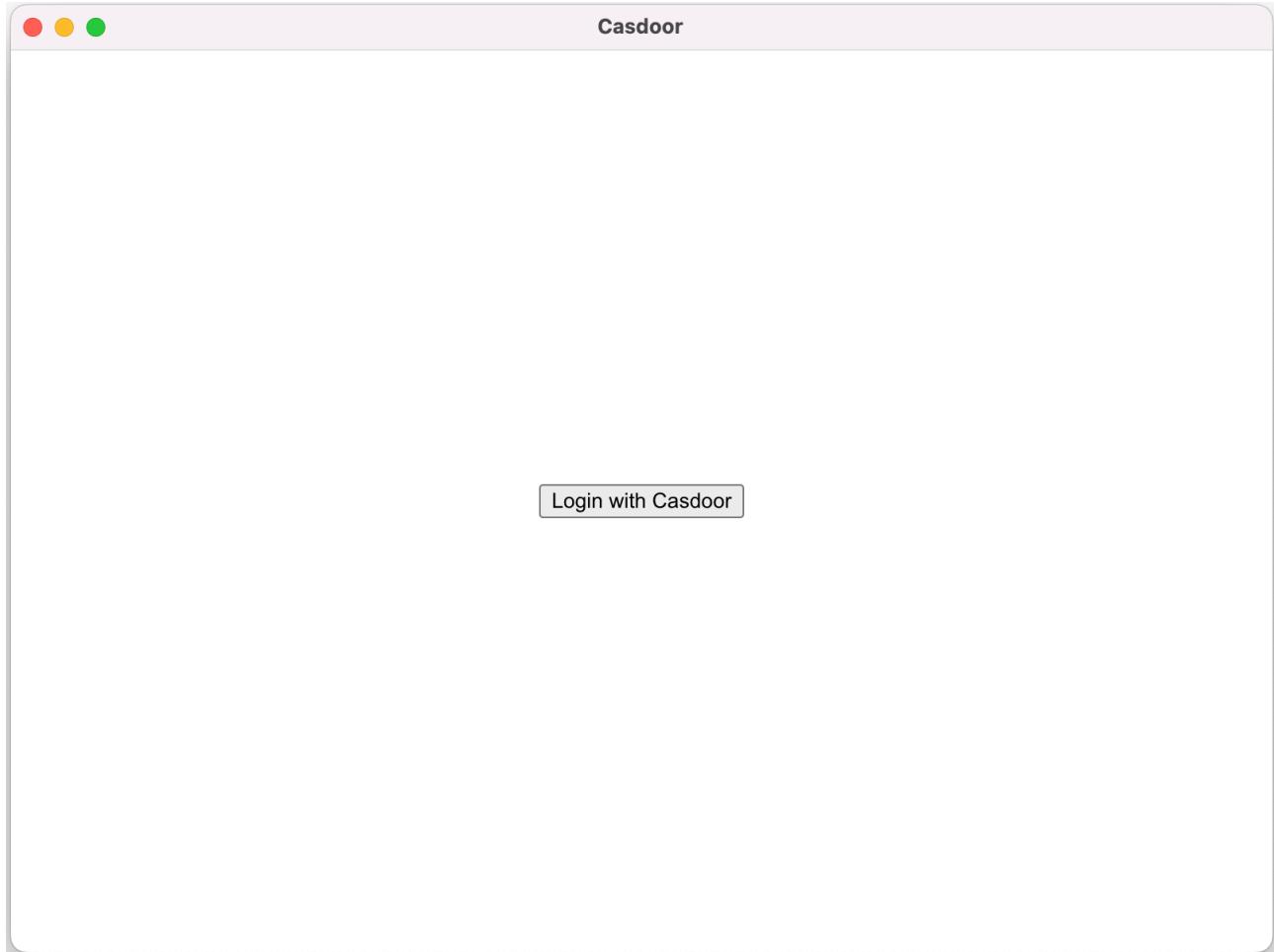
`npm run make` 或者 `yarn make`

打包并分发您的应用程序。它将创建 `out` 文件夹，您的软件包将被定位：

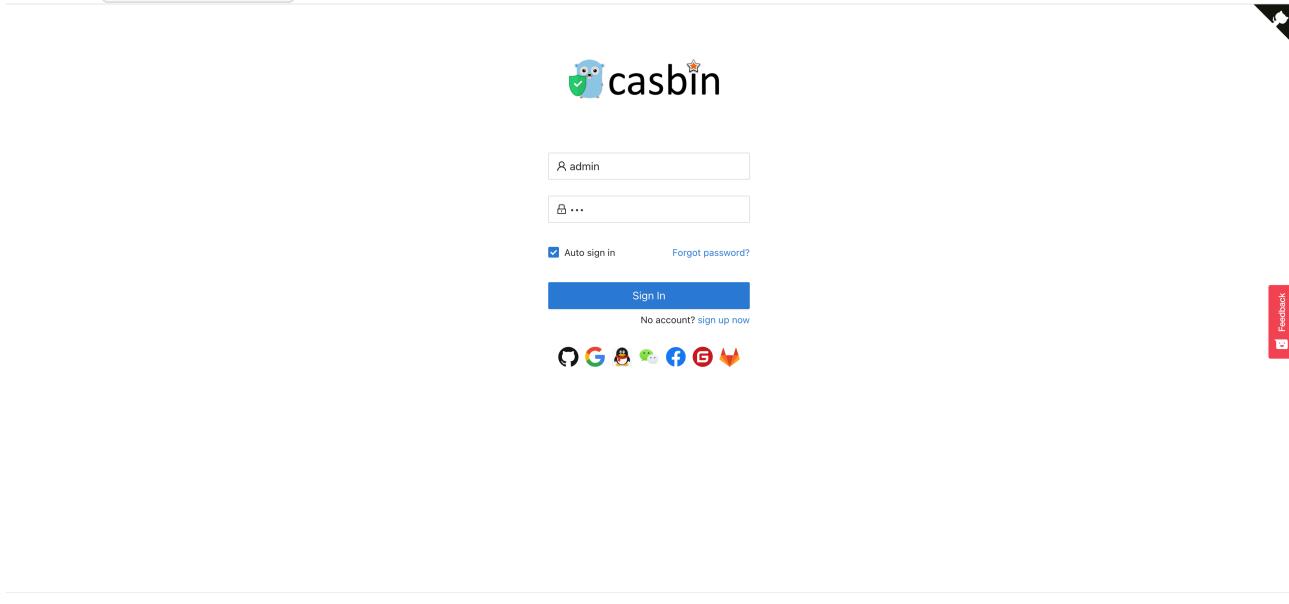
```
// macOS下的out/示例
├── out/make/zip/darwin/x64/casdoor-electron-example-darwin-x64-1.0.0.zip
├── ...
└── out/casdoor-electron-example-darwin-x64/casdoor-electron-example.app/Contents/MacOS/casdoor-electron-example
```

预览

一旦你运行这个Electron应用程序，一个新的窗口将会出现在你的桌面上。



如果你点击 `Login with Casdoor` 按钮，你的默认浏览器将自动打开并显示登录页面。

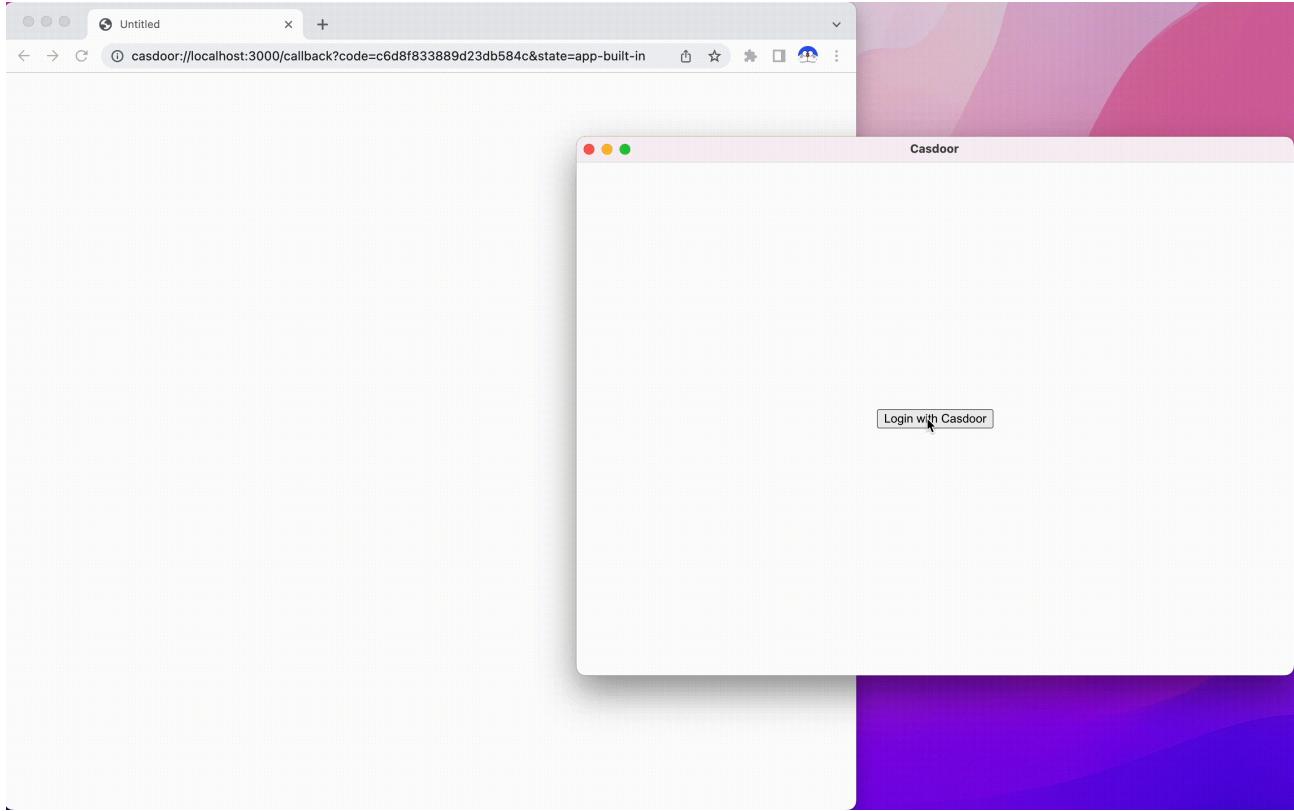


Made with ❤ by Casdoor

登录成功后，您的Electron应用程序将会打开，并且您的用户名将会在您的应用程序上显示。



您可以在下面的gif图像中预览整个过程。



集成步骤

设置自定义协议

首先，您需要设置自定义协议名为 `casdoor`。

```
const protocol = "casdoor";

if (process.defaultApp) {
  if (process.argv.length >= 2) {
    app.setAsDefaultProtocolClient(protocol, process.execPath, [
      path.resolve(process.argv[1]),
    ]);
  }
} else {
  app.setAsDefaultProtocolClient(protocol);
}
```

这将允许浏览器打开你的电子应用程序并将登录信息发送到电子应用程序。

在浏览器中打开登录URL

```
const serverUrl = "https://door.casdoor.com";
const appName = "app-casnnode";
const redirectPath = "/callback";
const clientId = "014ae4bd048734ca2dea";
const clientSecret = "f26a4115725867b7bb7b668c81e1f8f7fae1544d";

const redirectUrl = "casdoor://localhost:3000" + redirectPath;
```

您可以更改前五个参数。

监听开启的应用程序事件

一旦您通过浏览器成功登录，浏览器将打开您的Electron应用程序。因此，你必须监听开放应用程序事件。

```
const gotTheLock = app.requestSingleInstanceLock();
const ProtocolRegExp = new RegExp(`^${protocol}://`);

if (!gotTheLock) {
  app.quit();
} else {
  app.on("second-instance", (event, commandLine, workingDirectory) => {
    if (mainWindow) {
      if (mainWindow.isMinimized()) mainWindow.restore();
      mainWindow.focus();
      commandLine.forEach((str) => {
        if (ProtocolRegExp.test(str)) {
          const params = url.parse(str, true).query;
          if (params && params.code) {
            store.set("casdoor_code", params.code);
            mainWindow.webContents.send("receiveCode", params.code);
          }
        }
      });
    }
  });
  app.whenReady().then(createWindow);

  app.on("open-url", (event, openUrl) => {
    const isProtocol = ProtocolRegExp.test(openUrl);
    if (isProtocol) {
      const params = url.parse(openUrl, true).query;
      if (params && params.code) {
        store.set("casdoor_code", params.code);
        mainWindow.webContents.send("receiveCode", params.code);
      }
    }
  });
}
```

您可以从broswer获取代码，即`casdoor_code`或`params.code`。

解析代码并获取用户信息

```
async function getUserInfo(clientId, clientSecret, code) {
  const { data } = await axios({
    method: "post",
    url: authCodeUrl,
    headers: {
      "content-type": "application/json",
    },
    data: JSON.stringify({
      grant_type: "authorization_code",
      client_id: clientId,
      client_secret: clientSecret,
      code: code,
    }),
  });
  const resp = await axios({
    method: "get",
    url: `${userInfoUrl}?accessToken=${data.access_token}`,
  });
  return resp.data;
```

最后，你可以解析代码并按照[OAuth文档页面](#)获取用户信息。

dotNET 桌面应用

一个用于Casdoor的[Dotnet桌面应用示例](#)。

如何运行示例

先决条件

- [dotNET 6 SDK](#)
- [WebView2 运行时](#) (通常预装在 Windows 上)

初始化

初始化需要5个参数，所有这些参数都是字符串类型：

名称	描述	文件
Domain	您的Casdoor服务器的主机/域	CasdoorVariables.cs
Clientid	您的 Casdoor 应用程序的客户端 ID	CasdoorVariables.cs
AppName	您的Casdoor应用程序的名称	CasdoorVariables.cs
CallbackURL	您的Casdoor应用程序的回调URL路径。如果未提供，它将是 <code>casdoor://callback</code>	CasdoorVariables.cs

名称	描述	文件
ClientSecret	您的Casdoor应用程序的客户端密钥	CasdoorVariables.cs

如果您不设置这些参数，项目将默认使用[Casdoor在线演示](#)作为Casdoor服务器，以及[Casnode](#)作为Casdoor应用程序。

运行中

Visual Studio

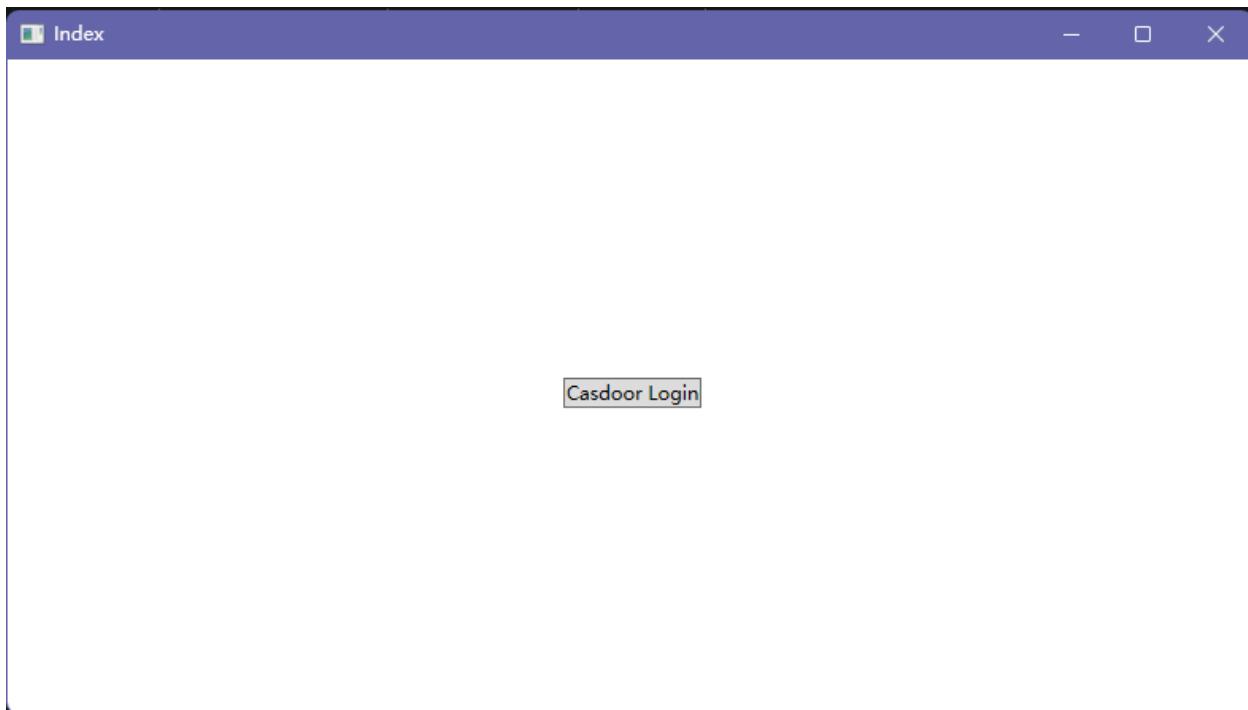
1. 打开 casdoor-dotnet-desktop-example.sln
2. 按 **Ctrl + F5** 开始

命令行

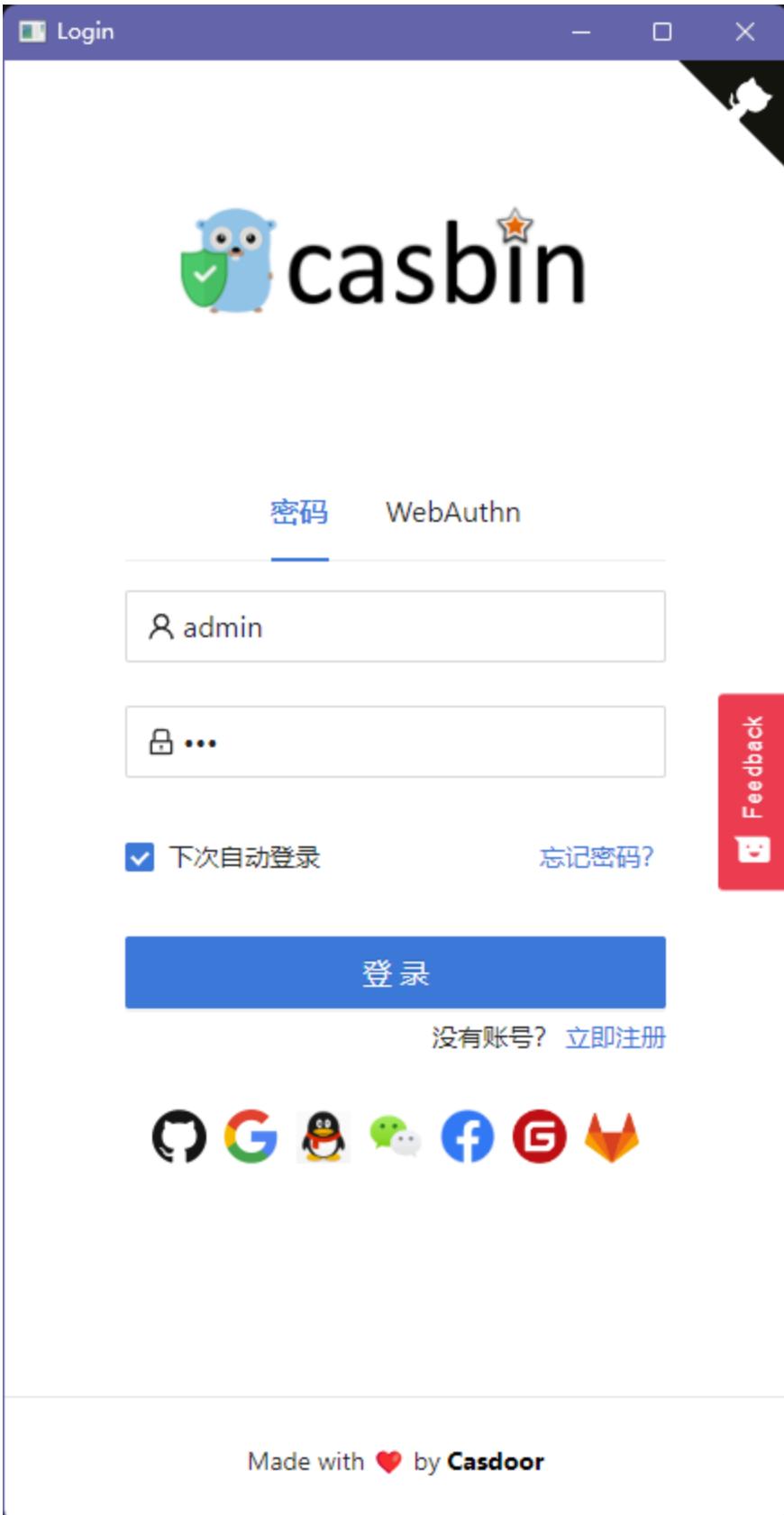
1. **cd src/DesktopApp**
2. **dotnet run**

预览

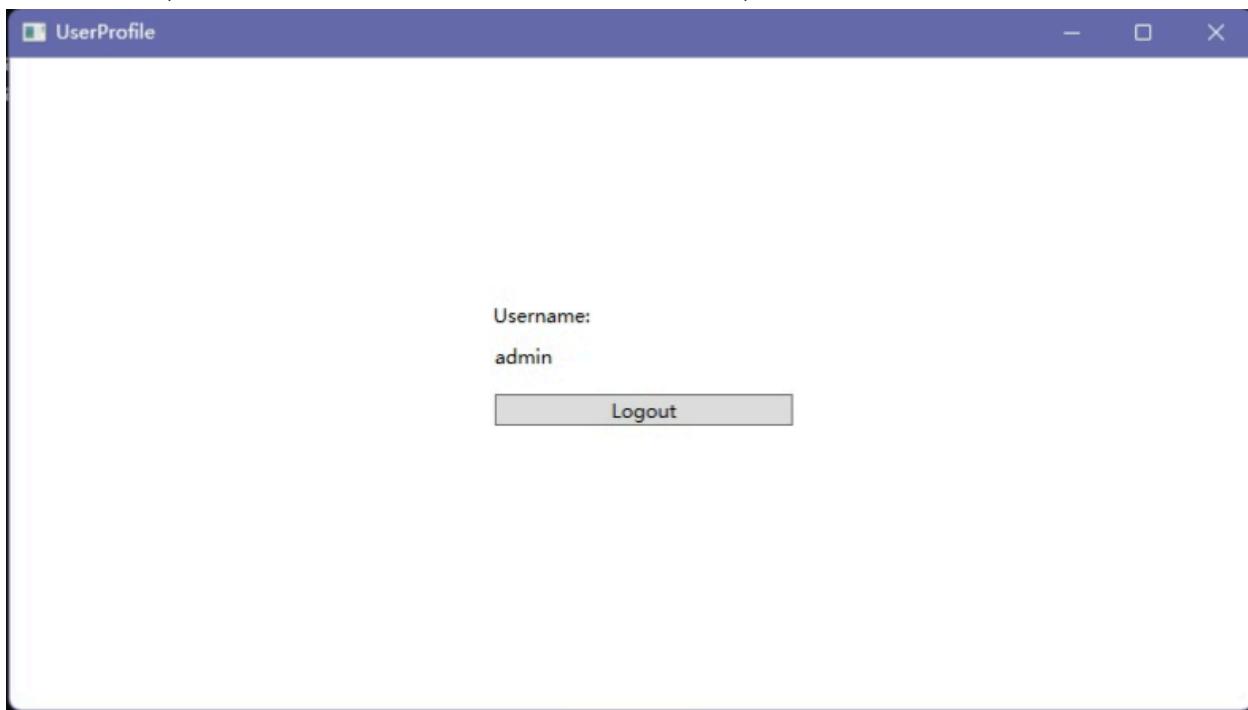
运行dotNET桌面应用程序后，您的桌面上将出现一个新窗口。



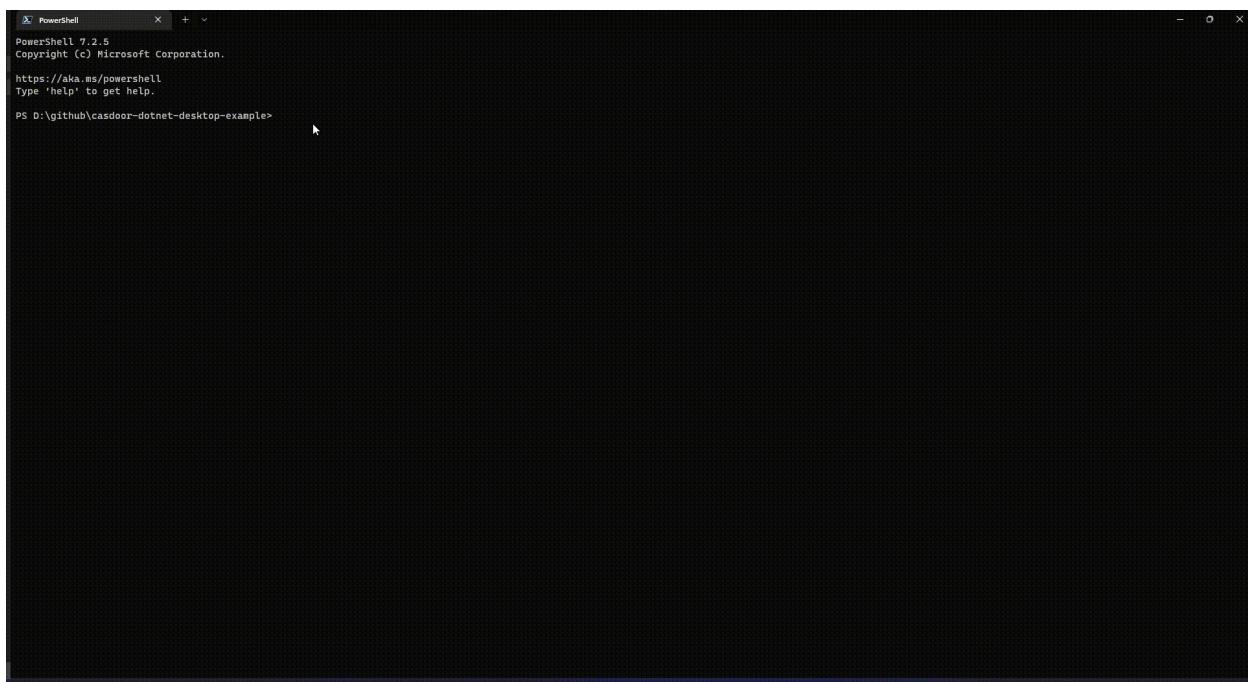
如果你点击 `Casdoor Login` 按钮，一个登录窗口将会出现在你的桌面上。



成功登录后，用户个人资料窗口将出现在您的桌面上，显示您的用户名。



您可以在下面的GIF图像中预览整个过程。



如何集成

打开登录窗口

```
var login = new Login();
// 当登录成功时触发，您将在事件处理器中收到一个授权码
login.CodeReceived += Login_CodeReceived;
login.ShowDialog();
```

使用授权码获取用户信息

```
public async Task<string?> RequestToken(string clientId, string
clientSecret, string code)
{
    var body = new
    {
        grant_type = "authorization_code",
        client_id = clientId,
        client_secret = clientSecret,
        code
    };

    var req = new RestRequest(_requestTokenUrl).AddJsonBody(body);
    var token = await _client.PostAsync<TokenDto>(req);

    return token?.AccessToken;
}

public async Task<UserDto?> GetUserInfo(string token)
{
    var req = new
    RestRequest(_getUserInfoUrl).AddQueryParameter("accessToken",
    token);
```


移动SDKs .NET MAUI应用

此仓库包含一个.NET MAUI应用和.NET MAUI库，用于演示Casdoor通过OpenID Connect进行身份验证。

演示

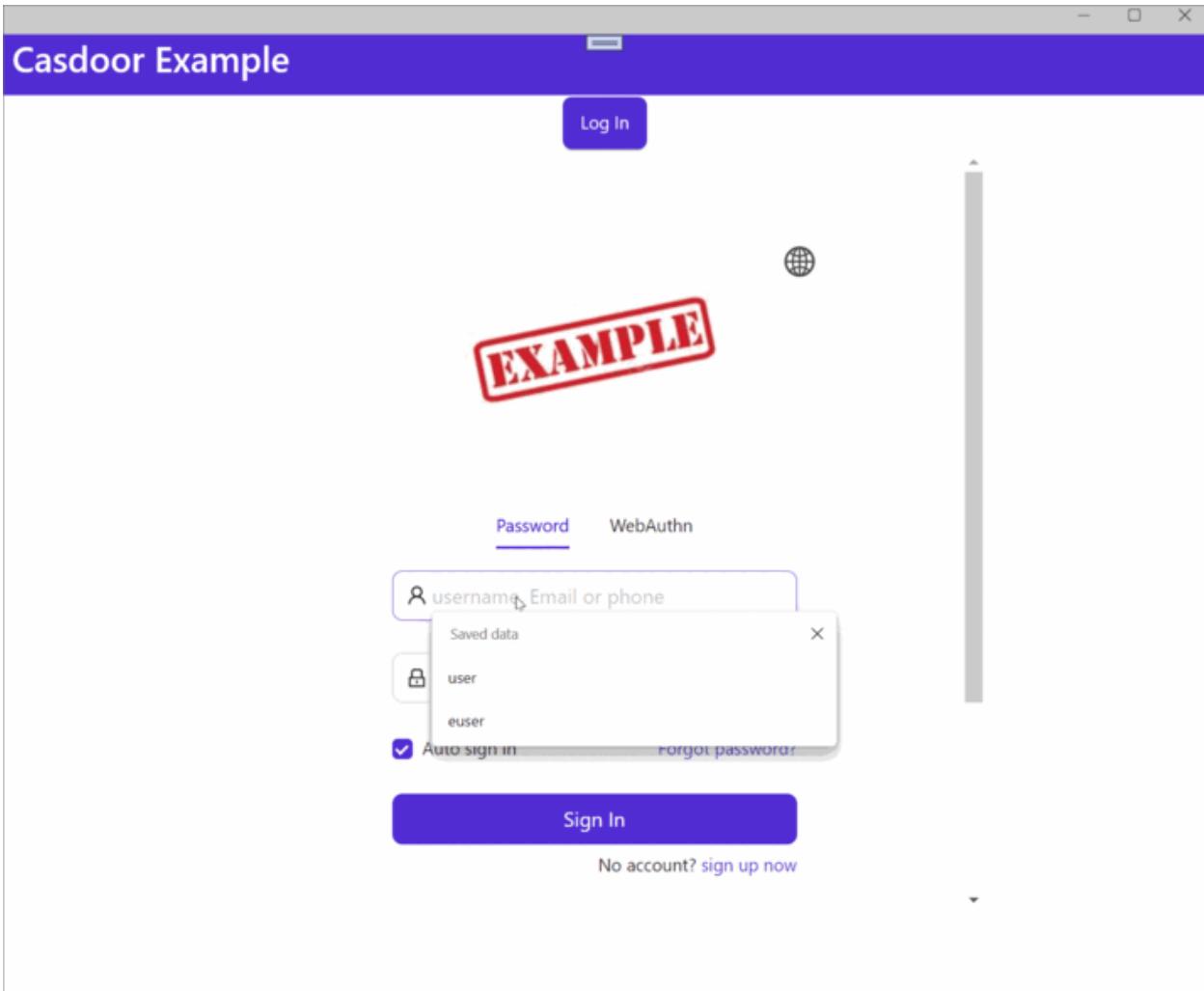
安卓

21:06



.NET

Windows



要求

- 在您的机器上安装.NET 7 SDK
- 需要您的目标平台所需的资产，如[这里](#)所述
- Windows 17.3的Visual Studio 2022或Mac 17.4的Visual Studio 2022（可选）

入门

步骤1：创建一个MAUI应用程序

创建您的MAUI应用程序。

步骤2：添加引用

在您的项目中添加对 `Casdoor.MauiOidcClient` 的引用。

步骤3：添加Casdoor客户端

在服务中将 `CasdoorClient` 添加为单例。

```
builder.Services.AddSingleton(new CasdoorClient(new()
{
    Domain = "<your domain>",
    ClientId = "<your client>",
    Scope = "openid profile email",

#if WINDOWS
    RedirectUri = "http://localhost/callback"
#else
    RedirectUri = "casdoor://callback"
#endif
}));
```

步骤4：设计用户界面

在 `MainPage` 文件中添加代码。

MainPage.xaml

```
<?xml version="1.0" encoding="utf-8" ?>
<ContentPage xmlns="http://schemas.microsoft.com/dotnet/2021/maui"
    xmlns:x="http://schemas.microsoft.com/winfx/2009/xaml"
    x:Class="Casdoor.MauiOidcClient.Example.MainPage">

    <ScrollView>
        <VerticalStackLayout>

            <StackLayout
                x:Name="LoginView">
                <Button
                    x:Name="LoginBtn"
                    Text="Log In"
                    SemanticProperties.Hint="Click to log in"
                    Clicked="OnLoginClicked"
                    HorizontalOptions="Center" />

                <WebView x:Name="WebViewInstance" />
            </StackLayout>

            <StackLayout
                x:Name="HomeView"
                IsVisible="false">

                <Label
                    Text="Welcome to .NET Multi-platform App UI"
                    SemanticProperties.HeadingLevel="Level2"
                    SemanticProperties.Description="Welcome to dot net
Multi-platform App UI"
                    FontSize="18"
                    HorizontalOptions="Center" />

                <Button
                    x:Name="CounterBtn"
                    Text="Click me"
```

MainPage.cs

```
namespace Casdoor.MauiOidcClient.Example
{
    public partial class MainPage : ContentPage
    {
        int count = 0;
        private readonly CasdoorClient client;
        private string accessToken;
        public MainPage(CasdoorClient client)
        {
            InitializeComponent();
            this.client = client;

#if WINDOWS
            client.Browser = new
                WebViewBrowserAuthenticator(WebViewInstance);
#endif
        }

        private void OnCounterClicked(object sender, EventArgs e)
        {
            count++;

            if (count == 1)
                CounterBtn.Text = $"Clicked {count} time";
            else
                CounterBtn.Text = $"Clicked {count} times";

            SemanticScreenReader.Announce(CounterBtn.Text);
        }

        private async void OnLoginClicked(object sender, EventArgs e)
        {
            var loginResult = await client.LoginAsync();
            accessToken = loginResult.AccessToken;
```

步骤5：支持Android平台

修改 `AndroidManifest.xml` 文件。

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/
    android">
    <application android:allowBackup="true" android:icon="@mipmap/
        appicon" android:roundIcon="@mipmap/appicon_round"
        android:supportsRtl="true"></application>
    <uses-permission
        android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <queries>
        <intent>
            <action
                android:name="android.support.customtabs.action.CustomTabsService"
            />
            </intent>
        </queries>
    </manifest>
```

步骤6：启动应用程序

Visual Studio：按Ctrl + F5开始。

Qt 桌面应用程序

一个为 Casdoor 的 [Qt桌面应用程序示例](#)。

如何运行这个示例

前置要求

- [Qt6 SDK](#)
- [OpenSSL工具包](#)

初始化

你需要初始化7个字符串参数：

名称	描述	文件
endpoint	您的 Casdoor 服务器主机/域	mainwindow.h
client_id	您的 Casdoor 应用程序的客户端 ID	mainwindow.h
client_secret	你的Casdoor应用的客户端密钥	mainwindow.h
certificate	Casdoor 应用程序证书的公钥	mainwindow.h
org_name	您的Casdoor应用程序的名称	mainwindow.h

名称	描述	文件
app_name	您的Casdoor应用程序的名称	mainwindow.h
redirect_url	您的Casdoor 应用程序的回调URL路径将是 casdoor://callback 如果没有提供	mainwindow.h

如果你不设置 endpoint 参数，这个项目将使用<http://localhost:8000>作为默认的 Casdoor服务器。

运行应用程序

使用Qt Creator

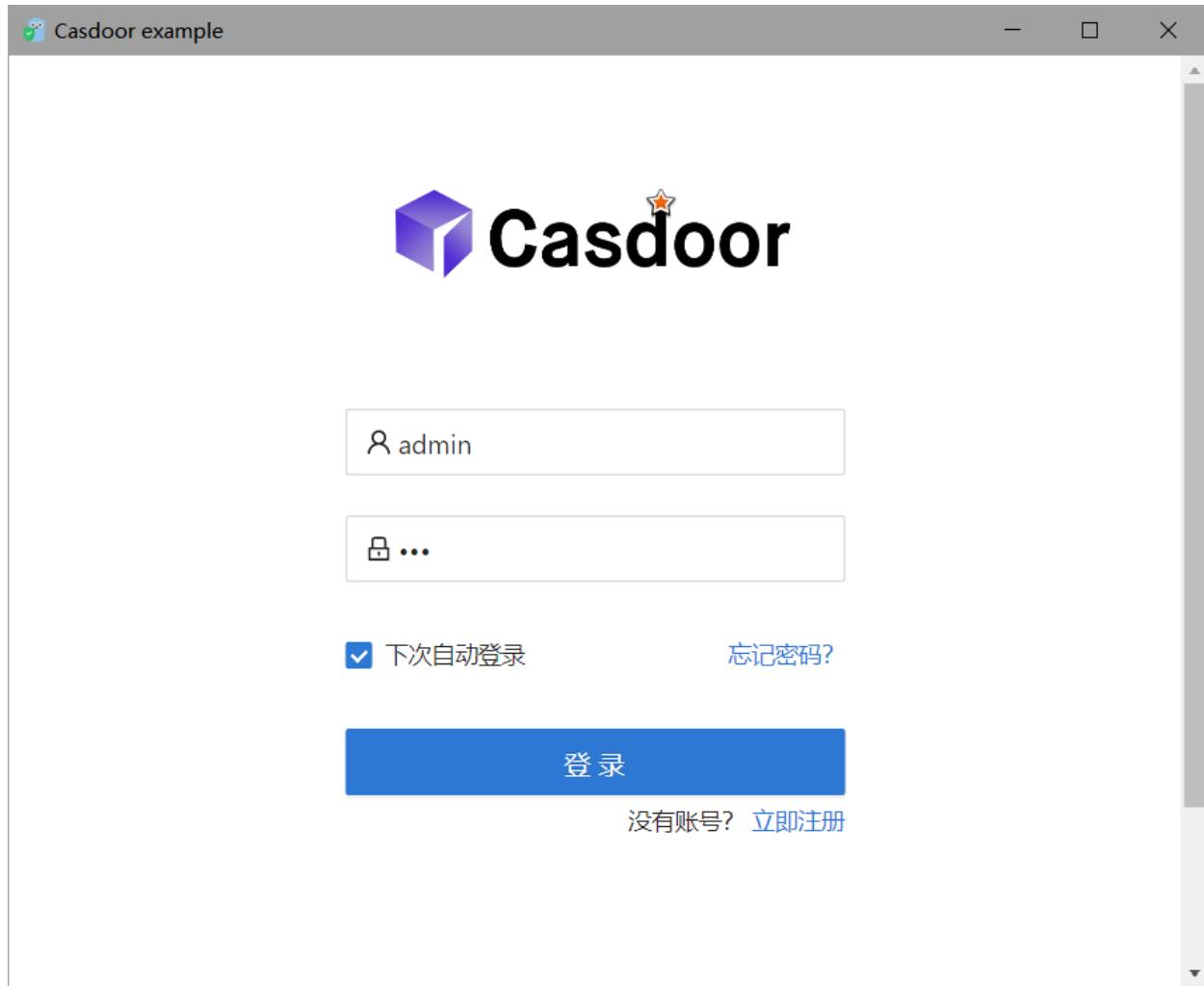
1. 打开 casdoor-cpp-qt-example.pro
2. 在 casdoor-cpp-qt-example.pro 中设置 OpenSSL 的 INCLUDEPATH
3. 按 Ctrl + R 开始

效果预览

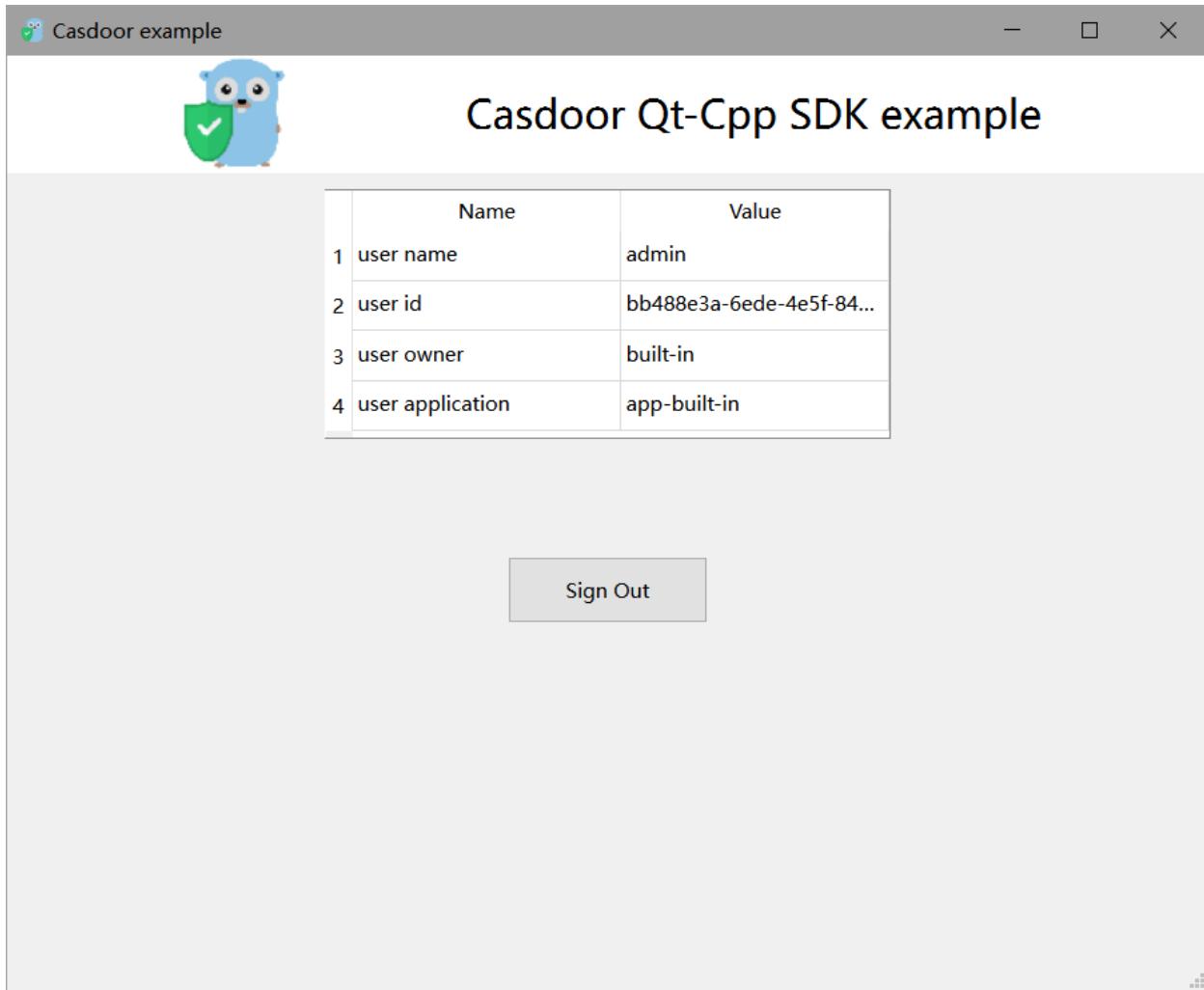
运行这个Qt桌面应用后，你的桌面上会显示一个新窗口。



如果你点击 `Sign In` 按钮，你的桌面上会显示一个登录窗口。



登录成功后，你的桌面上会显示一个用户资料窗口，显示你的用户信息。



你可以在下面的GIF图像中预览整个过程。



如何集成

打开登录窗口

```
// Load and display the login page of Casdoor
m_webview->page()->load(*m_signin_url);
m_webview->show();
```

监听打开应用事件

```
// Initialize the TcpServer object and listen on port 8080
m_tcpserver = new QTcpServer(this);
if (!m_tcpserver->listen(QHostAddress::LocalHost, 8080)) {
    qDebug() << m_tcpserver->errorString();
    close();
}
connect(m_tcpserver, SIGNAL(newConnection()), this,
SLOT(on_tcp_connected()));
```

使用授权码获取用户信息

```
// 获取令牌并使用JWT库解析
std::string token = m_casdoor->GetOAuthToken(code.toStdString());
auto decoded = m_casdoor->ParseJwtToken(token);
```

移动 SDKs

React Native应用

Casdoor的React Native移动应用示例

React Native应用

这里有一个[Casdoor React Native移动应用示例](#), 可以帮助你快速了解如何在React Native中使用Casdoor。

如何运行示例

快速开始

- 下载代码

```
git clone git@github.com:casdoor/casdoor-react-native-example.git
```

- 安装依赖

```
cd casdoor-react-native-example
yarn install
cd ios/
pod install
```

- 在ios上运行

```
cd casdoor-react-native-example
react-native start
react-native run-ios
```

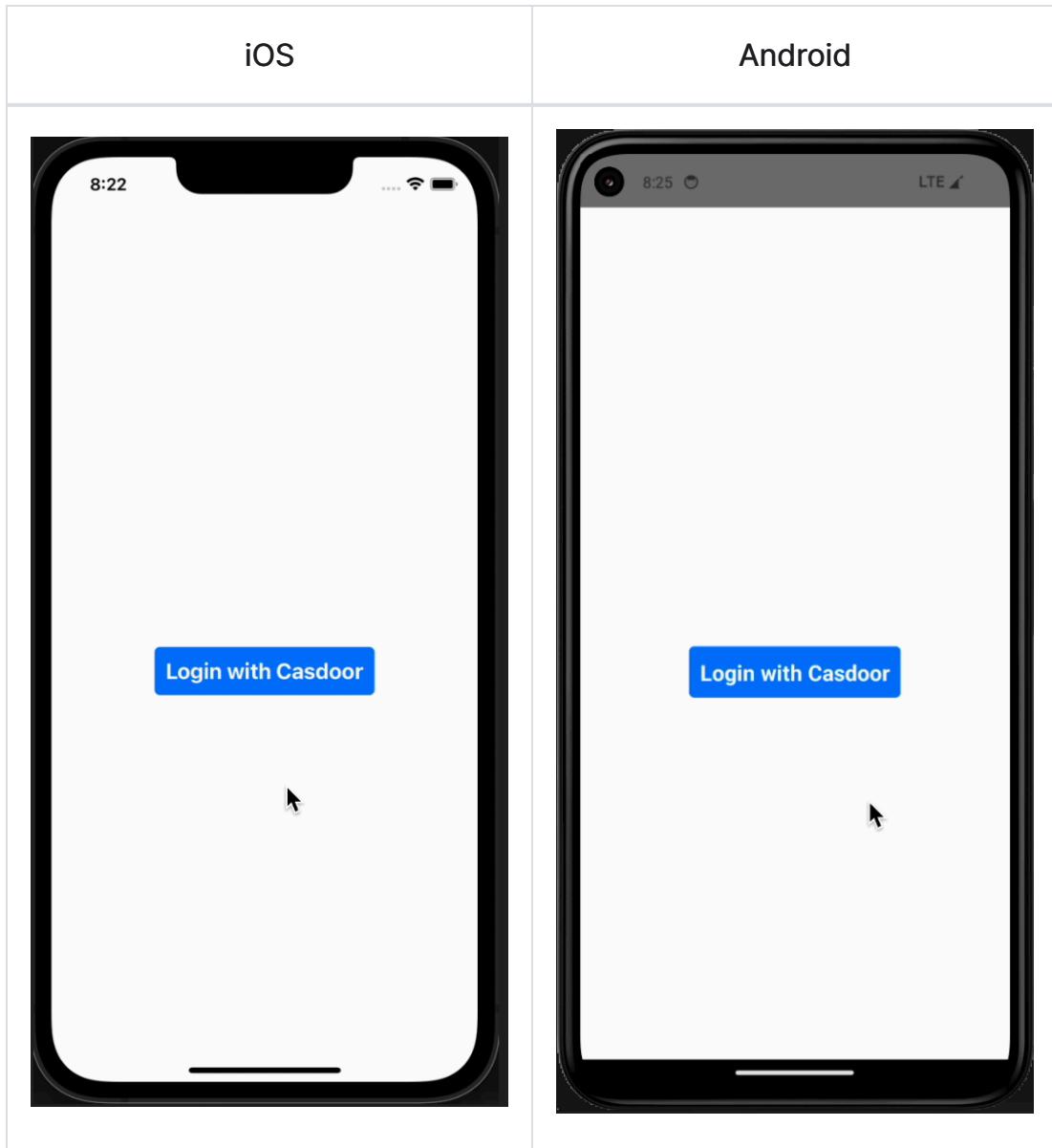
- 在android上运行

```
cd casdoor-react-native-example  
react-native start  
react-native run-android
```

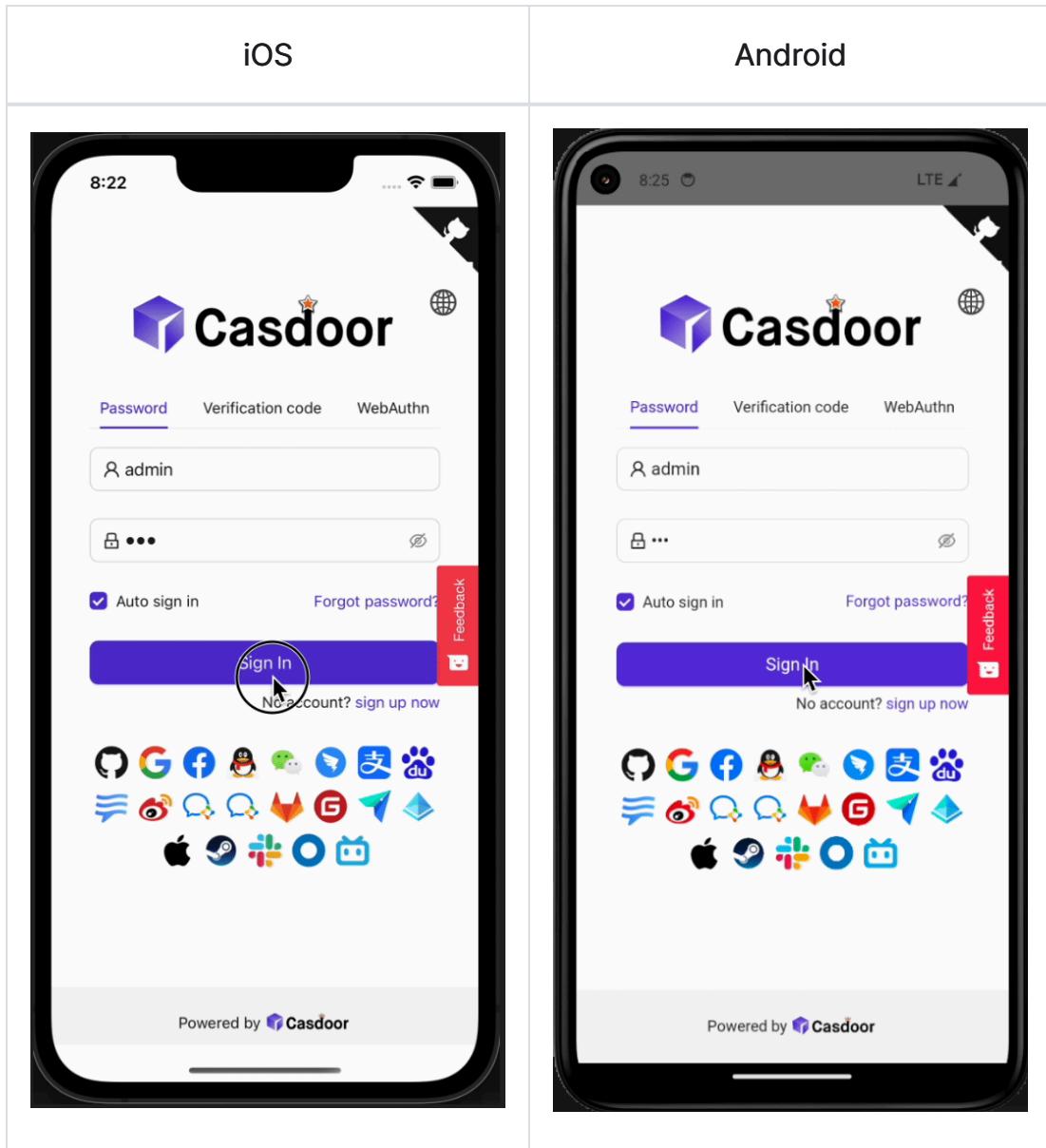
确保在运行之前打开模拟器或真实设备。

预览

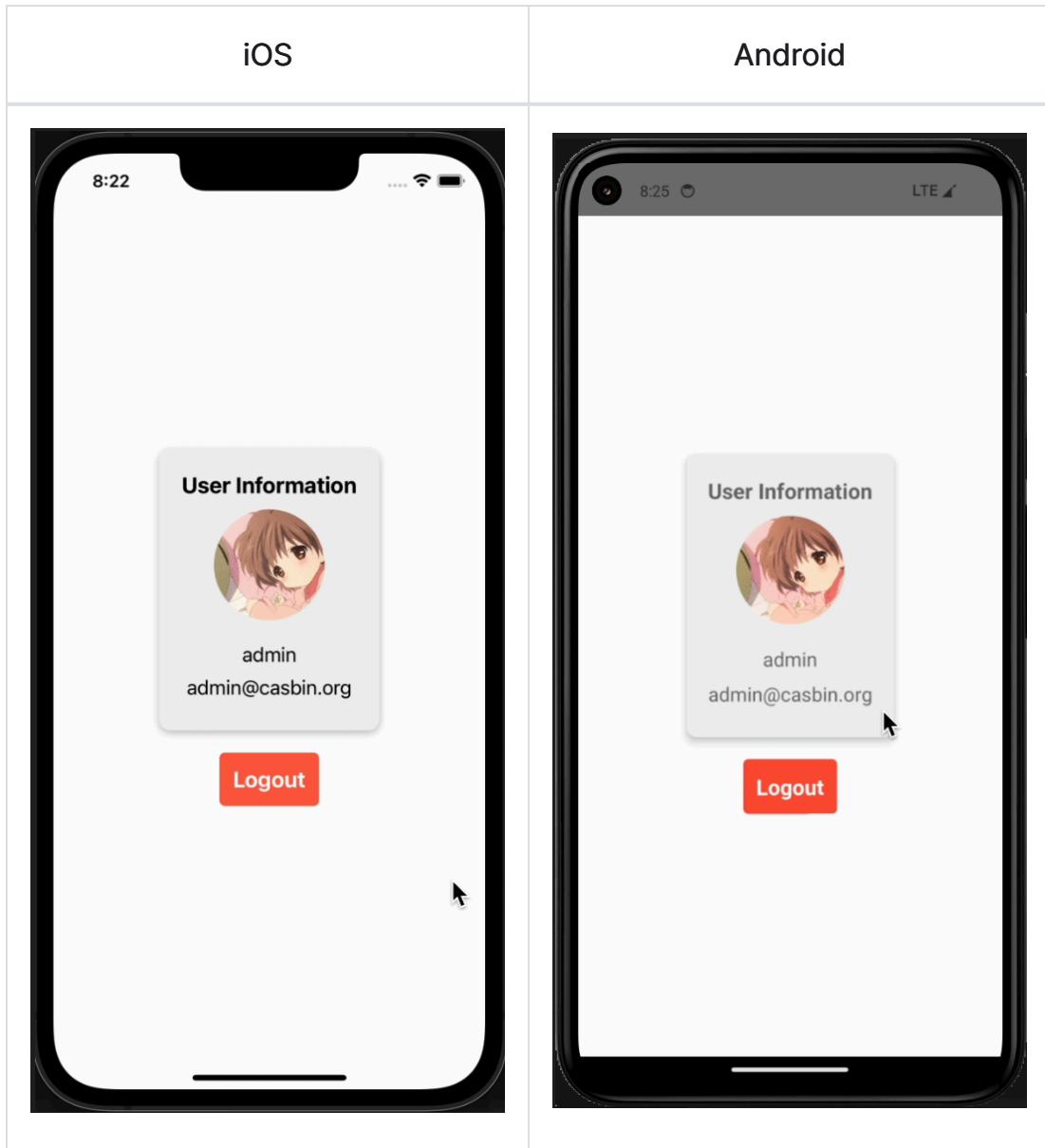
运行这个react-native-example移动应用后，以下窗口将在模拟器或真实设备上显示。



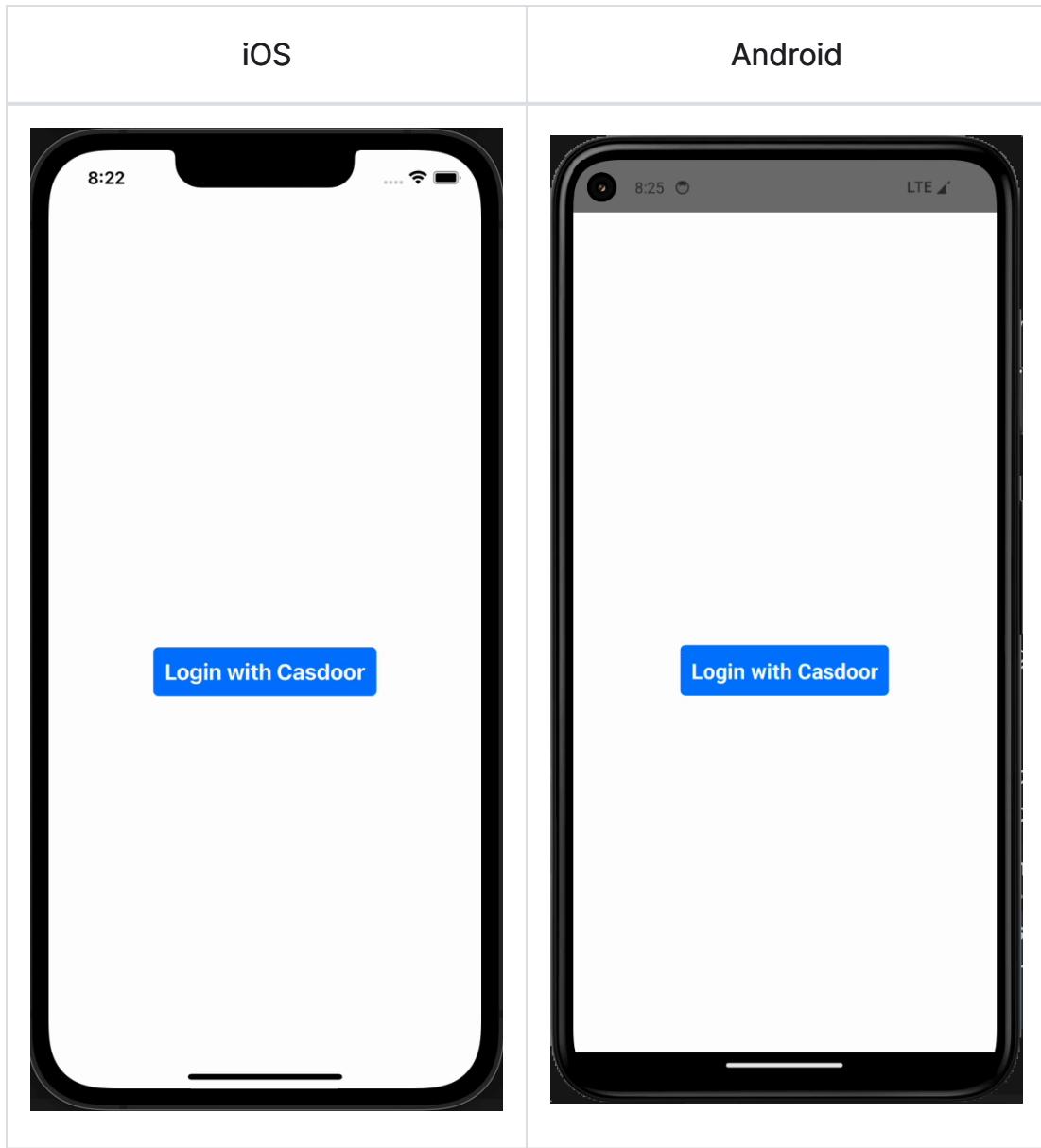
如果你点击 `使用Casdoor登录` 按钮，Casdoor登录窗口将出现在屏幕上。



登录成功后，一个用户资料窗口将出现在你的屏幕上，显示你的用户信息。



你可以在下面的GIF图像中预览整个过程。



如何集成

上述示例使用了[casdoor-react-native-sdk](#)，你也可以在你自己的项目中集成这个sdk。

集成和使用sdk非常简单，下面的步骤将向你展示如何集成和使用：

步骤1：导入SDK

```
# NPM  
npm i casdoor-react-native-sdk  
  
# Yarn  
yarn add casdoor-react-native-sdk
```

步骤2：初始化SDK

初始化需要7个参数，都是字符串类型：

名称（按顺序）	必须	描述
serverUrl	是	你的Casdoor服务器URL
clientId	是	你的Casdoor应用的客户端ID
appName	是	你的Casdoor应用的名称
organizationName	是	与你的Casdoor应用关联的Casdoor组织的名称
redirectPath	否	你的Casdoor应用的重定向URL的路径，如果未提供，将是 /callback
signinPath	否	你的Casdoor应用的登录URL的路径

```
import SDK from 'casdoor-react-native-sdk'

const sdkConfig = {
  serverUrl: 'https://door.casdoor.com',
  clientId: 'b800a86702dd4d29ec4d',
  appName: 'app-example',
  organizationName: 'casbin',
  redirectPath: 'http://localhost:5000/callback',
  signinPath: '/api/signin',
};
const sdk = new SDK(sdkConfig)
```

步骤3：使用SDK

在适当的地方使用sdk的相应API接口。

最简单的casdoor授权和认证过程可以通过使用以下三个API实现：

```
// 获取登录url
getSigninUrl()

// 获取访问令牌
getAccessToken(redirectUrl); // http://localhost:5000/
callback?code=b75bc5c5ac65ffa516e5&state=gjmfqf498

// 解码jwt令牌以获取用户信息
JwtDecode(jwtToken)
```

如果你想使用其他接口，请查看[casdoor-react-native-sdk](#)以获取更多帮助。



> 如何连接到Casdoor

> Casdoor CLI

Casdoor CLI

Casdoor CLI is the official command-line interface for [Casdoor](#), providing a powerful and intuitive way to manage your Casdoor identity and access management system directly from the terminal.

GitHub repository: <https://github.com/casdoor/casdoor-cli>

Features

OAuth2 Browser-Based Authentication

The CLI uses a secure browser-based OAuth2 flow for authentication, ensuring your credentials are protected through Casdoor's standard authentication mechanism.

Secure Token Storage

Credentials are safely stored using your system's keyring interface (GNOME Keyring on Linux, Keychain on macOS), ensuring tokens never touch disk in plaintext.

User Management

Create, update, and delete users with ease directly from the command line.

Permission Management

Control user permissions through Casdoor's group feature with built-in roles:

- `lector`: Read-only access
- `editor`: Can create users, with limited modification rights
- `administrator`: Full control over user creation, modification, and deletion

Group Management

Create, modify, and delete user groups to organize users and manage permissions efficiently.

Installation

Prerequisites

- Go 1.22.0 or higher
- macOS or Linux operating system
- GNOME Keyring (Linux) or Keychain (macOS) for secure credential storage

注意事项

Platform Support: Currently supports macOS and Linux (tested on Debian 12 and macOS Sonoma). Windows support via WSL is not available as the CLI requires GNOME's Secret Service DBus interface (GNOME Keyring) for secure credential storage.

macOS

```
make build TARGET_OS=darwin && make install TARGET_OS=darwin
```

Linux

```
make build TARGET_OS=linux && make install TARGET_OS=linux
```

Configure Your Shell

After installation, add `casdoor-cli` to your `PATH`:

For Bash users:

```
echo 'export PATH="/usr/local/bin:$PATH"' >> ~/.bashrc
source ~/.bashrc
```

For Zsh users:

```
echo 'export PATH="/usr/local/bin:$PATH"' >> ~/.zshrc
source ~/.zshrc
```

Verify the installation:

```
casdoor --help
```

Configuration

Casdoor Server Setup

To use the CLI, you need a configured Casdoor application. You have two options:

1. **Using the provided bootstrap data:** An `init_data.json` file is included in the repository to quickly bootstrap Casdoor's configuration. Refer to the [Data Initialization documentation](#) for initialization instructions.
2. **Manual configuration:** Create an application directly in your Casdoor admin panel and configure it according to your requirements.

CLI Configuration

On first launch, `casdoor-cli` will prompt you to provide a `config.yaml` file containing your Casdoor connection details. See the included `config.yaml.example` file in the repository for reference.

Required configuration fields:

```
application_name: your-app-name
casdoor_endpoint: https://your-casdoor-instance.com
certificate: |
  -----BEGIN CERTIFICATE-----
  Your certificate content here
  -----END CERTIFICATE-----
client_id: your-client-id
client_secret: your-client-secret
organization_name: your-organization
redirect_uri: http://localhost:9000/callback
```

Your configuration will be securely stored in `~/.casdoor-cli/config.yaml` (base64 encoded) for subsequent use.

Usage

Available Commands

Usage:

```
casdoor [command]
```

Available Commands:

completion	Generate the autocompletion script <code>for</code> the specified shell
<code>groups</code>	Manage Casdoor permissions
help	Help about any command
login	Login to your Casdoor account
logout	Logout from your Casdoor account
<code>users</code>	Manage Casdoor <code>users</code>

Flags:

<code>-d, --debug</code>	verbose logging
<code>-h, --help</code>	help <code>for</code> casdoor

Login

To authenticate with your Casdoor instance:

```
casdoor login
```

This will open your default browser for OAuth2 authentication.

Managing Users

```
# List users
casdoor users list

# Create a user
casdoor users create

# Update a user
casdoor users update

# Delete a user
casdoor users delete
```

Managing Groups

```
# List groups
casdoor groups list

# Create a group
casdoor groups create

# Update a group
casdoor groups update

# Delete a group
casdoor groups delete
```

Logout

To logout from your Casdoor account:

```
casdoor logout
```

Development

Local Development Environment

A Docker Compose environment is provided in the repository for local testing and development:

```
docker compose up -d
```

ⓘ 备注

Allow a few moments for the Casdoor container to fully initialize. The container will restart multiple times as it sets up the database.

Development Configuration

Create a `config.yaml` file from the provided `config.yaml.example` template at the repository root with your local development settings.

Testing the CLI

Test the login functionality with the default development credentials provided in the repository documentation.

Run directly with Go:

```
go run main.go login
```

Or build and install first:

```
make build TARGET_OS=darwin && make install TARGET_OS=darwin  #
For macOS
# OR
make build TARGET_OS=linux && make install TARGET_OS=linux      #
For Linux

casdoor login
```

Casdoor插件

Casdoor还为一些非常流行的平台提供插件或中间件，例如Java的Spring Boot，PHP的WordPress，Python的Odoo等等。

For command-line interface integration, see the [Casdoor CLI](#) documentation.

Casdoor 插件	语言	源代码
Spring Boot插件	Java	https://github.com/casdoor/casdoor-spring-boot-starter
Spring Boot示例	Java	https://github.com/casdoor/casdoor-spring-boot-example
WordPress 插件	PHP	https://github.com/casdoor/wordpress-casdoor-plugin
Odoo 插件	Python	https://github.com/casdoor/odoo-casdoor-oauth
Django 插件	Python	https://github.com/casdoor/django-casdoor-auth
Chrome extension	JavaScript	https://github.com/casdoor/casdoor-chrome-extension

要获取官方Casdoor插件的完整列表，请访问[Casdoor仓库](#)。

Chrome Extension

`casdoor-chrome-extension` is an example of how to integrate Casdoor in a Chrome browser extension. We will guide you through the steps below.

Step 1: Deploy Casdoor

Firstly, Casdoor should be deployed.

You can refer to the Casdoor official documentation for the [Server Installation](#). Please deploy your Casdoor instance in production mode.

After a successful deployment, make sure the following:

- Open your favorite browser and visit <http://localhost:8000>. You will see the login page of Casdoor.
- Test the login functionality by entering `admin` as the username and `123` as the password.

After that, you can quickly implement a Casdoor-based login page in your Chrome extension using the following steps.

Step 2: Configure Casdoor Application

Before using Casdoor for authentication in your Chrome extension, you need to configure a Casdoor application:

1. Go to your Casdoor instance and navigate to [Applications](#).
2. Create a new application or use an existing one.
3. Configure the application settings:
 - Set the [Redirect URLs](#) to include your Chrome extension URL. For example: `https://<extension-id>.chromiumapp.org/` or `http://localhost:3000/callback` for development.
 - Note down the [Client ID](#) and [Client Secret](#).
 - Make sure the application has proper OAuth settings enabled.

Step 3: Set Up Chrome Extension

1. Create Manifest File

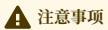
Create a `manifest.json` file in your Chrome extension project with the necessary permissions:

```
{  
  "manifest_version": 3,  
  "name": "Casdoor Chrome Extension",  
  "version": "1.0.0",  
  "description": "Chrome extension integrated with Casdoor",  
  "permissions": [  
    "identity",  
    "storage"  
  ],  
  "host_permissions": [  
    "http://localhost:8000/*",  
    "https://door.casdoor.com/*"  
  ],  
  "action": {  
    "default_popup": "popup.html",  
    "default_icon": {  
      "16": "icons/icon16.png",  
      "48": "icons/icon48.png",  
      "128": "icons/icon128.png"  
    }  
  }  
}
```

2. Configure Extension Identity

In the `manifest.json`, you may need to add OAuth2 configuration if using Chrome's identity API:

```
{  
  "oauth2": {  
    "client_id": "your-client-id.apps.googleusercontent.com",  
    "scopes": ["openid", "profile", "email"]  
  }  
}
```



Replace the configuration values with your own Casdoor instance, especially the `client_id` and the host permissions URLs.

Step 4: Implement Authentication Flow

1. Create Background Script

Create a `background.js` file to handle the authentication:

```
const CASDOOR_ENDPOINT = "http://localhost:8000";  
const CLIENT_ID = "your-client-id";  
const CLIENT_SECRET = "your-client-secret";  
const ORGANIZATION_NAME = "built-in";  
const APPLICATION_NAME = "app-built-in";  
const REDIRECT_URI = chrome.identity.getRedirectURL();  
  
// Generate the authorization URL  
function getAuthUrl() {  
  const state = Math.random().toString(36).substring(7);  
  const authUrl = `${CASDOOR_ENDPOINT}/login/oauth/  
authorize?client_id=${CLIENT_ID}&response_type=code&redirect_uri=${encodeURIComponent(REDIRECT_URI)}&scope=openid%20profile%20email&state=${state}`;  
  
  chrome.storage.local.set({ oauthState: state });  
  
  return authUrl;  
}  
  
// Handle OAuth callback  
async function handleOAuthCallback(redirectUrl) {  
  const url = new URL(redirectUrl);  
  const code = url.searchParams.get('code');  
  const state = url.searchParams.get('state');  
  
  // Verify state  
  const { oauthState } = await chrome.storage.local.get('oauthState');  
  if (state !== oauthState) {  
    throw new Error('Invalid state parameter');  
  }  
  
  // Exchange code for token  
  const tokenResponse = await fetch(`${CASDOOR_ENDPOINT}/api/login/oauth/access_token`, {  
    method: 'POST',  
    headers: {  
      'Content-Type': 'application/json',  
    },  
    body: JSON.stringify({  
      grant_type: 'authorization_code',  
      client_id: CLIENT_ID,  
    }),  
  }).  
  .then(response => response.json())  
  .catch(error => console.error(error));  
  
  const { access_token, refresh_token } = tokenResponse;  
  const userResponse = await fetch(`${CASDOOR_ENDPOINT}/api/user/me`, {  
    headers: {  
      Authorization: `Bearer ${access_token}`  
    },  
  }).  
  .then(response => response.json())  
  .catch(error => console.error(error));  
  
  const user = userResponse.data;  
  const userStorage = {  
    id: user.id,  
    name: user.name,  
    email: user.email,  
    roles: user.roles,  
    organization: user.organization,  
    application: user.application,  
    picture: user.picture,  
  };  
  
  chrome.storage.local.set({ user });  
  chrome.tabs.create({  
    url: `${CASDOOR_ENDPOINT}/#/profile`  
  });  
}
```

2. Create Popup HTML

Create a `popup.html` file for the extension popup:

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Casdoor Login</title>
  <style>
    body {
      width: 300px;
      padding: 20px;
      font-family: Arial, sans-serif;
    }
    button {
      width: 100%;
      padding: 10px;
      margin: 5px 0;
      cursor: pointer;
      background-color: #4285f4;
      color: white;
      border: none;
      border-radius: 4px;
    }
    button:hover {
      background-color: #357ae8;
    }
    #user-info {
      margin-top: 20px;
    }
  </style>
</head>
<body>
  <div id="login-section">
    <h2>Casdoor Login</h2>
    <button id="login-btn">Login with Casdoor</button>
  </div>

  <div id="user-section" style="display: none;">
    <h2>Welcome!</h2>
    <div id="user-info"></div>
    <button id="logout-btn">Logout</button>
  </div>

  <script src="popup.js"></script>
</body>
</html>
```

3. Create Popup Script

Create a `popup.js` file to handle user interactions:

```
document.addEventListener('DOMContentLoaded', () => {
  const loginSection = document.getElementById('login-section');
  const userSection = document.getElementById('user-section');
  const loginBtn = document.getElementById('login-btn');
  const logoutBtn = document.getElementById('logout-btn');
  const userInfo = document.getElementById('user-info');

  // Check if user is already logged in
  chrome.runtime.sendMessage({ action: 'getUser' }, (response) => {
    if (response.user) {
```

Step 5: Load and Test the Extension

1. Open Chrome and navigate to `chrome://extensions/`.
2. Enable **Developer mode** in the top right corner.
3. Click **Load unpacked** and select your extension directory.
4. Click on the extension icon in the Chrome toolbar.
5. Click the **Login with Casdoor** button to test the authentication flow.

Step 6: Handle Token Storage and Refresh

To maintain user sessions, you should implement token refresh logic:

```
async function refreshToken(refreshToken) {  
  const response = await fetch(`[${CASDOOR_ENDPOINT}]/api/login/oauth/refresh_token`, {  
    method: 'POST',  
    headers: {  
      'Content-Type': 'application/json',  
    },  
    body: JSON.stringify({  
      grant_type: 'refresh_token',  
      refresh_token: refreshToken,  
      client_id: CLIENT_ID,  
      client_secret: CLIENT_SECRET,  
    }),  
  });  
  
  return await response.json();  
}  
  
// Check token validity and refresh if needed  
async function getValidAccessToken() {  
  const { user } = await chrome.storage.local.get('user');  
  
  if (!user || !user.access_token) {  
    return null;  
  }  
  
  // Check if token is expired (decode JWT)  
  try {  
    const payload = JSON.parse(atob(user.access_token.split('.')[1]));  
    const expiry = payload.exp * 1000; // Convert to milliseconds  
  
    if (Date.now() >= expiry) {  
      // Token expired, refresh it  
      if (user.refresh_token) {  
        const newTokens = await refreshToken(user.refresh_token);  
        await chrome.storage.local.set({ user: newTokens });  
        return newTokens.access_token;  
      }  
      return null;  
    }  
  
    return user.access_token;  
  } catch (error) {  
    console.error('Error checking token validity:', error);  
    return null;  
  }  
}
```

What's More

You can explore the following projects/docs to learn more about integrating Casdoor with Chrome extensions:

- [casdoor-chrome-extension](#) - Official example repository
- [Casdoor OAuth Documentation](#)
- [Chrome Extension Identity API](#)
- [Casdoor JavaScript SDK](#)

Next.js

[nextjs-auth](#)是一个如何在next-js项目中集成casdoor的示例。 我们将引导您完成以下步骤。

步骤1：部署Casdoor

首先，应部署Casdoor。

您可以参考Casdoor官方文档中的[服务器安装](#)。 请在**生产模式**下部署您的Casdoor实例。

成功部署后，请确保以下内容：

- 打开您最喜欢的浏览器并访问**<http://localhost:8000>**。 您将看到Casdoor的登录页面。
- 通过输入 `admin` 作为用户名和 `123` 作为密码来测试登录功能。

之后，您可以使用以下步骤在您自己的应用中快速实现基于Casdoor的登录页面。

步骤2：添加中间件

中间件允许您在请求完成之前运行代码。 然后，根据传入的请求，您可以通过重写、重定向、修改请求或响应头，或直接响应来修改响应。

使用项目根目录中的 `middleware.ts` (或 `.js`) 文件来定义中间件。 例如，与 `pages` 或 `app` 同级，或者在 `src` 内 (如果适用)。

示例

```
// 定义中间件将在哪些路径上运行
const protectedRoutes = ["/profile"];

export default function middleware(req) {
  if (protectedRoutes.includes(req.nextUrl.pathname)) {
    // 将传入的请求重定向到不同的URL
    return NextResponse.redirect(new URL("/login", req.url));
  }
}
```

查看next.js官方文档[middleware](#)以获取更多详细信息。

步骤3：使用Casdoor SDK

1. 安装SDK

首先，通过NPM或Yarn安装casdoor-javascript-sdk：

```
npm install casdoor-javascript-sdk
```

或者：

```
yarn add casdoor-javascript-sdk
```

2. 初始化SDK

然后按照以下顺序初始化6个字符串类型的参数：

名称	必需	描述
serverUrl	是	Casdoor服务器URL, 例如 <code>http://localhost:8000</code>
clientId	是	应用客户端ID
clientSecret	是	应用客户端密钥
organizationName	是	应用组织
appName	是	应用名称
redirectPath	是	重定向URL

示例

```
const sdkConfig = {
  serverUrl: "https://door.casdoor.com",
  clientId: "294b09fbc17f95daf2fe",
  clientSecret: "dd8982f7046ccba1bbd7851d5c1ece4e52bf039d",
  organizationName: "casbin",
  appName: "app-vue-python-example",
  redirectPath: "/callback",
};
```

⚠ 注意事项

用您自己的Casdoor实例替换配置值, 特别是 `clientId`, `clientSecret` 和

serverUrl。

3.重定向到登录页面

当您需要对访问您的应用的用户进行身份验证时，您可以发送目标URL并重定向到Casdoor提供的登录页面。

请确保您已经在应用配置中提前添加了回调URL（例如**<http://localhost:8080/callback>**）。

```
const CasdoorSDK = new Sdk(sdkConfig);
CasdoorSDK.signin_redirect();
```

4.获取令牌和存储

在通过Casdoor验证后，它将带着令牌重定向回您的应用程序。

您可以选择使用cookie来存储令牌。

```
CasdoorSDK.exchangeForAccessToken()
  .then((res) => {
    if (res && res.access_token) {
      //Get Token
      return CasdoorSDK.getUserInfo(res.access_token);
    }
  })
  .then((res) => {
    // Storage Token
    Cookies.set("casdoorUser", JSON.stringify(res));
  });
});
```

您可以参考Casdoor官方文档了解如何使用Casdoor SDK。

步骤4：添加中间件认证功能

当用户试图访问受保护的路由时，中间件认证功能会验证他们的身份。如果用户未经认证，他们将被重定向到登录页面或被拒绝访问。

示例

```
//受保护的路由
const protectedRoutes = ["/profile"];
const casdoorUserCookie = req.cookies.get("casdoorUser");
const isAuthenticated = casdoorUserCookie ? true : false;

//认证功能
if (!isAuthenticated &&
protectedRoutes.includes(req.nextUrl.pathname)) {
  return NextResponse.redirect(new URL("/login", req.url));
}
```

Nuxt

[nuxt-auth](#)是一个如何在nuxt项目中集成casdoor的示例。 我们将引导您完成以下步骤。许多步骤与nextjs-auth相似。

步骤1：部署Casdoor

首先，应部署Casdoor。

您可以参考Casdoor官方文档中的[服务器安装](#)。 请以**生产模式**部署您的Casdoor实例。

成功部署后，请确保以下内容：

- 打开您喜欢的浏览器并访问**<http://localhost:8000>**。 您将看到Casdoor的登录页面。
- 通过输入 `admin` 作为用户名和 `123` 作为密码来测试登录功能。

之后，您可以使用以下步骤在您自己的应用中快速实现基于Casdoor的登录页面。

步骤2：添加中间件

中间件允许您在请求完成之前运行代码。 然后，根据传入的请求，您可以通过重写、重定向、修改请求或响应头，或直接响应来修改响应。

在项目根目录的 `middleware` 目录中创建 `.js` 或 `.ts` 文件来定义中间件。 并且文件名被识别为中间件的名称。 例如，在 [nuxt-auth](#) 中，我们在 `middleware` 目录中创建了一个名为 `myMiddleware.js` 的文件，可以在 `nuxt.config.js` 等其他地方引用为 `myMiddleware`。

示例

```
// 定义中间件将在哪些路径上运行
const protectedRoutes = ["/profile"];

export default function ({route, redirect}) {

  if (protectedRoutes.includes(route.path)) {
    // 将传入的请求重定向到不同的URL
    redirect('/login');
  }
}
```

要使中间件工作，您应该在 `nuxt.config.js` 中添加路由，如下所示：

```
export default {
  // 其他配置

  // 需要添加的内容
  router: {
    middleware: ['myMiddleware'] // 替换为你的中间件名称
  },
}
```

查看 [nuxt官方文档middleware](#) 以获取更多详细信息。

步骤3：使用Casdoor SDK

1. 安装SDK

首先，通过NPM或Yarn安装casdoor-javascript-sdk：

```
npm install casdoor-javascript-sdk
```

或者：

```
yarn add casdoor-javascript-sdk
```

2. 初始化SDK

然后按以下顺序初始化6个字符串类型的参数：

名称	必需	描述
serverUrl	是	Casdoor服务器URL，例如 <code>http://localhost:8000</code>
clientId	是	应用客户端ID
clientSecret	是	应用客户端密钥
organizationName	是	应用组织

名称	必需	描述
appName	是	应用名称
redirectPath	是	重定向URL

示例

```
const sdkConfig = {
  serverUrl: "https://door.casdoor.com",
  clientId: "294b09fbc17f95daf2fe",
  clientSecret: "dd8982f7046ccba1bbd7851d5c1ece4e52bf039d",
  organizationName: "casbin",
  appName: "app-vue-python-example",
  redirectPath: "/callback",
};
```

⚠ 注意事项

将配置值替换为您自己的Casdoor实例，特别是 `clientId`、`clientSecret` 和 `serverUrl`。

3. 重定向到登录页面

当您需要验证访问您的应用的用户时，您可以发送目标URL并重定向到Casdoor提供的登录页面。

确保您已经在应用配置中提前添加了回调URL（例如**<http://localhost:8080/callback>**）。

```
const CasdoorSDK = new Sdk(sdkConfig);
CasdoorSDK.signin_redirect();
```

4. 获取令牌和存储

Casdoor验证通过后，它将带着令牌重定向回您的应用。

您可以选择使用cookie来存储令牌。

```
CasdoorSDK.exchangeForAccessToken()
  .then((res) => {
    if (res && res.access_token) {
      // 获取令牌
      return CasdoorSDK.getUserInfo(res.access_token);
    }
  })
  .then((res) => {
    // 存储令牌
    Cookies.set("casdoorUser", JSON.stringify(res));
  });
});
```

您可以参考[Casdoor官方文档中的如何使用Casdoor SDK](#)。

步骤4：添加中间件认证功能

当用户试图访问受保护的路由时，中间件认证功能会验证他们的身份。如果用户未经认证，他们将被重定向到登录页面或被拒绝访问。

示例

```
import Cookies from "js-cookie";
```


OAuth 2.0

介绍

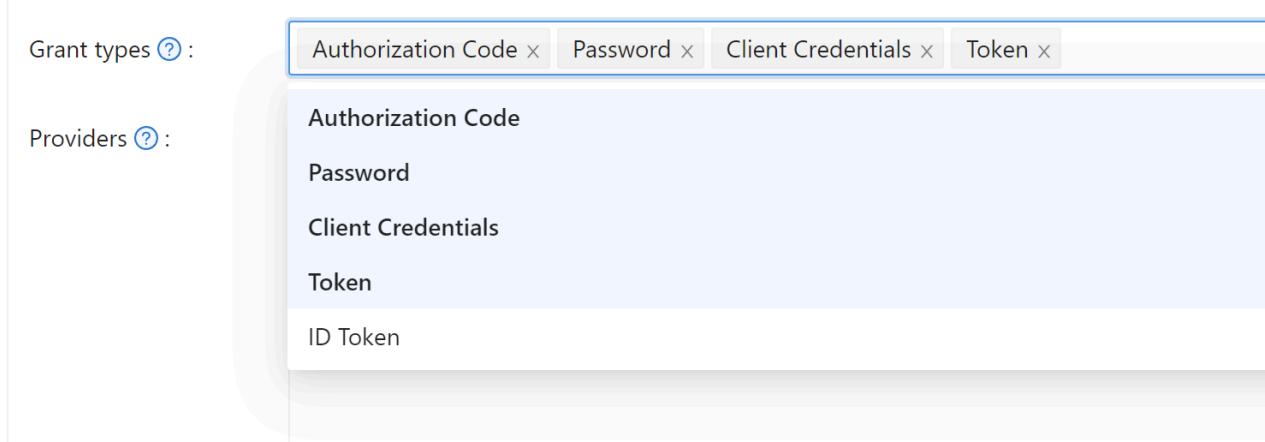
Casdoor 支持使用 AccessToken 验证客户端。在本节中，我们将向您展示如何获取 AccessToken，如何验证 AccessToken，以及如何使用 AccessToken。

如何获取AccessToken

获取访问令牌有两种方式：您可以使用 [Casdoor SDK](#) 详情请参阅SDK文档。这里我们将主要向您展示如何使用 API 来获取访问令牌。

Casdoor支持四种OAuth 授予类型: [Authorization Code Grant](#), [Implicit Grant](#), [Resource Owner Password Credentials Grant](#), 和 [Client Credentials Grant](#).

出于安全考虑，Casto应用默认已开启授权码模式。如果您需要使用其他模式，请前往相应的应用程序来设置它。



获取授权码

首先，重定向您的用户到：

```
https://<CASDOOR_HOST>/login/oauth/authorize?  
client_id=CLIENT_ID&  
redirect_uri=REDIRECT_URI&  
response_type=code&  
scope=openid&  
state=STATE
```

可用的作用域 (scope)

名称	描述
openid (no scope)	sub (用户ID), iss (发行人) 和 aud (受众)
profile	用户资料信息，包括名称、显示名称、头像
email	用户的电子邮件地址
address	用户地址
phone	用户的电话号码

① 信息

您的 OAuth 应用程序可以在首次重定向时带上请求的作用域。您可以指定多个作用域并使用空格（转义后为%20）分隔：

```
https://<CASDOOR_HOST>/login/oauth/authorize?  
client_id=...&  
scope=openid%20email
```

更多详情，请参阅 [OIDC 标准](#)

当您的用户通过 Casdoor 身份验证后，他会被 Casdoor 重定向到：

```
https://REDIRECT_URI?code=CODE&state=STATE
```

现在您已经获得授权码，在你的后端应用发送 POST 请求：

```
https://<CASDOOR_HOST>/api/login/oauth/access_token
```

在你的后端应用

```
{  
  "grant_type": "authorization_code",  
  "client_id": ClientId,  
  "client_secret": ClientSecret,  
  "code": Code,  
}
```

您将得到以下响应：

```
{  
    "access_token": "eyJhb...","  
    "id_token": "eyJhb...","  
    "refresh_token": "eyJhb...","  
    "token_type": "Bearer",  
    "expires_in": 10080,  
    "scope": "openid"  
}
```

ⓘ 备注

Casdoor 也支持 PKCE 功能。当获取验证码时，您可以添加两个参数来启用PKCE:

```
&code_challenge_method=S256&code_challenge=YOUR_CHANNELLENGE
```

获取令牌时，您需要传递 `code_verifier` 参数来验证 PKCE。值得一提的是，启用 PKCE 后，`Client_Secret` 并不是必需的，但如果您要传递这个参数，它的值就必须是正确的。

隐式授权

如果您的应用程序没有后端，您需要使用隐式授权。首先，您需要确保您启用了隐式授权，然后将您的用户请求重定向到:

```
https://<CASDOOR_HOST>/login/oauth/  
authorize?client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&response_type=token&scope=openid&state=STATE
```

在您的用户通过Casdoor进行身份验证后，Casdoor将会将他们重定向到:

```
https://REDIRECT_URI/#access_token=ACCESS_TOKEN
```

Casdoor也支持`id_token`作为`response_type`，这是OpenID的一个特性。

Device Grant

Maybe your devices have limited input capabilities or lack a suitable browser, and you need to use Device Grant. First, you need to make sure you have Device Grant enabled, the request `device_authorization_endpoint` in OIDC discover, then use QR code or text to show `verification_uri` and lead user to enter login page.

Second, you should request `token endpoint` to get Access Token with parameter define in [rfc8628](#).

使用资源拥有者的密码凭据授权

如果您的应用程序没有前端来重定向用户到Casdoor，那么您可能需要这个功能。

首先，您需要确保已启用密码凭据授权，并向以下地址发送POST请求:

```
https://<CASDOOR\_HOST>/api/login/oauth/access\_token
```

```
{  
    "grant_type": "password",  
    "client_id": ClientId,  
    "client_secret": ClientSecret,  
    "username": Username,  
    "password": Password,  
}
```

您将得到以下响应：

```
{  
    "access_token": "eyJhb...","  
    "id_token": "eyJhb...","  
    "refresh_token": "eyJhb...","  
    "token_type": "Bearer",  
    "expires_in": 10080,  
    "scope": "openid"  
}
```

使用客户端凭据授权

当应用程序没有前端时，您也可以使用客户端凭据授权。

首先，你需要确保你已启用客户端凭证授权，并发送POST请求到https://<CASDOOR_HOST>/api/login/oauth/`access_token`：

```
{  
    "grant_type": "client_credentials",  
    "client_id": ClientId,  
    "client_secret": ClientSecret,  
}
```

您将得到以下响应：

```
{  
    "access_token": "eyJhb...","  
    "id_token": "eyJhb...","  
    "refresh_token": "eyJhb...","  
    "token_type": "Bearer",  
    "expires_in": 10080,  
    "scope": "openid"  
}
```

必须指出，以这种方式获得的AccessToken不同于前三个，因为它与应用程序相对应，而不是与用户相对应。

刷新令牌

也许你想更新你的访问令牌，那么你可以使用上面获得的 `refreshToken`。

首先，您需要在应用中设置刷新令牌的过期时间（默认为0小时），并向 `https://<CASDOOR_HOST>/api/login/oauth/refresh_token` 发送POST请求

```
{  
    "grant_type": "refresh_token",  
    "refresh_token": REFRESH_TOKEN,  
    "scope": SCOPE,  
    "client_id": ClientId,  
    "client_secret": ClientSecret,  
}
```

你会得到这样的回应：

```
{  
    "access_token": "eyJhb... ",  
    "id_token": "eyJhb... ",  
    "refresh_token": "eyJhb... ",  
    "token_type": "Bearer",  
    "expires_in": 10080,  
    "scope": "openid"  
}
```

如何验证访问令牌

Casdoor 目前支持 [令牌自省](#) 端点。此端点受基本身份验证保护（ClientId:ClientSecret）。

```
POST /api/login/oauth/introspect HTTP/1.1  
Host: CASDOOR_HOST  
Accept: application/json  
Content-Type: application/x-www-form-urlencoded  
Authorization: Basic Y2xpZW50X2lkOmNsawVudF9zzWNyZXQ=  
  
token=ACCESS_TOKEN&token_type_hint=access_token
```

您将收到以下响应：

```
{  
    "active": true,  
    "client_id": "c58c... ",  
    "username": "admin",  
    "token_type": "Bearer",  
    "exp": 1647138242,  
    "iat": 1646533442,
```

如何使用 AccessToken

您可以使用AccessToken访问需要认证的 Casdoor API。

例如，有两种不同的方式来请求 /api/userinfo。

类型1：查询参数

```
https://<CASDOOR_HOST>/api/userinfo?accessToken=<your_access_token>
```

类型2：HTTP Bearer 令牌

```
https://<CASDOOR_HOST>/api/userinfo with the header: "Authorization: Bearer <your_access_token>"
```

Casdoor将解析access_token，并根据 scope 返回相应的用户信息。你将收到相同的响应，看起来像这样：

```
{  
  "sub": "7a6b4a8a-b731-48da-bc44-36ae27338817",  
  "iss": "http://localhost:8000",  
  "aud": "c58c..."  
}
```

如果您期望获得更多用户信息，请在获取AccessToken的步骤授权码授予中添加 scope。

userinfo 和 get-account APIs之间的差异

- /api/userinfo：此API作为OIDC协议的一部分返回用户信息。它提供有限的信息，包括仅在OIDC标准中定义的基本信息。要查看Casdoor支持的可用范围列表，请参阅[可用范围](#)部分。
- /api/get-account：此API用于检索当前登录账户的用户对象。这是一个特定于Casdoor的API，允许您获取Casdoor中[用户](#)的所有信息。

使用Casdoor作为CAS服务器

使用Casdoor作为CAS服务器

Casdoor现在可以作为CAS服务器使用。它目前支持CAS 3.0。

简介

Casdoor中的CAS端点前缀是`<Casdoor endpoint>/cas/<organization name>/<application name>`。这是一个使用端点`https://door.casdoor.com`，在`casbin`组织下名为`cas-java-app`的应用程序的示例：

- `/login` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/login`
- `/logout` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/logout`
- `/serviceValidate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/serviceValidate`
- `/proxyValidate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/proxyValidate`
- `/proxy` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/proxy`
- `/validate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/validate`
- `/p3/serviceValidate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/p3/serviceValidate`
- `/p3/proxyValidate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/p3/proxyValidate`
- `/samlValidate` endpoint: `https://door.casdoor.com/cas/casbin/cas-java-app/samlValidate`

For more information about CAS, its different versions, and parameters for these endpoints, refer to the [CAS Protocol Specification](#).

一个例子

这是一个官方示例 [GitHub 仓库](#)，其中包含一个网页应用，并使用官方的 CAS Java 客户端 [GitHub 仓库](#)。通过这个例子，你可以学习如何通过CAS连接到Casdoor。

ⓘ 备注

注意：目前，Casdoor只支持CAS的所有三个版本：CAS 1.0, 2.0和3.0。

CAS配置位于`src/main/webapp/WEB-INF/web.yml`中。

默认情况下，此应用程序使用CAS 3.0，由以下配置指定：

```
<filter-name>CAS Validation Filter</filter-name>
<filter-
class>org.jasig.cas.client.validation.Cas30ProxyReceivingTicketValidationFilter</filter-
class>
```

如果您想要使用CAS 2.0保护此网页应用程序，请将CAS验证过滤器更改为以下内容：

```
<filter-name>CAS Validation Filter</filter-name>
<filter-
class>org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter</filter-
class>
```

对于 CAS 1.0，请使用以下内容：

```
<filter-name>CAS Validation Filter</filter-name>
<filter-class>org.jasig.cas.client.validation.Cas10TicketValidationFilter</filter-class>
```

将所有 `casServerUrlPrefix` 参数的实例更改为：

```
<param-name>casServerUrlPrefix</param-name>
<param-value>http://door.casdoor.com/cas/casbin/cas-java-app</param-value>
```

将所有的 `casServerLoginUrl` 参数实例更改为：

```
<param-name>casServerLoginUrl</param-name>
<param-value>http://door.casdoor.com/cas/casbin/cas-java-app/login</param-value>
```

如果您需要自定义更多配置，请查看[Java CAS客户端GitHub仓库](#)以获取详细信息。

SAML

概述

使用Casdoor作为SAML IdP

AWS Client VPN

使用Casdoor作为SAML IdP

Keycloak

使用Casdoor作为SAML IdP

Google Workspace

使用Casdoor作为SAML IdP

Appgate (POST)

如何使用 Casdoor 作为SAML IdP for Appgate

腾讯云

使用Casdoor作为SAML IdP

概述

现在可以使用Casdoor作为SAML IdP。到目前为止，Casdoor已经支持了SAML 2.0的主要功能。

在SP中的配置

一般来说，SP需要三个必填字段：`Single Sign-On`，`Issuer`和`Public Certificate`。大多数SP可以通过上传XML元数据文件或XML元数据URL来自动完成这些字段。

Casdoor中的SAML端点的元数据是`<Endpoint of casdoor>/api/saml/metadata?application=admin/<application name>`。假设Casdoor的端点是`https://door.casdoor.com`，并且它包含一个名为`app-built-in`的应用程序。XML元数据端点将是：

```
https://door.casdoor.com/api/saml/metadata?application=admin/app-built-in
```

您也可以在应用程序编辑页面中找到元数据。点击按钮复制URL并粘贴到浏览器中下载XML元数据。

```
SAML metadata ⓘ <EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://door.casdoor.com">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">MIIE+TCCAuGgAwIBAgIDAeJAMAOCSqGSib3DQEBCwUAMDYxHTAbBgNVBAoTFeNh2Rvb3IgT3JnYW5pemFOaW9uMRUwEwYDVQQDEwxDYXNkb2NQIEA&lt;!-- X509 certificate content --&gt;
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <SingleSignOnService Bindings="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://door.casdoor.com/login/saml/authorize/admin/app-built-in"></SingleSignOnService>
  </IDPSSODescriptor>
</EntityDescriptor>
```

Copy SAML metadata URL

在Casdoor IdP中的配置

Casdoor支持GET和POST `SAMLResponse`。当Casdoor将`SAMLResponse`发送到SP时，Casdoor需要知道SP支持哪些类型的请求。您需要根据您的SP支持的`SAMLResponse`类型在Casdoor中配置应用程序。

① 信息

如果您填写了`Reply URL`，Casdoor将通过POST请求发送`SAMLResponse`。如果回复URL为空，Casdoor将使用GET请求。您可能会想知道，如果`Reply URL`为空，Casdoor如何知道SP的`Reply URL`。实际上，Casdoor可以通过解析`SAMLRequest`获取名为`AssertionConsumerServiceURL`的URL，并将带有`SAMLResponse`的请求发送到`AssertionConsumerServiceURL`。`Reply URL`将覆盖`SAMLRequest`中的`AssertionConsumerServiceURL`。

- **回复URL：**输入验证SAML响应的ACS的URL。

Grant types [?](#) : Authorization Code Password

SAML Reply URL [?](#) :

Enable SAML compress [?](#) :

- 重定向URL: 输入一个唯一的名称。在您的SP中，这可能被称为 Audience 或 Entity ID。确保您在此处填写的 Redirect URL 与您的SP中的一致。

Redirect URLs [?](#) :

Redirect URLs	Add
Redirect URL	<input type="text" value="appgate"/>
	https://git.casbin.com/user/oauth2/casdoor/callback
	http://localhost:3000/callback

SAML attributes

Some SP will require you to provide external attributes in SAML Response, you can add those in SAML attributes table. And you can insert user's field to it.

For example

名称	Name format	Value
https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName	Unspecified	<input type="text" value="\$user.name"/>
https://www.aliyun.com/SAML-Role/Attributes/Role	Unspecified	<input type="text" value="acs:ram::1879818006829152:role/\$user.roles,acs:ram::1879818006829152:saml-provider/testa"/>

will generate response with external `saml:Attribute`

```

<saml:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:string">admin122n@outlook.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:string">acs:ram::1879818006829152:role/
role1,acs:ram::1879818006829152:saml-provider/testa</saml:AttributeValue>

```

① 信息

We only support insert

`$user.owner`, `$user.name`, `$user.email`, `$user.id`, `$user.phone`, `$user.roles`, `$user.permissions`, `$user.groups`

用户资料

成功登录后，Casdoor返回的SAMLResponse中的用户资料有三个字段。XML中的属性和Casdoor中的用户属性的映射如下：

XML属性名称	用户字段
电子邮件	电子邮件
显示名称	显示名称
Name	名称

有关SAML及其不同版本的更多信息，请参见https://en.wikipedia.org/wiki/SAML_2.0。

一个例子

gosaml2是基于etree和goxmldsig的服务提供商的SAML 2.0实现，这是XML数字签名的纯Go实现。我们使用这个库来测试Casdoor中的SAML 2.0，如下所示。

假设您可以通过<http://localhost:7001>访问Casdoor，并且您的Casdoor包含一个名为app-built-in的应用程序，该应用程序属于一个名为built-in的组织。这两个URL：<http://localhost:6900/acs/example>和<http://localhost:6900/saml/acs/example>，应该添加到app-built-in中的重定向URLs。

```
import (
    "crypto/x509"
    "fmt"
    "net/http"

    "io/ioutil"

    "encoding/base64"
    "encoding/xml"

    saml2 "github.com/russellhaering/gosaml2"
    "github.com/russellhaering/gosaml2/types"
    dsig "github.com/russellhaering/goxmldsig"
)

func main() {
    res, err := http.Get("http://localhost:7001/api/saml/metadata?application=admin/app-built-in")
    if err != nil {
        panic(err)
    }

    rawMetadata, err := ioutil.ReadAll(res.Body)
    if err != nil {
        panic(err)
    }

    metadata := &types.EntityDescriptor{}
```

运行上述代码，控制台将显示以下消息。

```
Visit this URL To Authenticate:  
http://localhost:7001/login/saml/authorize/admin/app-built-in?SAMLRequest=lFVbk6K8Fv0rFvNo2QR...  
Supply:  
SP ACS URL : http://localhost:6900/v1/_saml_callback
```

点击URL进行身份验证，Casdoor的登录页面将被显示。

A screenshot of a browser window showing the Casdoor login page. The URL in the address bar is 'localhost:7001/login/saml/authorize/admin/app-built-in?SAMLRequest=lFVbk6K8Fv0rFvNo2QR...'. The page features a logo with a blue owl and the word 'casbin'. Below it is a button labeled 'Continue with:' followed by a box containing a user icon and the text 'admin (Admin)'. There are also fields for 'username, Email or phone' and 'Password', and links for 'Auto sign in' and 'Forgot password?'. At the bottom are buttons for 'Sign In', 'Sign in with code', and 'No account? sign up now'.

身份验证后，您将收到如下所示的响应消息。

A screenshot of a browser window showing the response message from the Casdoor login page. The URL in the address bar is 'localhost:6900/v1/_saml_callback?SAMLResponse=PHNh...'. The page displays a large block of XML response data. The XML includes sections for 'NameID', 'Assertions', and 'Warnings'. The 'NameID' section shows 'admin@example.com'. The 'Assertions' section contains several SAML assertion elements with details like 'FriendlyName', 'NameFormat', and 'Value'. The 'Warnings' section includes a note about 'ProxyRestriction' and 'NotInAudience'.

```
NameID: admin@example.com  
Assertions:  
  <Assertion>  
    <Attribute>  
      <Name>Email</Name>  
      <Value>admin@example.com</Value>  
    </Attribute>  
    <Attribute>  
      <Name>Name</Name>  
      <Value>admin</Value>  
    </Attribute>  
    <Attribute>  
      <Name>Display Name</Name>  
      <Value>admin</Value>  
    </Attribute>  
  </Assertion>  
Warnings:  
&{OneTimeUse:false ProxyRestriction:{nil} NotInAudience:false InvalidTime:false}
```


AWS Client VPN

Casdoor作为AWS Client VPN中的SAML IdP

本指南将向您展示如何配置Casdoor和AWS Client VPN，以在AWS Client VPN中添加Casdoor作为SAML IdP。

先决条件

要完成此设置，您将需要：

- 具有访问服务提供商配置设置的管理权限的AWS账户。
- 带有EC2实例的Amazon VPC
 - [设置VPC](#)
 - [启动EC2实例](#)
 - 在实例安全组中，允许来自VPC CIDR范围的ICMP流量 - 这是测试所需的。
- 将私有证书导入到[AWS证书管理器\(ACM\)](#)
 - [生成并导入证书到ACM](#)
- 运行最新AWS Client VPN软件的Windows或Mac系统。
 - [下载软件](#)

配置SAML应用程序

- 在Casdoor应用程序中，将 Redirect URL 设置为 `urn:amazon:webservices:clientvpn`。

Tags [?](#) :

Client ID [?](#) : 235aca38d69a868ae432

Client secret [?](#) : d8942f2181908041106f3b2b56c2f91fd2ad13de

Cert [?](#) : cert-built-in

Redirect URLs [?](#) :

Redirect URLs	Add
Redirect URL	<code>urn:amazon:webservices:clientvpn</code>

Token format [?](#) :

Token expire [?](#) : 168 Hours

Refresh token expire [?](#) : 0 Hours

Enable password [?](#):

- 将 SAML 回复 URL 设置为 `http://127.0.0.1:35001`。

Signup HTML [?](#) :

Signin HTML [?](#) :

Grant types [?](#) : Authorization Code x

SAML reply URL [?](#) : `http://127.0.0.1:35001`

Enable SAML compression [?](#) :

SAML metadata [?](#) :

```
<EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="urn:urn:oasis:names:tc:SAML:2.0:metadata" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" protocol="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
```

- 将 SAML 元数据 的内容保存为 XML 文件。

```
SAML metadata <EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="urn:urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" protocol="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">MIIE+TCCAUgGwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENhc2Rvb3IgT3JnYW&lt;/X509Data>
        </KeyInfo>
      </KeyDescriptor>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Locations="https://test.v2tl.com/login/saml/authorize/admin/app">
```

[Copy SAML metadata URL](#)

配置AWS

将 Casdoor 配置为 AWS 身份提供商

- 打开 IAM 控制台，从导航栏中选择 **身份提供商**。
- 点击 **创建提供商**。

3. 为提供商类型指定SAML，为此提供商添加一个唯一的名称，并上传元数据文档 - 与您在上一节中从Casdoor应用程序保存的文件相同。

4. 点击下一步。在下一个屏幕上，点击创建。

The screenshot shows the AWS IAM Identity providers page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Dashboard', 'Access management' (with 'Identity providers' highlighted), 'Access reports', and 'Account settings'. The main area has a header 'Identity providers (1) Info' and a note about AWS IAM Identity Center. Below is a table with one row for 'casdoor' (Type: SAML, Creation time: Yesterday). A red box highlights the 'Add provider' button.

The screenshot shows the 'Add an Identity provider' configuration page. At the top, it says 'Add an Identity provider Info'. Below is a section titled 'Configure provider' with 'Provider type' set to 'SAML'. There are two options: 'SAML' (selected) and 'OpenID Connect'. The 'SAML' option describes establishing trust between AWS and a SAML 2.0 compatible Identity Provider like Shibboleth or Active Directory Federation Services. The 'OpenID Connect' option describes establishing trust between AWS and Identity Provider services like Google or Salesforce. Below is a 'Provider name' field containing 'casdoor', with a note about character limits. At the bottom, there's a 'Metadata document' section with a 'Choose file' button, which is highlighted with a red box. A note below says 'File needs to be a valid UTF-8 XML document.' A red number '3' is placed next to the 'Choose file' button.

创建AWS Client VPN端点

1. 在您选择的AWS区域中打开Amazon VPC控制台。
2. 在左侧导航中，选择客户端VPN端点，位于虚拟专用网络(VPN)下。
3. 点击创建客户端VPN端点。
4. 在客户端IPv4 CIDR字段中输入您的远程用户的IP范围，以分配IP范围。
5. 对于服务器证书ARN，选择您创建的证书。
6. 对于身份验证选项，选择使用基于用户的身份验证，然后选择联合身份验证。
7. 对于SAML提供商ARN，选择您创建的身份提供商。
8. 点击创建客户端VPN端点。

The screenshot shows the AWS VPC Client VPN endpoints page. On the left, there's a navigation sidebar with options like Virtual private network (VPN), Customer gateways, Virtual private gateways, Site-to-Site VPN connections, and Client VPN endpoints (which is highlighted with a red box). Below that is another section for Transit gateways. The main area has a title 'Client VPN endpoints (1/1)' with an 'Info' link, a 'Actions' dropdown, and a 'Create client VPN endpoint' button (also highlighted with a red box). There's a search bar labeled 'Filter client VPN endpoints'. A table lists one endpoint: Name: cvpn-endpoint-06e947f15ddf5687c, State: Available, Client CIDR: 172.31.32.0/20. The table has columns for Name, Client VPN endpoint ID, State, and Client CIDR. At the bottom right of the table area is a small '=' symbol.

Client IPv4 CIDR [Info](#)

The IP address range, in CIDR notation, from which client IP addresses are allocated.

X

CIDR block cannot be larger than /12 or smaller than /22.

Authentication information [Info](#)

Server certificate ARN

The server certificate must be provisioned with or imported into AWS Certificate Manager (ACM).

▼

Authentication options

Choose one or a combination of authentication methods to use.

Use mutual authentication
 Use user-based authentication

User-based authentication options

Active directory authentication
 Federated authentication

SAML provider ARN

The ARN of SAML provider.

▼

Self-service SAML provider ARN - optional [Info](#)

▼

将客户端VPN与目标VPC关联

1. 在客户端VPN选项中选择目标网络关联，然后点击关联目标网络。
2. 从下拉菜单中，选择您想要将您的端点关联的目标VPC和子网。

The screenshot shows the AWS CloudFormation console with the navigation bar on the left. Under the 'Virtual private network (VPN)' section, 'Client VPN endpoints' is selected. A table lists one endpoint: 'cvpn-endpoint-06e947f15ddf5687c' (Status: Available, CIDR: 172.31.32.0/20). The endpoint details page is open, showing tabs for 'Details', 'Target network associations' (which is highlighted with a red box), 'Security groups', 'Authorization rules', 'Route table', 'Connections', and 'Tags'. The 'Target network associations' tab displays one association: 'cvpn-assoc-0bf639762212d5a04' (Associated, Network ID: subnet-0596ebfd975cdd125, Security group: sg-09d2a80e3c2795429, Endpoint ID: cvpn-endpoint-06e947f15d). A red box also highlights the 'Associate target network' button.

配置SAML组特定授权

1. 在您的客户端VPN选项中，选择授权规则选项卡，然后点击添加授权规则。
2. 对于要启用的目标网络，指定在先决条件中创建的EC2实例的IP地址。例如，`172.31.16.0/20`。
3. 在授予访问权限下，选择允许特定访问组中的用户访问。例如，`casdoor`。
4. 提供一个可选的描述，然后点击添加授权规则。

Add authorization rule Info

Add authorization rules to grant clients access to the networks.

Details

Client VPN endpoint ID
 cvpn-endpoint-06e947f15ddf5687c

Destination network to enable access
The IP address, in CIDR notation, of the destination network.
 2

Grant access to:
 Allow access to all users
 Allow access to users in a specific access group

Access group ID
Unique group identifier. It can be active directory SID or group name in IDP.
 3

Description - optional
A brief description of the authorization rule.
 4

连接到客户端VPN

1. 选择您刚刚创建的客户端VPN端点。现在应该处于可用状态。
2. 点击下载客户端配置，将配置文件下载到您的桌面。
3. 在您的机器上打开AWS Client VPN桌面应用程序。
4. 在顶部菜单中，选择文件和管理配置文件。
5. 点击添加配置文件，并指向最近下载的文件。
6. 您现在应该在AWS Client VPN软件的列表中看到该配置文件。选择它并点击连接。

VPC dashboard ×

EC2 Global View New

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Client VPN endpoints (1/1) Info

Actions ▼

Download client configuration

Create client VPN endpoint

Filter client VPN endpoints

Name	Client VPN endpoint ID	State	Client CIDR
-	cvpn-endpoint-06e947f15ddf5687c	Available	172.31.32.0/20

cvpn-endpoint-06e947f15ddf5687c ×

Details Target network associations Security groups Authorization rules Route table Connections Tags

Details				
Client VPN endpoint ID cvpn-endpoint-06e947f15ddf5687c	Server certificate ARN arn:aws:acm:ap-southeast-1:580652580210:certificate/f028f870-16ee-41b7-8b4e-66a2a0ebfe33	Connection log false	Transport protocol udp	
Description -		Cloudwatch log group -	Split-tunnel Disabled	

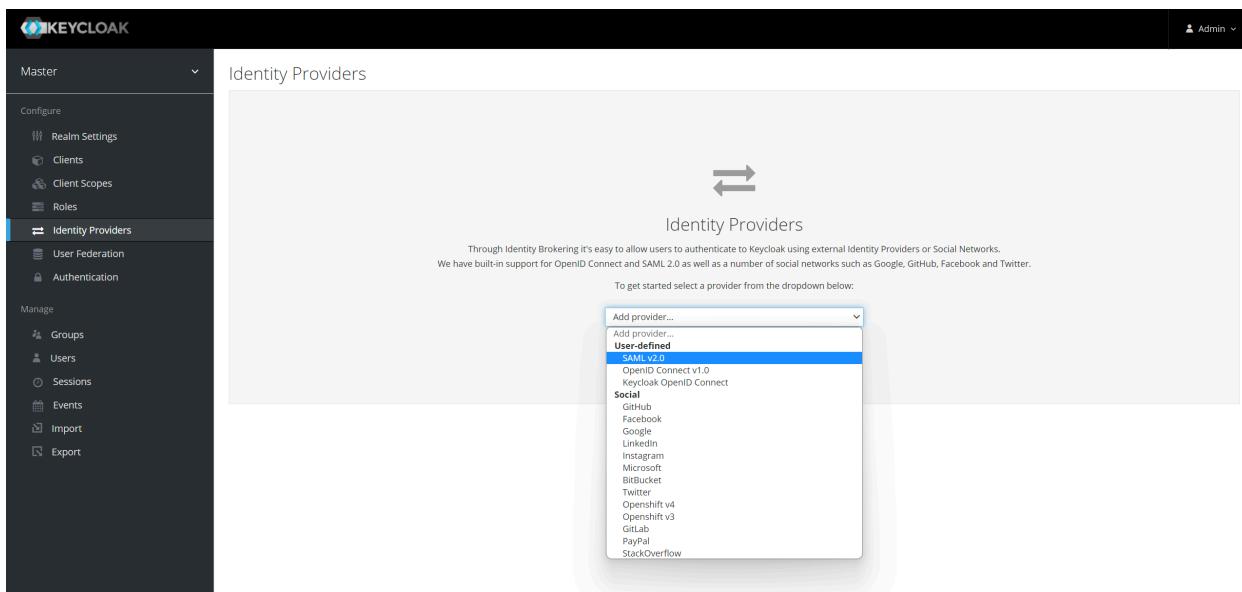
Keycloak

在Keycloak中的Casdoor作为SAML IdP

本指南将向您展示如何配置Casdoor和Keycloak，以在Keycloak中添加Casdoor作为SAML IdP。

在Keycloak中添加SAML IdP

打开Keycloak管理员页面，点击**身份提供商**，并从提供商列表中选择**SAML v2.0**。



① 信息

您可以访问Keycloak SAML身份提供商[文档](#)以获取更详细的信息。

在Keycloak IdP编辑页面中输入**别名**和**从URL导入**。从URL导入的内容可以在Casdoor

应用程序编辑页面上找到。 点击导入， SAML配置将自动填充。

Import External IDP Config

Import from URL: http://localhost:7001/api/saml/metadata?application=admin/app-built-in

Import

Import from file Select file

Save Cancel

记住服务提供商实体ID并保存配置。

在Casdoor中配置SAML应用程序

在应用程序编辑页面中，添加一个包含来自Keycloak的服务提供商实体ID的重定向URL。 另外，确保为Keycloak启用SAML压缩。

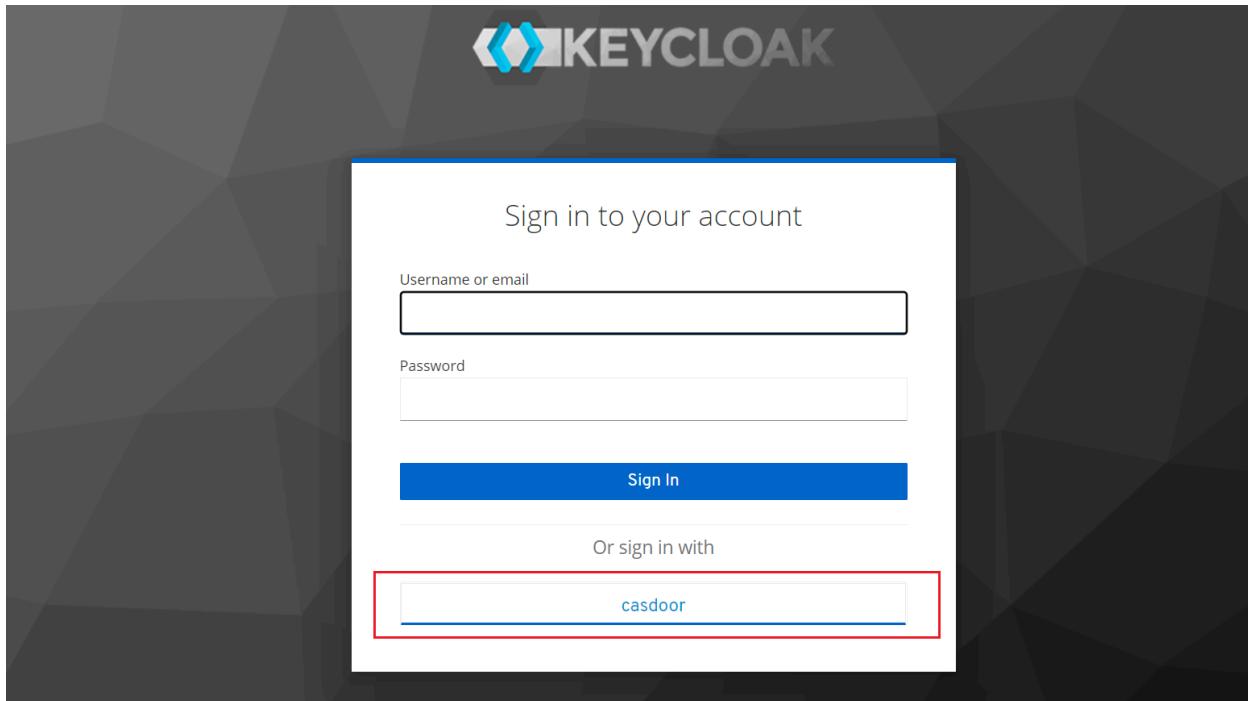
Enable SAML compress

```
SAML metadata: <EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityId="http://localhost:8000">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signin">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Certificate>MIIE+TC...</X509Certificate>
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
  </IDPSSODescriptor>
</EntityDescriptor>
```

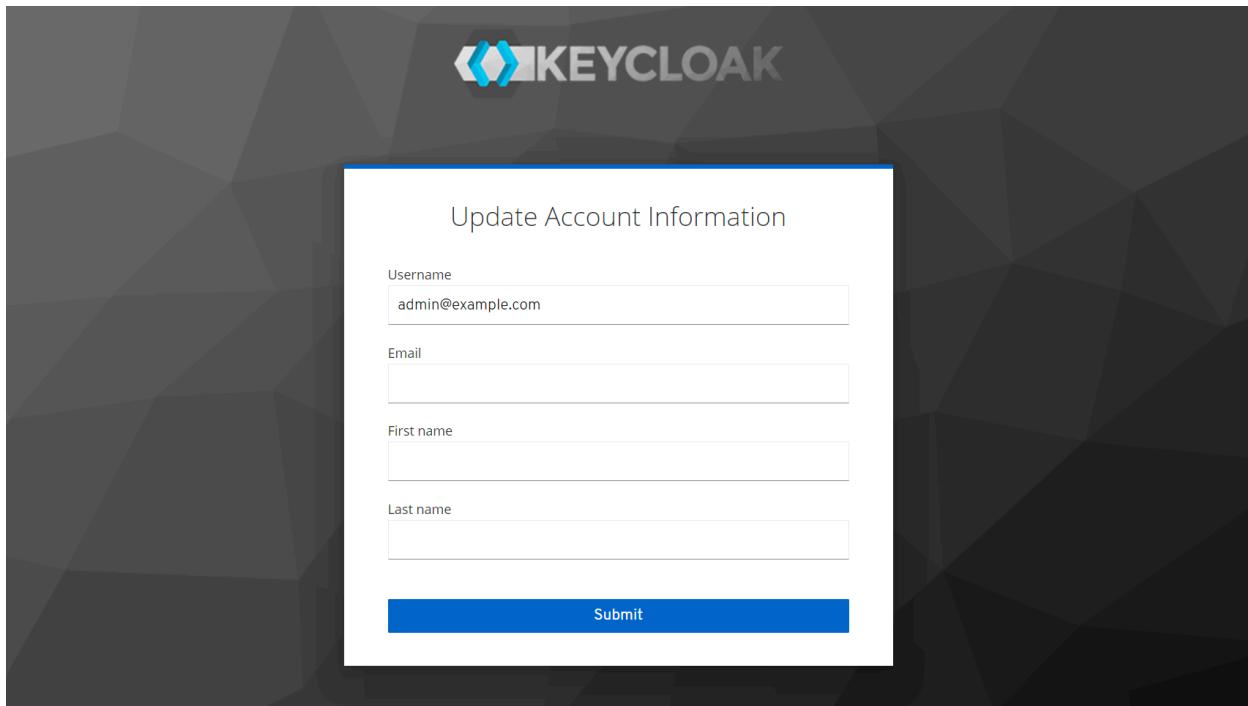
Copy SAML metadata URL

使用Casdoor SAML登录

打开Keycloak登录页面，您会发现一个额外的按钮，允许您使用Casdoor SAML提供商登录Keycloak。



点击该按钮，您将被重定向到Casdoor SAML提供商进行身份验证。身份验证成功后，您将被重定向回Keycloak。然后你需要将用户分配给应用程序。



我们还提供了一个演示视频，展示了整个过程，希望对您有所帮助。

Google Workspace

将Casdoor作为Google Workspace中的SAML IdP

本指南将向您展示如何配置Casdoor和Google Workspace，以在Google Workspace中添加Casdoor作为SAML IdP。

添加证书

在Casdoor中，添加一种类型为X.509的证书，使用RSA加密算法，并下载它。

The screenshot shows the 'Edit Cert' page with the following fields:

- Organization: admin (Shared)
- Name: cert-built-in
- Display name: Built-in Cert
- Scope: JWT
- Type: x509 (highlighted with a red box)
- Crypto algorithm: RS256 (highlighted with a red box)
- Bit size: 4096
- Expire in years: 20
- Certificate: -----BEGIN CERTIFICATE-----
MIIE+TCCAUgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgN
VBAoTFNh-----END CERTIFICATE----- (highlighted with a red box)
- Private key: -----BEGIN PRIVATE KEY-----
MIJKQIBAAKCAgEAslnpb5E1ym0f1RfSDSSE8R7y+lw+RJj74e5ejrq4b8zMY-----END PRIVATE KEY-----
- Buttons: Save, Save & Exit, Copy certificate, Download certificate (highlighted with a red box), Copy private key, Download private key

配置SAML应用程序

在应用程序编辑页面上，选择您刚刚创建的证书。将您将使用的Google应用程序的域名添加到重定向URL中，例如google.com。

Cert ⓘ: cert-built-in

Redirect URLs ⓘ:

Action
<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/>
<input type="button" value=""/> <input type="button" value=""/> <input type="button" value=""/>

在SAML回复URL字段中，输入 `https://www.google.com/a/<your domain>/acs`，这是ACS URL。您可以在这里找到有关ACS URL的相关信息：[SSO断言要求](#)。

SAML reply URL: `https://www.google.com/a/casbin.com/acs`

Enable SAML compression ⓘ:

SAML metadata: `<EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><KeyDescriptor use="signing"><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#><X509Data xmlns="http://www.w3.org/2000/09/xmldsig#><X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">MIIE+TCCAuGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENhc2Rvb3IgT3JnYW</X509Data></KeyInfo></KeyDescriptor><NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:7001/login/saml/authorize/admin/wor</SingleSignOnService></IDPSSODescriptor></EntityDescriptor>`

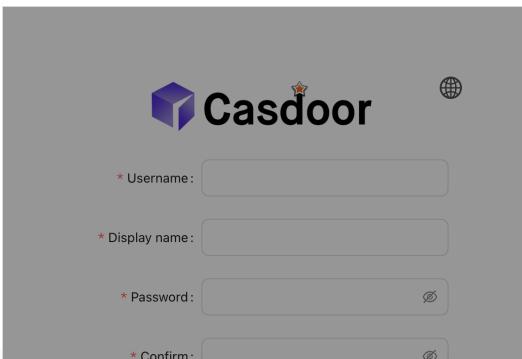
复制登录页面URL。这将在下一步中使用。

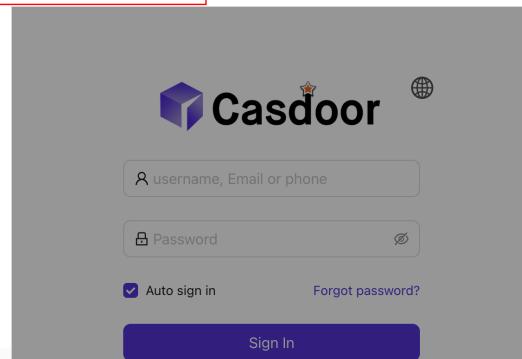
Providers ⓘ:

Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action

No data

Preview ⓘ:





为Google Workspace添加第三方SAML IdP

在Google Workspace管理控制台中，导航到安全性，然后是概览。寻找与第三方IdP的SSO部分。点击“添加SSO配置文件”以访问编辑页面。勾选“与第三方身份提供商设置SSO”复选框。将复制的登录页面URL粘贴到登录页面URL和登出页面URL字段中。上传在上一步中下载的证书。点击“保存”以保存更改。

The screenshot shows the Google Workspace Admin console. On the left, the navigation menu is open, showing "Overview" selected under "Security". The main content area is titled "Third-party SSO profile for your organisation". It includes a sidebar with "Single Sign-On (SSO) with third-party Identity Providers (IDPs)" and a main panel for setting up SSO with a third-party provider. The "Sign-in page URL" field contains the URL `https://localhost/login/oauth/authorize?client_id=12`, which is highlighted with a red box. The "Sign-out page URL" field also contains the same URL, also highlighted with a red box. A "Verification certificate" section shows a uploaded file and a "REPLACE CERTIFICATE" button, with a note that the certificate must contain the public key for Google to verify sign-in requests.

添加测试用户

在Google Workspace中，创建一个用户名为“test”的用户（您可以自定义用户名，这只是一个例子）。

Your new user can start using Google Workspace within 24 hours. In most cases, it should just take a few minutes.



test test

Username: test@casbin.com

[COPY PASSWORD](#)

Send sign-in instructions

The email will provide a link to set the password and sign in to Google Workspace

PREVIEW AND SEND



The user will be assigned licences based on your current subscriptions. [View billing](#)

ADD ANOTHER USER

DONE

在Casdoor中，添加一个与Google Workspace中设置的用户名相同的用户。确保选择适当的组织并输入用户的电子邮件地址。

Organization [?](#) : built-in

ID [?](#) : 4899cef3-8eeb-485a-8f6d-12b41df0d8d2

Name [?](#) : test

Display name [?](#) : test

Avatar [?](#) :

Preview:



Upload a photo...

User type [?](#) : normal-user

Password [?](#) : [Modify password...](#)

Email [?](#) : test@casbin.com

Phone [?](#) : +1 34086653696

以“google.com”为例，按照以下步骤操作：

1. 点击Google.com页面上的登录按钮。 输入用户的电子邮件地址以启动登录过程。
2. 您将被重定向到Casdoor页面。 在Casdoor页面上，输入相应的电子邮件地址和密码。
3. 如果登录成功，您将被重定向回google.com。

Gmail Images ☰ Sign in



Google Search I'm Feeling Lucky

Google offered in: 日本語

Japan

About Advertising Business How Search works

Privacy Terms Settings

Appgate (POST)

在Appgate中的Casdoor作为SAML IdP

Appgate accepte `SAMLResponse` 由 POST 请求发送。如果您使用另一个也支持POST请求的服务供应商(SP)，您可以引用此文档。

Casdoor 配置

转到您的 Casdoor 帐户并添加一个新的应用程序。

在应用程序中输入基本的 SAML 配置：

- 重定向URLs：输入一个唯一的名称。在您的SP中，这可能被称为 `Audience` 或 `Entity ID`。见下表。

Redirect URLs ② :

Redirect URLs	Add
Redirect URL	
🔗 appgate	
🔗 https://git.casbin.com/user/oauth2/casdoor/callback	
🔗 http://localhost:3000/callback	

- Reply URL—键入验证SAML响应的ACS（声明消费者服务）的URL。请参阅下表。

Grant types [?](#) : Authorization Code Password

SAML Reply URL <https://mycontroller.mycompany.com/admin/saml> (?)

Enable SAML compress [?](#)

管理员验证	用户认证
重定向URL = "AppGate"	重定向URL = "AppGate Client"
SAML回复URL = https://mycontroller.your-site-url.com/admin/saml	SAML回复URL = https://redirectserver.your-site-url.com/saml

下载XML元数据文件

您可以复制元数据的URL，并从浏览器下载文件。

Enable SAML compress [?](#)

SAML metadata [?](#)

```

<KeyDescriptor use="signing">
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">MIIE+TC CAuGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFFNh2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxSYXNkbz
    </X509Data>
  </KeyInfo>
</KeyDescriptor>
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://door.casdoor.com/login/saml/authorize/admin/app-gitea"><SingleSignOnService>
<Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="E-Mail" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"></Attribute>
<Attribute Name="DisplayName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="displayName" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"></Attribute>

```

在Appgate中添加SAML IdP

在您的AppGate SDP控制台:

- 选择系统 > 身份提供商。
- 创建一个新的身份提供商。
- 选择SAML类型。
- 按照下表中的详细信息开始配置您的身份提供程序。

管理员验证	
姓名	输入一个唯一的名称，例如“Casdoor SAML Admin”。
单点登录URL	见下文
发行人	见下文
受众	在Casdoor应用中输入重定向URL
公共证书	见下文

- 上传XML元数据文件以自动完成单点登录、发行人和公共证书字段。
- 点击选择文件并选择您之前下载的元数据文件 - 这将自动完成相关字段。

映射属性

将名称映射到用户名。 您完成的表格应该看起来像这样:

Name mapped to claim username

测试集成

在您的AppGate SDP控制器控制台:

- 退出管理员界面。
- 使用以下信息登录:
 - 身份提供商 - 从下拉列表中选择您的Azure IdP。
 - 点击用浏览器登录以连接到您的验证器。
- 您可能会看到以下消息: "您没有任何管理权限" - 这确认了测试用户凭据已经被您的身份提供商成功验证。

访问策略

您需要修改访问策略，以允许管理员使用SAML IdP登录到Appgate。输入内置管理员策略：

您完成的表格应该看起来像这样:

Editing Policy - Admin

- Enabled
 Disabled

Assignment - Active when custom logic is met ▾

 Add New

Custom Logic (1 OR 3) AND 2

- 1 Identity Provider is local
- 2 user.username is admin
- 3 Identity Provider is Casdoor SAML Admin



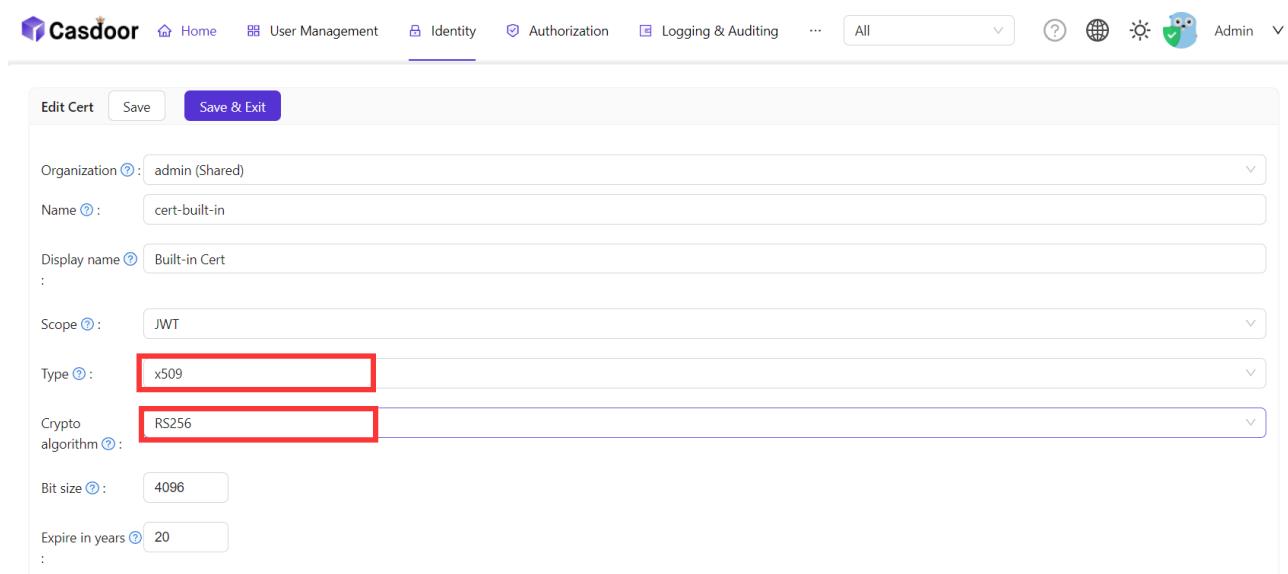
腾讯云

在腾讯云中使用Casdoor作为SAML IdP

本指南将向您展示如何配置Casdoor和腾讯云，以在腾讯云中添加Casdoor作为SAML IdP。

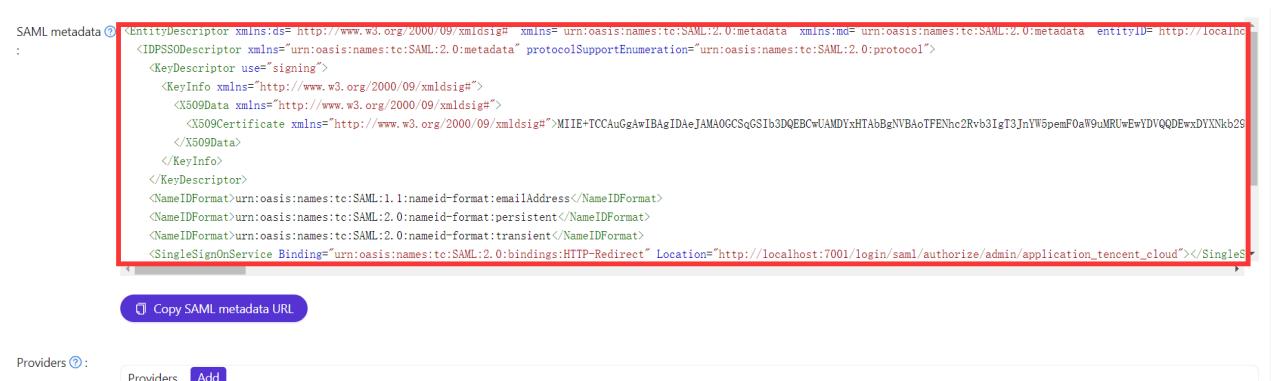
复制Saml元数据

在Casdoor中，添加一种类型为X.509的证书，使用RSA加密算法。



The screenshot shows the 'Edit Cert' page in Casdoor. The 'Type' field is set to 'x509' and the 'Crypto algorithm' field is set to 'RS256'. Both fields are highlighted with red boxes.

然后复制Casdoor中的SamlMetadata。



The screenshot shows the 'Providers' page in Casdoor. A large block of XML code representing the SAML metadata is displayed, with the entire block highlighted by a red rectangle. Below the XML, there is a button labeled 'Copy SAML metadata URL'.

在腾讯云中添加SAML IdP

登录腾讯云并进入访问管理界面。

The screenshot shows the Tencent Cloud Account Center interface. On the left sidebar, under '账号中心' (Account Center), the '访问管理' (Access Management) option is highlighted with a red box. The main content area displays account information for a '微信用户' (WeChat User). The '基本信息' (Basic Information) section includes fields like 账号昵称 (Account Nickname), 账号ID (Account ID), APPID, 认证状态 (Authentication Status), 所属行业 (Industry), and 注册时间 (Registration Time). Below this is the '登录方式' (Login Methods) section, which lists various authentication methods: 微信 (WeChat), QQ, 企业微信 (Enterprise WeChat), 邮箱 (Email), and 微信公众号 (WeChat Official Account). Each method has a status (e.g., 支持微信扫码授权登录 (Supported WeChat QR code authorization login)) and a binding status (e.g., 未关联 (Not associated) or 绑定 (Bound)). On the right side, there is a sidebar with options like '微信用户' (WeChat User), '账号信息' (Account Information), '实名认证 (已实名)' (Real-name authentication (verified)), '安全设置' (Security settings), '项目管理' (Project management), '访问管理' (Access management), '标签' (Tags), '项目管理' (Project management), '安全管控' (Security control), '导航偏好设置' (Navigation preference settings), and '退出' (Logout). A red box highlights the '访问管理' (Access Management) button in the sidebar.

创建一个新的身份提供商并将之前复制的saml元数据上传到腾讯云。

The screenshot shows the Tencent Cloud Access Management (SSO) interface. On the left sidebar, under '身份提供商' (Identity Provider), the '角色SSO' (Role SSO) option is highlighted with a red box. The main content area is titled '角色SSO' (Role SSO) and contains a '新建提供商' (Create Provider) button. It also includes a note about '身份提供商(IdP)使用背景' (Background of Identity Provider(IdP)) and two points: 1. 角色SSO: 企业在本地IdP中管理员工信息，无需进行腾讯云和企业IdP间的用户同步，企业员工通过指定的CAM角色登录腾讯云； 2. 用户SSO: 腾讯云通过IdP颁发的SAML断言或OIDC令牌确定企业用户与腾讯云CAM用户的对应关系，企业用户登录后，使用该CAM用户访问腾讯云。 Below this is a table with columns: 提供商名称 (Provider Name), 提供商类型 (Provider Type), 创建时间 (Creation Time), 最后更新时间 (Last Update Time), and 操作 (Operations). The table currently shows '暂无数据' (No data available). At the bottom, there are pagination controls: 10 条 / 页, 1 / 1 页, and icons for refresh, copy, print, and close. A red box highlights the '角色SSO' (Role SSO) button in the sidebar.

然后创建一个新的角色，并选择之前的身份提供商作为idp提供商。

The screenshot shows the Tencent Cloud CAM (Cloud Access Management) interface under the '访问管理' (Access Management) section. On the left sidebar, '角色' (Role) is selected and highlighted with a red box. The main area displays a table of roles with columns: 角色名称 (Role Name), 角色ID (Role ID), 角色载体 (Role Carrier), 角色描述 (Role Description), 标签信息 (Tag Information), 会话最大时长 (Session Max Duration), and 创建时间 (Creation Time). A search bar at the top right allows filtering by role name or description. On the far right of the table, there are several icons for managing individual roles.

在Casdoor中配置SAML应用

在应用编辑页面，选择你刚刚创建的证书。在重定向URLs中添加你将使用的腾讯云应用的域名。

This screenshot shows the Casdoor application configuration page for a SAML application. It includes fields for Cert (selected: cert-built-in), Redirect URLs (with https://cloud.tencent.com added), Token format (JWT), Token expire (168 Hours), Refresh token expire (168 Hours), and a list of SAML attributes.

在应用编辑页面，输入ACS URL并配置Saml属性。

This screenshot continues the Casdoor configuration for the SAML application. It shows the Grant types (Authorization Code), SAML reply URL (https://cloud.tencent.com/login/saml), and the SAML Attribute section. The SAML Attribute table is highlighted with a red box, showing two entries: one for Role and one for RoleSessionName, both with their respective Name format and Value fields filled.

Saml属性的配置信息如下：

名称	名称格式	值
<code>https://cloud.tencent.com/SAML/Attributes/Role</code>	未指定	qcs::cam::uin/{AccountID}:roleName/{RoleName1};qcs::cam::uin/{AccountID}:roleName/{RoleName2},qcs::cam::uin/{AccountID}:provider/{ProviderName}
<code>https://cloud.tencent.com/SAML/Attributes/RoleSessionName</code>	未指定	casdoor

① 信息

- 在角色源属性中，将{AccountID}、{RoleName}和{ProviderName}替换为以下内容：
- 将{AccountID}替换为您的腾讯云账户ID，可以在[账户信息 - 控制台](#)中查看。
- 将{RoleName}替换为您在腾讯云中创建的角色名称，可以在[角色 - 控制台](#)中查看。
- 将{ProviderName}替换为您在腾讯云中创建的SAML身份提供商的名称，可以在[身份提供商 - 控制台](#)中查看。

您可以访问[腾讯云SAML身份提供商文档](#)以获取更详细的信息。

使用Casdoor SAML登录

SAML的一般登录步骤如下：用户 → 腾讯云（未登录） → 重定向到Casdoor进行登录 → 腾讯云（已登录）。现在，使用外部代码模拟前两步并生成一个重定向到Casdoor的URL。示例代码：

```
func main() {
    res, err := http.Get("your casdoor application saml metadata url")
    if err != nil {
        panic(err)
    }

    rawMetadata, err := ioutil.ReadAll(res.Body)
    if err != nil {
        panic(err)
    }

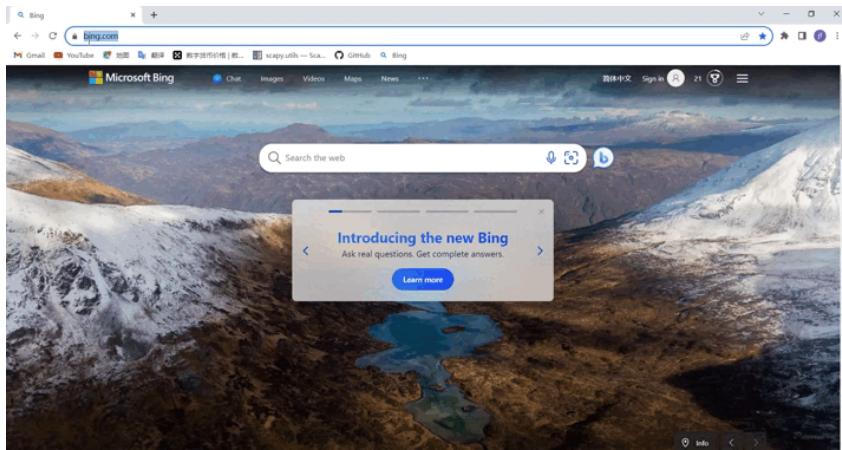
    metadata := &types.EntityDescriptor{}
    err = xml.Unmarshal(rawMetadata, metadata)
    if err != nil {
        panic(err)
    }

    certStore := dsig.MemoryX509CertificateStore{
        Roots: []*x509.Certificate{},
    }

    for _, kd := range metadata.IDPSSODescriptor.KeyDescriptors {
        for idx, xcert := range kd.KeyInfo.X509Data.X509Certificates {
            if xcert.Data == "" {
                panic(fmt.Errorf("metadata certificate(%d) must not be empty", idx))
            }
            certData, err := base64.StdEncoding.DecodeString(xcert.Data)
            if err != nil {
                panic(err)
            }

            idpCert, err := x509.ParseCertificate(certData)
```

一旦我们运行代码并获取到auth URL，点击URL就可以测试登录了。我们提供了一个这个过程的演示。



面部识别

概述

我们现在通过利用 face-api.js，将 Face ID 登录集成到了 Casdoor 中。

启用方法

在组织的个人页设置项中添加 Face ID 选项

用户管理 → 组织 → 选择一个组织 → 找到 个人页设置项 部分并添加 Face ID。

The screenshot shows the 'Account items' configuration page in Casdoor. On the left, there is a list of account items: Name, Organization, ID, Name, Display name, Avatar, User type, Password, Email, Phone, Country code, Country/Region, Location, Affiliation, Title, Homepage, Bio, Tag, Signup application, Roles, Permissions, Groups, 3rd-party logins, Properties, Is admin, Is forbidden, Is deleted, Multi-factor authentication, WebAuthn credentials, and Managed accounts. A red arrow points to the 'Add' button at the top right of the list. Another red arrow points to the 'Face ID' entry in the 'Properties' section, which is highlighted with a red border.

在此之后，你会在用户界面下找到 Face ID 选项，用户可以上传他们的面部数据用于登录。

用户管理 → 用户 → 选择一个用户 → 找到 Face IDs 并添加面部数据。你最多可以添加 5 条面部数据，并且可以为每条面部数据自定义名称。



第三步：在应用程序的登录方式部分中添加 Face ID 作为登录选项。

身份认证 → 应用 → 选择一个应用程序 → 转到 登录方式 部分 并将 Face ID 作为登录选项。



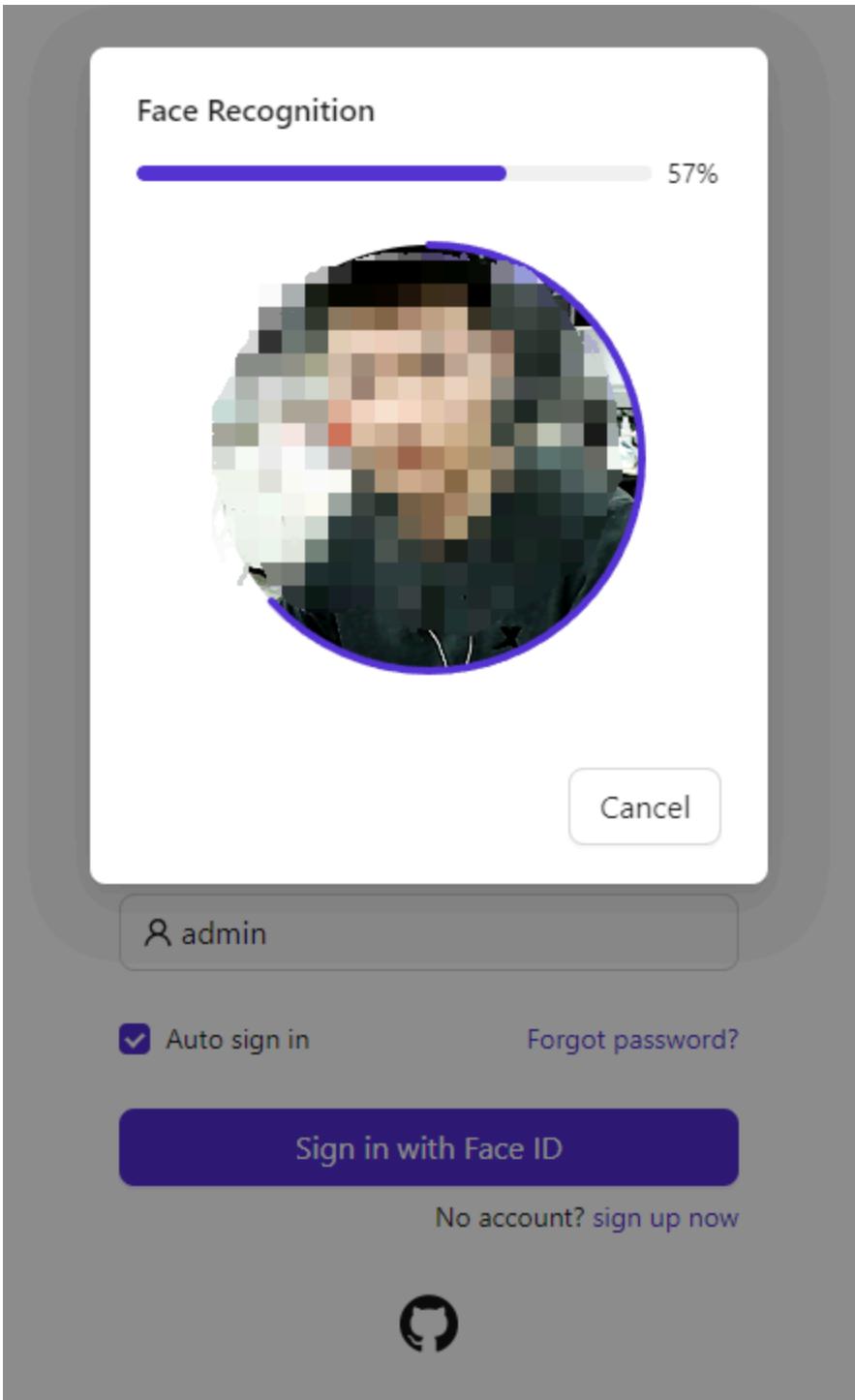
最后，你可以在登录页面使用 Face ID 方式进行登录。

1. 在登录页面，选择 Face ID 登录方式。
2. 输入用户名。点击 人脸登录。
3. 一旦你授予摄像头访问权限，你就可以使用 Face ID 进行登录。



Casdoor

[Password](#)[Email](#)[Face ID](#)[WebAuthn](#) admin Auto sign in[Forgot password?](#)[Sign in with Face ID](#)[No account? sign up now](#)



这是一个演示如何配置 Face ID 登录的视频：

WebAuthn

概述

我们很高兴地通知Casdoor的客户， Casdoor现在支持使用WebAuthn登录。这意味着您可以使用您的生物识别，如指纹或面部识别，甚至U盘登录，只要您的设备支持这些酷炫的授权方法和WebAuthn。

什么是 WebAuthn？

WebAuthn是Web认证API，由W3C和FIDO与Google、Mozilla、Microsoft、Yubico等公司共同编写的规范。这个API允许服务器使用公钥加密而不是密码来注册和认证用户。它使服务器能够与设备内置的强大认证器集成，如Windows Hello或Apple的Touch ID。

简单来说，WebAuthn要求用户生成一个公钥-私钥对，并将公钥提供给网站。当用户想要登录一个网站时，网站生成一个随机数，并要求用户用他们的私钥加密它并将结果发送回来。收到结果后，网站使用公钥对其进行解密。如果解密后的数字与之前生成的随机数匹配，用户被视为合法用户，并被授予登录权限。公钥和必要信息（如用户名或用户的授权者信息）的组合被称为WebAuthn凭证，由网站存储。

公钥-私钥对独有且唯一地与三个信息关联：用户的用户名、用户的授权者和网站的URL。这意味着，如果（用户的用户名、用户的授权者和网站的URL）的组合相同，那么密钥对应该是相同的，反之亦然。

关于WebAuthn技术的更详细信息，您可以访问<https://webauthn.guide/>。

如何在Casdoor中使用WebAuthn？

在登录页面，您可能已经注意到了使用WebAuthn登录的选项。然而，如果你还没有

WebAuthn凭证（可以类比为WebAuth密码），这个教程将向你展示如何创建和管理一个凭证，然后使用它登录。

步骤0：修改配置并启用WebAuthn认证

在 `conf/app.conf` 文件中，你可以找到以下配置：

```
origin = "http://localhost:8000"
```

请确保此配置与您网站的URL完全匹配。

注意：只有HTTPS支持WebAuthn，除非你正在使用localhost。

接下来，以管理员身份登录，进入你的应用的编辑页面。打开“启用WebAuthn登录”开关。默认情况下，此功能未启用。

步骤1：进入“我的账户”页面

导航到账户页面。在这个页面，你应该看到“添加WebAuthn凭证”按钮和一个显示你之前注册的所有WebAuthn凭证的列表。

The screenshot shows the Casdoor account management interface. At the top, there is a search bar labeled "Signup application" and a dropdown menu. Below it, under "3rd-party logins", there is a GitHub icon with the text "(empty)" and a "Link" button. Under "WebAuthn credentials", there is a table with one row containing a QR code and a "Delete" button. Below the table, there are sections for "Roles", "Permissions", and several toggle switches for "Is admin", "Is global admin", "Is forbidden", and "Is deleted". At the bottom, there are "Save" and "Save & Exit" buttons.

点击按钮并按照设备的指示在Casdoor中注册一个新的凭证。你可以使用列表中的“删

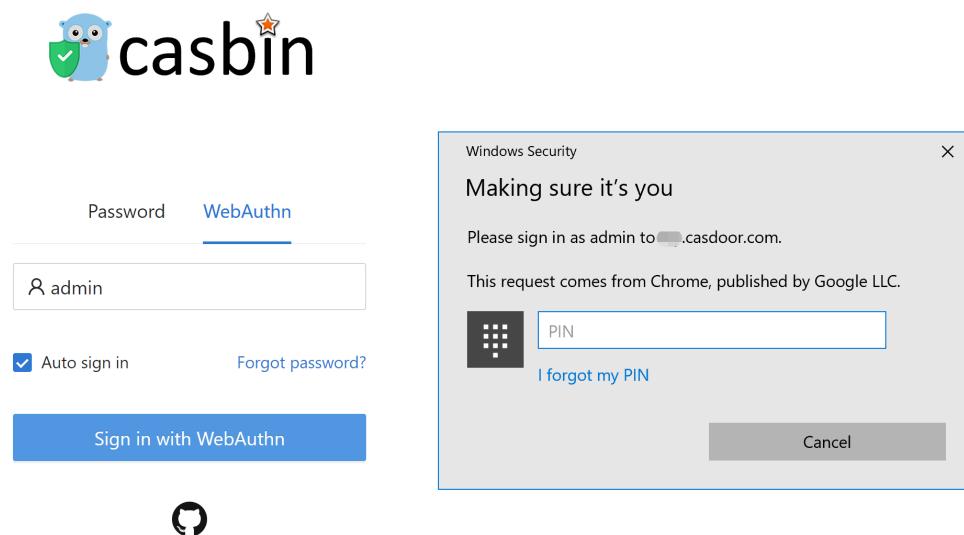
除"按钮删除任何凭证。

步骤2：使用WebAuthn登录

在开始这一步之前，确保你已经退出了Casdoor。

进入登录页面，选择WebAuthn登录方法，输入你的用户名，然后点击登录按钮。按照设备的指示操作。

(例如，如果你正在使用指纹和Windows Hello，你应该看到这样的东西)



然后你就会成功登录。



>

开发指南

开发指南

前端

Casdoor 前端开发指南

生成 Swagger 文件

生成 Swagger 文件

前端

Casdoor的前端源代码位于 /web 文件夹内: <https://github.com/casdoor/casdoor/tree/master/web>

这是一个 [Create-React-App \(CRA\)](#) 项目，遵循下面概述的经典CRA文件夹结构：

文件/目录	描述
public	React的根HTML文件
src	源代码
craco.config.js	Craco配置文件。 您可以在此处更改主题颜色（默认为蓝色）
crowdin.yml	Crowdin i18n 配置文件
package.json	NPM/Yarn 依赖文件
yarn.lock	Yarn lockfile

在 /src 目录中，您将找到几个重要的文件和文件夹：

文件/目录	描述
account	已登录用户的"我的个人资料"页面
auth	所有与身份验证相关的代码，如OAuth, SAML, 注册

文件/目录	描述
	页面， 登录页面， 忘记密码页面等。
backend	调用Go后端API的SDK。 它包含所有的 <code>fetch()</code> 调用
basic	Casdoor的主页（仪表板页面）， 包含了几个卡片小部件
common	共享UI部件
locales	i18n翻译文件以JSON格式， 与我们的Crowdin项目同步： https://crowdin.com/project/casdoor-site
App.js	包含所有路由的入口JS文件
Setting.js	其他代码使用的实用函数
OrganizationListPage.js	组织列表的页面， 与所有其他的 <code>xxxListPage.js</code> 文件类似
OrganizationEditPage.js	用于编辑一个组织的页面， 与所有其他的 <code>XXXEditPage.js</code> 文件类似

生成 Swagger 文件

概述

我们知道，beego框架提供了生成swagger文件的支持，以通过名为"bee"的命令行工具来阐明API。Casdoor也是基于beego构建的。然而，我们发现由bee生成的swagger文件未能使用"@Tag"标签对API进行分类。所以，我们修改了原始的蜜蜂以实现这个功能。

如何写comment

大多数规则与原始蜜蜂注释格式完全相同。唯一的差异在于，API应根据"@Tag"标签划分为不同的组。因此，开发者有责任确保这个标签被正确添加。这是一个例子：

```
// @Title Login
// @Tag Login API
// @Description login
// @Param oAuthParams     query    string  true        "oAuth
parameters"
// @Param body    body    RequestForm  true        "Login
information"
// @Success 200 {object} controllers.api_controller.Response The
Response object
// @router /login [post]
func (c *ApiController) Login() {
```

带有相同"@Tag"标签的API将被放入同一组。

如何生成swagger文件

0. 以正确的格式为API编写注释。
1. 获取此仓库: <https://github.com/casbin/bee>。
2. 构建修改后的蜜蜂。例如，在casbin/bee的根目录中，运行以下命令：

```
go build -o mybee .
```

3. 将mybee复制到casdoor的基础目录。
4. 在那个目录中，运行以下命令：

```
mybee generate docs
```

5. (可选) 如果你想为特定的标签或API生成swagger文档，以下是一些示例命令：

```
mybee generate docs --tags "Adapter API"  
mybee generate docs --tags "Adapter API,Login API"  
mybee generate docs --apis "add-adapter"  
mybee generate docs --apis "add-adapter,delete-adapter"
```

值得注意的是：当提供多个标签/接口时，我们只接受逗号，作为分隔符。

然后你会发现新的swagger文件已经生成。



>

组织

组织

概述

Casdoor的基本单位 — 组织

组织树

组织内的用户群组(group)

密码复杂度

支持不同的密码复杂度选项。

Password Obfuscator

Supporting different password obfuscator options.

 **账户自定义**

自定义用户帐户项目

 **自定义主题**

了解如何为组织和组织内的应用程序定制主题

 **管理多因素认证项目**

在组织中配置多因素认证项目

概述

组织是Casdoor的基本单位，它管理着用户和应用。如果一个用户登录到一个组织，他可以在无需再次登录的情况下访问属于该组织的所有应用。

在[应用](#)和[提供商](#)配置中，选择一个组织是很重要的一项，它决定了一个用户是否能够使用特定的提供商访问该应用。

我们还可以在Casdoor建立LDAP。更多详细信息，请参阅[LDAP 文档](#)。

Casdoor提供了多种密码存储算法，可在组织编辑页面中选择。

名称	算法	描述	场景
plain	-	密码将以明文形式存储。(默认)	-
salt	SHA-256	SHA-256 是一个获得专利的加密哈希函数，输出256位长的值。	-
md5-salt	MD5	MD5 message-digest algorithm是一种加密中断但仍广泛使用的哈希函数，可产生128位哈希值。	Discuz!
bcrypt	bcrypt	bcrypt 是一个密码哈希函数，用于安全地对密码进行哈希和加密。	Spring Boot, WordPress
pbkdf2-salt	SHA256	PBKDF2 是一个简单的派生函数，能够	Keycloak

名称	算法	描述	场景
	与 PBKDF2	抵制字典攻击和彩虹表攻击. 它是 Cassdoor 为 Keycloak 同步器而采用的原生实现。如果您通过 Keycloak 同步器导入用户，请选择此选项。	

💡 提示

除了通过应用程序登录到 Casdoor 之外(重定向到Casdoor以便SSO)， Casdoor 用户也可以选择通过该组织的登录页面直接登录到 Casdoor:

`/login/<organization_name>`，例如示例站点中的
<https://door.casdoor.com/login/casbin>

组织树

群组是组织内用户的一个集合 一个用户可以属于多个群组

Group properties

- **Owner**: 群组所属的组织
- **Name**: 群组的唯一名称
- ``
- ``
- ``
- **Type**: 群组可以被区分为 **Physical** 或 **Virtual** 一个用户只能存在在一个 **Physical** 组中, 但可以存在在多个 **Virtual** 组中.
- **ParentGroup**: 群组的父级群组.(最顶级群组的父组是其组织)

管理群组

有两种方式管理群组

1. 在组织列表页, 你可以预览所有组织下的群组

Name	Organization	Created time	Updated time	Display name	Type	Parent group	Action
casdoor_virtual	built-in	2023-06-12 12:37:44	2023-06-12 12:37:51	Casdoor Project Virtual Team	Virtual		<button>Edit</button> <button>Delete</button>
casbin_virtual	built-in	2023-06-12 12:37:18	2023-06-12 12:37:36	Casbin Project Virtual Team	Virtual		<button>Edit</button> <button>Delete</button>
dev_frontend	built-in	2023-06-12 09:43:18	2023-06-12 12:35:51	Dev (Frontend)	Physical		<button>Edit</button> <button>Delete</button>
dev_backend	built-in	2023-06-12 09:20:28	2023-06-12 12:35:58	Dev (Backend)	Physical		<button>Edit</button> <button>Delete</button>
dev	built-in	2023-06-09 18:19:06	2023-06-12 12:36:08	R & D	Physical		<button>Edit</button> <button>Delete</button>
sales	built-in	2023-06-09 01:27:19	2023-06-12 12:36:27	Sales	Physical		<button>Edit</button> <button>Delete</button>
marketing	built-in	2023-06-09 01:26:16	2023-06-12 12:36:32	Marketing	Physical		<button>Edit</button> <button>Delete</button>
hr	built-in	2023-06-09 01:25:46	2023-06-12 12:36:43	HR	Physical		<button>Edit</button> <button>Delete</button>
sales_and_marketing	built-in	2023-06-09 01:23:35	2023-06-12 12:36:57	Sales & Marketing	Physical		<button>Edit</button> <button>Delete</button>

9 in total < 1 > 10 / page

2. 在组织的列表页中单击 群组 按钮

Name	Created time	Display name	Favicon	Website URL	Password type	Password salt	Action
saas	2023-05-31 00:05:42	SaaS Users		https://saas.casbin.com	plain		<button>Edit</button> <button>Delete</button>
gsoc	2021-02-11 23:26:20	GSoC Community		https://gsoc.com.cn	plain		<button>Edit</button> <button>Delete</button>
casbin	2021-02-11 23:26:20	Casbin Organization		https://forum.casbin.com	plain		<button>Edit</button> <button>Delete</button>
built-in	2021-02-10 00:37:06	Built-in Organization		https://door.casdoor.com	plain		<button>Edit</button> <button>Delete</button>

4 in total < 1 > 10 / page

这将展示组织下群组的树形结构

The screenshot shows the Casdoor interface for managing organizations. On the left, there is a sidebar with a tree view of groups:

- Root node: Casdoor Project Virtual Team
- Child node: Casbin Project Virtual Team
- Child node: R & D
 - Child node: Dev (Frontend)
 - Child node: Dev (Backend)
- Child node: HR
- Child node: Sales & Marketing
 - Child node: Sales
 - Child node: Marketing

To the right of the tree view is a table listing users:

Organization	Application	Name	Created time	Display name
built-in	app-built-in	牛头	2023-06-16 16:16:35	牛头
built-in	app-built-in	喝咖啡就大蒜	2023-06-15 10:58:48	喝咖啡就大蒜
built-in	app-built-in	danceshow	2023-06-15 10:53:48	街舞show
built-in	app-built-in	TT珍惜	2023-06-15 10:36:46	TT珍惜
built-in	app-built-in	hashjoin	2023-06-15 01:01:17	hashjoin
built-in	app-built-in	zhangyaphet@gmail.com	2023-06-14 15:50:23	pengwei zhang

这里有一个视频展示了如何管理群组

The screenshot shows the Casdoor interface for managing groups. The table lists the following groups:

Name	Organization	Created time	Updated time	Display name	Type	Parent group	Action
group_smf8bi	built-in	2023-06-13 23:25:31	2023-06-13 23:25:36	总部	Virtual	built-in	<button>Edit</button> <button>Delete</button>
group_zxak7d	built-in	2023-06-11 23:28:45	2023-06-13 23:24:36	New Group - zxak7d	Virtual	New Group - nahuap	<button>Edit</button> <button>Delete</button>
group_1t8lrr	built-in	2023-06-09 09:39:44	2023-06-13 23:24:46	美工	Virtual	研发子部门	<button>Edit</button> <button>Delete</button>
group_nahuap	built-in	2023-06-09 09:27:47	2023-06-12 09:36:45	New Group - nahuap	Virtual		<button>Edit</button> <button>Delete</button>
group_38ii7o	built-in	2023-06-07 21:48:49	2023-06-11 09:49:13	研发子部门	Virtual		<button>Edit</button> <button>Delete</button>
group_gnrtip9	built-in	2023-06-07 20:59:10	2023-06-13 23:24:51	实体组3	Physical	built-in	<button>Edit</button> <button>Delete</button>
group_5aca0x	forum	2023-06-06 08:24:33	2023-06-13 23:25:12	实体组2	Physical	forum	<button>Edit</button> <button>Delete</button>
group_3tt9wf	forum	2023-06-06 08:20:14	2023-06-13 23:25:06	顶级2	Virtual	forum	<button>Edit</button> <button>Delete</button>
group_azpdif	forum	2023-06-06 08:19:32	2023-06-09 10:50:25	顶级1	Virtual		<button>Edit</button> <button>Delete</button>
group_r89hga	built-in	2023-06-05 14:41:41	2023-06-12 09:38:28	研发部1	Virtual		<button>Edit</button> <button>Delete</button>

群组也可以在用户的资料页被编辑。

Title ? :	1122
Homepage ? :	
Bio ? :	
Tag ? :	222
Karma ? :	333
Signup application ? :	app-built-in
Groups ? :	 Dev (Frontend)   Casdoor Project Virtual Team 
Roles ? :	
Permissions ? :	

密码复杂度

Casdoor支持为每个组织的用户密码自定义密码复杂度选项。

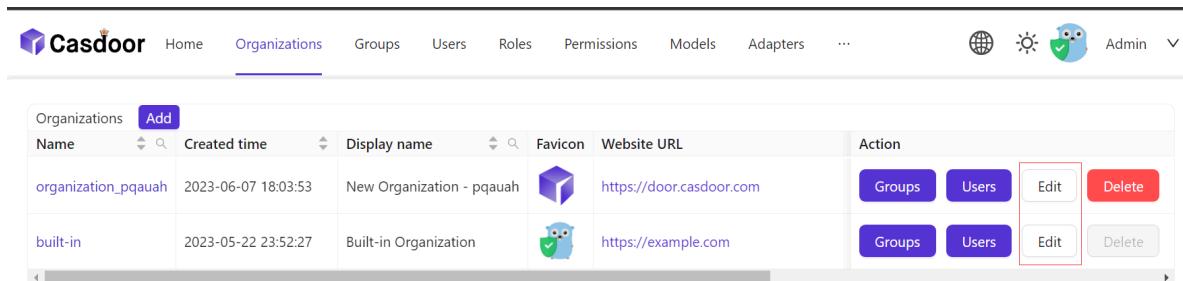
支持的复杂度选项

我们目前支持五个选项：

- `AtLeast6`: 密码必须至少有六个字符。
- `AtLeast8`: 密码必须至少有八个字符。
- `Aa123`: 密码必须至少包含一个大写字母，一个小写字母和一个数字。
- `SpecialChar`: 密码必须至少包含一个特殊字符。
- `NoRepeat`: 密码不能包含任何重复的字符。

如果你想使用多个选项，你可以在组织编辑页面上选择它们：

1. 在组织列表页面上点击编辑按钮。



The screenshot shows the Casdoor web application's organization management page. At the top, there is a navigation bar with links for Home, Organizations (which is underlined in blue), Groups, Users, Roles, Permissions, Models, Adapters, and more. On the far right, there are icons for a globe, a sun, a user profile, and Admin. Below the navigation is a search bar with placeholder text 'Search' and a magnifying glass icon. The main content area is a table titled 'Organizations'. It has a header row with columns for Name, Created time, Display name, Favicon, Website URL, and Action. There are two data rows: one for 'organization_pquaah' (created on 2023-06-07 18:03:53) and another for 'built-in' (created on 2023-05-22 23:52:27). Each row has a set of buttons in the 'Action' column: 'Groups', 'Users', 'Edit' (which is highlighted with a red border), and 'Delete'. The 'Edit' button for the 'organization_pquaah' row is specifically highlighted with a red box.

Name	Created time	Display name	Favicon	Website URL	Action
organization_pquaah	2023-06-07 18:03:53	New Organization - pquaah		https://door.casdoor.com	<button>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>
built-in	2023-05-22 23:52:27	Built-in Organization		https://example.com	<button>Groups</button> <button>Users</button> <button>Edit</button> <button>Delete</button>

2. 然后在密码复杂度选项列中选择你需要的选项。

Name: built-in

Display name: Built-in Organization

Favicon: URL: https://cdn.casbin.org/img/casbin/favicon.ico

Website URL: https://example.com

Password type: plain

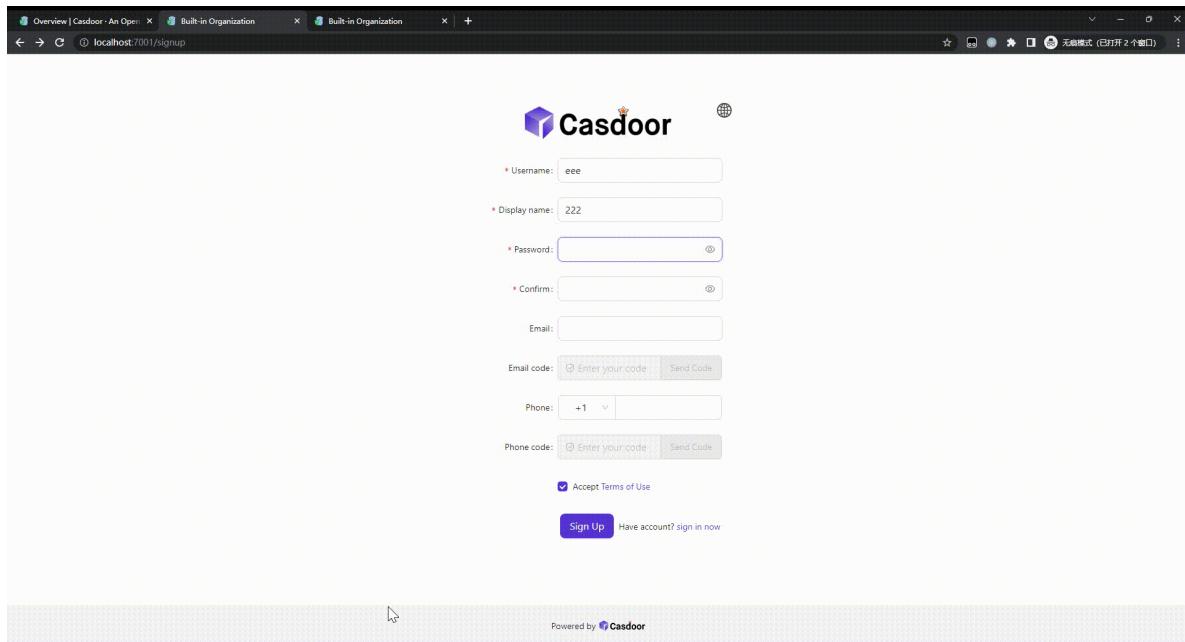
Supported country codes:

Languages:

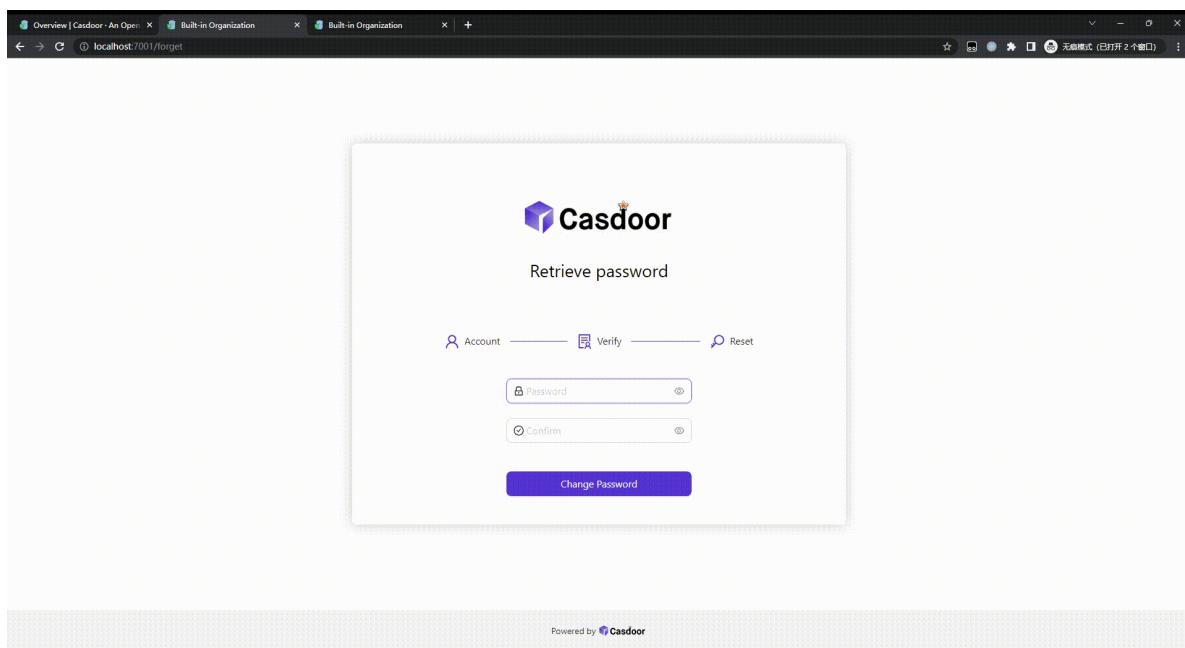
密码复杂度验证

我们在以下页面支持密码复杂度验证：

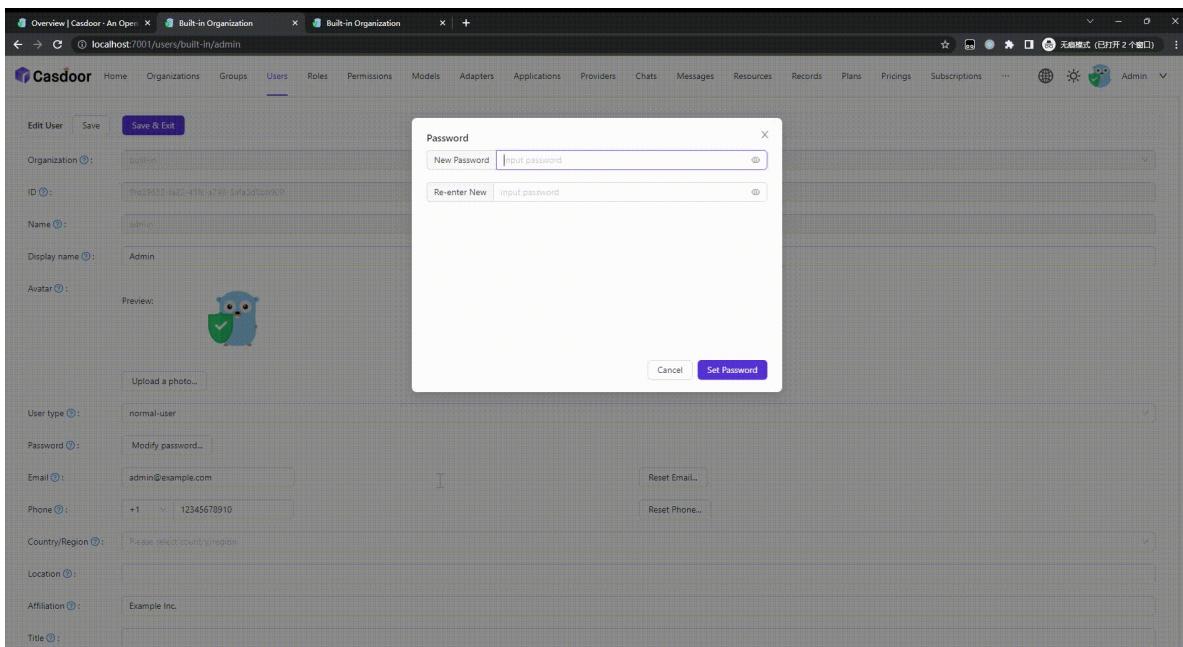
1. 注册页面。



2. 忘记密码页面。



3. 用户编辑页面。



Password Obfuscator

Here, we will show you how to enable the option to specify the password obfuscator for password parameters in the login and set-password APIs.

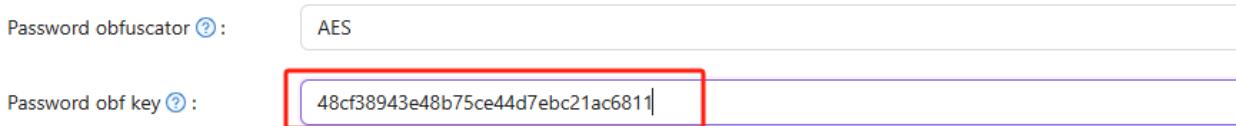
Configuration

On the organization edit page, you can find the `Password obfuscator` configuration option. You can select the encryption algorithm from the dropdown list.



- Plain: Password parameters will be transmitted directly in plain text.
- AES: Password parameters will first be encrypted using the AES algorithm and then transmitted in ciphertext form.
- DES: Password parameters will first be encrypted using the DES algorithm and then transmitted in ciphertext form.

Each time you update the encryption algorithm other than Plain, Casdoor will randomly generate an encryption key for you and populate it into the `Password obf key` configuration option. If you want to specify the encryption key for the encryption algorithm, you can modify the key in `Password obf key` configuration option:



ⓘ 备注

If your key does not meet the encryption algorithm requirements, Casdoor will prompt you with the regular expression that the key should meet in the error message.

API Support

Password obfuscation is supported by the following APIs:

- Login API (`/api/login`): Encrypts the password field during authentication
- Set Password API (`/api/set-password`): Encrypts both `oldPassword` and `newPassword` fields when changing passwords

When password obfuscation is enabled, Casdoor's frontend automatically encrypts password values before sending them to the server. The backend decrypts these values using the configured key and algorithm, then processes them normally.

Backward Compatibility

The set-password API maintains full backward compatibility. If obfuscation is not configured or decryption fails, the API automatically falls back to accepting plaintext passwords. This ensures compatibility with:

- Casdoor SDKs that may not support obfuscation yet
- Direct HTTP API calls using plaintext passwords
- Legacy integrations

Here is a demo video that shows how to use password obfuscator:

账户自定义

介绍

在组织中，您可以自定义用户的 账户项。这包括每个项目是否是 可见 及其 视图规则 和 修改规则。

当您自定义一个组织中的账户项目时，此配置将在该组织所有成员的主页上生效。

如何定制？

账户项目有四个属性：

Column Name	Selectable Value	Description
Name	-	Account item name.
Visible	<input type="checkbox"/> True / <input type="checkbox"/> False	Select whether this account item is visible on the user home page.
ViewRule	Rule Items	Select a rule to use when viewing the account item. Controls who can view this field.
ModifyRule	规则项	选择用于修改帐户项目的规则。 Controls who can edit this field.

Understanding View Rule and Modify Rule

View rule and Modify rule provide field-level permission control for user account items:

- **View rule:** Determines who can see the value of this account field (e.g., email, phone number, address)
- **Modify rule:** Determines who can change the value of this account field

This is different from the broader [Permission](#) feature, which controls access to applications and resources. View rule and Modify rule specifically control access to individual user profile fields.

Configuration Steps

要自定义账户项目，请遵循以下步骤：

1. Navigate to Organizations in the Casdoor sidebar
2. Click on your organization to open the Edit Organization page
3. Scroll down to the Account items section

Name	visible	viewRule	modifyRule	Action
Organization	<input checked="" type="checkbox"/>	Public	Admin	  
ID	<input checked="" type="checkbox"/>	Public	Immutable	  
Name	<input checked="" type="checkbox"/>	Public	Admin	  
Display name	<input checked="" type="checkbox"/>	Public	Self	  
Avatar	<input checked="" type="checkbox"/>	Public	Self	  
User type	<input checked="" type="checkbox"/>	Public	Admin	  
Password	<input checked="" type="checkbox"/>	Self	Self	  
Email	<input checked="" type="checkbox"/>	Public	Self	  
Phone	<input checked="" type="checkbox"/>	Public	Self	  
Country/Region	<input checked="" type="checkbox"/>	Public	Self	  
Location	<input checked="" type="checkbox"/>	Public	Self	  
Affiliation	<input checked="" type="checkbox"/>	Public	Self	  
Title	<input checked="" type="checkbox"/>	Public	Self	  
Homepage	<input checked="" type="checkbox"/>	Public	Self	  
Bio	<input checked="" type="checkbox"/>	Public	Self	  
Tag	<input checked="" type="checkbox"/>	Public	Admin	  
Signup application	<input checked="" type="checkbox"/>	Public	Admin	  
3rd-party logins	<input checked="" type="checkbox"/>	Self	Self	  

4. Casdoor 提供简单的操作来配置帐户项目：

a. Set item visibility

Control whether this account item is shown on the user home page:

Name	visible	viewRule	modifyRule
Organization	<input checked="" type="checkbox"/>	Public	Admin
ID	<input type="checkbox"/>		
Name	<input checked="" type="checkbox"/>	Public	Admin
Display name	<input checked="" type="checkbox"/>	Public	Self
Avatar	<input checked="" type="checkbox"/>	Public	Self
User type	<input checked="" type="checkbox"/>	Public	Admin

b. Set viewing and modifying rules

Configure who can view and modify each field:

visible	viewRule	modifyRule	Action
<input checked="" type="checkbox"/>	Public	Admin	<input type="button" value="^"/> <input type="button" value="v"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	Public		<input type="button" value="^"/> <input type="button" value="v"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	Self	Admin	<input type="button" value="^"/> <input type="button" value="v"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	Admin	Self	<input type="button" value="^"/> <input type="button" value="v"/> <input type="button" value="Delete"/>

Available Rules

There are 3 rules available for both View rule and Modify rule:

- Public: Everyone has permission. Any user can view/modify this field for any user.
- Self: Each user has their own permission. Users can only view/modify their own field values.
- Admin: The administrator has permission. Only organization administrators can view/modify this field for users.

Example Use Cases

Here are some common configuration patterns:

Field	View Rule	Modify Rule	Use Case
姓名	Public	Self	Everyone can see names, but users can only change their own

Field	View Rule	Modify Rule	Use Case
邮件	Self	Self	Users can only see and change their own email
手机号	Admin	Admin	Only admins can see and change phone numbers (for privacy)
显示名称	Public	Self	Public profile name visible to all
密码	Self	Self	Users can only change their own password

提示

Use Admin rules for sensitive fields like phone numbers, addresses, or internal identifiers that should only be managed by administrators.

备注

These field-level permissions work in conjunction with the broader [Permission system](#) in Casdoor. The Permission system controls access to applications and API resources, while View rule and Modify rule control access to specific user profile fields within the [Edit Organization](#) page configuration.

账户列表

以下是帐户项目中的所有字段。 关于描述详情，您可以查看 [用户](#)。

- 组织
- ID
- Name
- Display name
- 头像
- 用户类型
- Password
- Email
- Phone
- 国家/地区
- 城市
- 附属机构
- 职务
- 个人主页
- 自我介绍
- 标签
- 注册应用
- 第三方登录
- 属性
- 是否为管理员
- 是否为全局管理员
- 是否被禁用
- 是否已删除

自定义主题

Casdoor允许您定制主题以满足业务或品牌的UI多样性要求，包括主色和边框半径。

在Casdoor中，可以在全局、组织和应用程序级别定制主题。

1. 全局范围：这是Casdoor的默认主题，适用于选择遵循全局主题的任何组织。修改只能在Casdoor源代码中进行，不能在web UI中修改。
2. 组织范围：可以在组织编辑页面上定制组织的主题。此主题适用于组织内用户的所有Casdoor登录后页面，以及遵循组织主题的应用程序的入口页面（注册，登录，忘记密码等）。
3. 应用程序范围：可以在应用程序编辑页面上定制应用程序的主题。此主题适用于特定应用程序的入口页面（注册，登录，忘记密码等）。

定制组织主题

我们提供一个演示，演示如何为组织配置主题：

The screenshot shows the Casdoor application theme editor interface. At the top, there is a grid of permission items (e.g., Roles, Permissions, 3rd-party logins, Properties, Is admin, Is global admin, Is forbidden, Is deleted, WebAuthn credentials, Managed accounts) on the left and a corresponding grid of roles (e.g., Public, Immutable, Admin, Self) on the right. Each item has a switch to enable or disable it and icons for moving it up, down, and deleting it. Below this is a 'Theme' section with 'Follow global theme' and 'Customize theme' buttons. Under 'LDAPs', there is a table with one entry: 'BuildIn LDAP Server' (Server Name), 'example.com:389' (Server), 'ou=BuildIn,dc=example,dc=com' (Base DN), 'Disable' (Auto Sync), and 'Sync' (Last Sync). Action buttons 'Save' and 'Save & Exit' are at the bottom.

① 信息

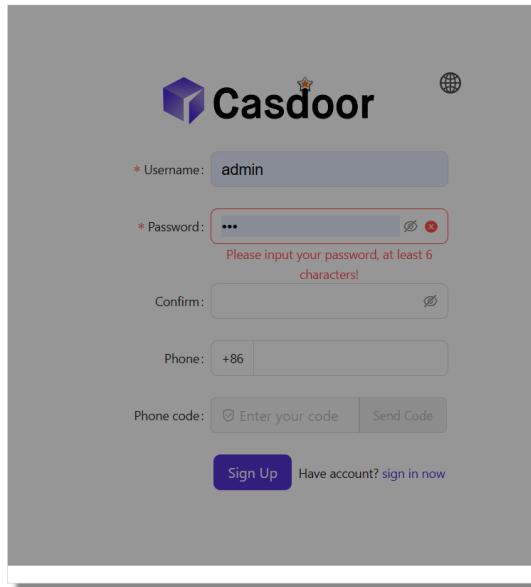
如果您的帐户组织与您正在编辑的组织相同，配置更改将立即生效，如上面的视频所示。但是，如果它们不同，您将需要登录到组织才能看到更改。

定制应用程序主题

应用程序可以使用与组织相同的主题编辑器定制主题。此外，您可以在预览面板中方便地预览主题。

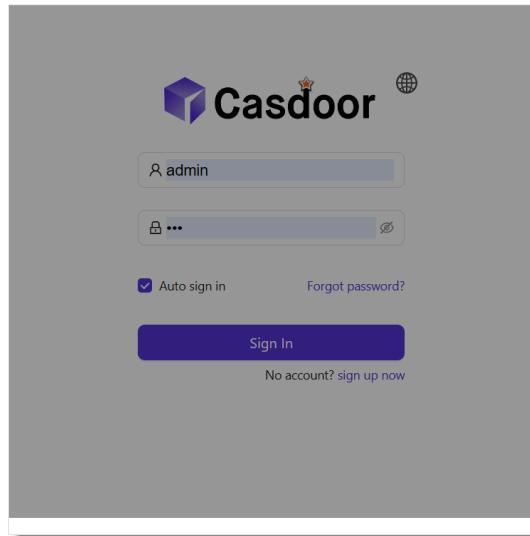
Preview ⓘ

 Copy signup page URL



The screenshot shows the Casdoor Signup page. It features a header with the Casdoor logo and a globe icon. Below the header are several input fields: a "Username" field containing "admin", a "Password" field with placeholder text "Please input your password, at least 6 characters!", a "Confirm" field, a "Phone" field with "+86", and a "Phone code" field with "Enter your code" and a "Send Code" button. At the bottom are "Sign Up" and "Have account? sign in now" buttons.

 Copy signin page URL



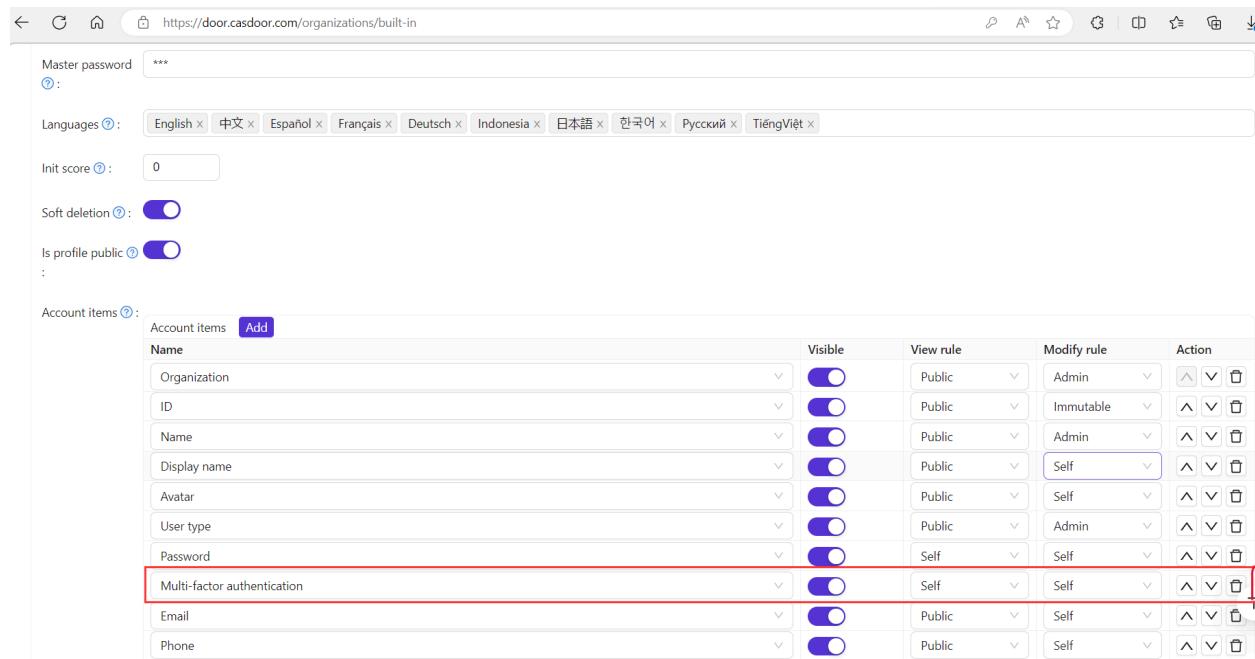
The screenshot shows the Casdoor Signin page. It has a header with the Casdoor logo and a globe icon. The "Username" field contains "admin". Below it is a "Password" field with a lock icon and a visibility toggle. To the right of the password field are "Auto sign in" and "Forgot password?" checkboxes. A large "Sign In" button is at the bottom, with a "No account? sign up now" link below it.

Background URL

管理多因素认证项目

在组织中添加多因素认证项目

在组织中，管理员可以将多因素认证项目添加到帐户设置中。这允许用户在他们自己的个人资料页面上配置多因素认证。



The screenshot shows the Casdoor organization settings page at <https://door.casdoor.com/organizations/built-in>. The 'Account items' section is displayed, listing various account fields like Name, ID, Display name, Avatar, User type, Password, and Multi-factor authentication. The 'Multi-factor authentication' row is highlighted with a red box. The table includes columns for 'Visible', 'View rule', 'Modify rule', and 'Action'. The 'Multi-factor authentication' row has 'Visible' set to 'Self', 'View rule' set to 'Self', and 'Modify rule' set to 'Self'. The 'Action' column contains icons for edit, delete, and copy.

Name	Visible	View rule	Modify rule	Action
Organization	<input checked="" type="checkbox"/>	Public	Admin	edit delete copy
ID	<input checked="" type="checkbox"/>	Public	Immutable	edit delete copy
Name	<input checked="" type="checkbox"/>	Public	Admin	edit delete copy
Display name	<input checked="" type="checkbox"/>	Public	Self	edit delete copy
Avatar	<input checked="" type="checkbox"/>	Public	Self	edit delete copy
User type	<input checked="" type="checkbox"/>	Public	Admin	edit delete copy
Password	<input checked="" type="checkbox"/>	Self	Self	edit delete copy
Multi-factor authentication	<input checked="" type="checkbox"/>	Self	Self	edit delete copy
Email	<input checked="" type="checkbox"/>	Public	Self	edit delete copy
Phone	<input checked="" type="checkbox"/>	Public	Self	edit delete copy

管理多因素认证项目

您可以管理多因素认证以确定哪些方法对用户可用。

管理多因素认证项目有两个规则：

- 可选：用户可以选择是否启用这种类型的多因素认证。

- 提示：如果用户未启用此多因素认证模式，他们在登录Casdoor后将被提示启用它。
- 必需：用户必须启用此多因素认证方法。

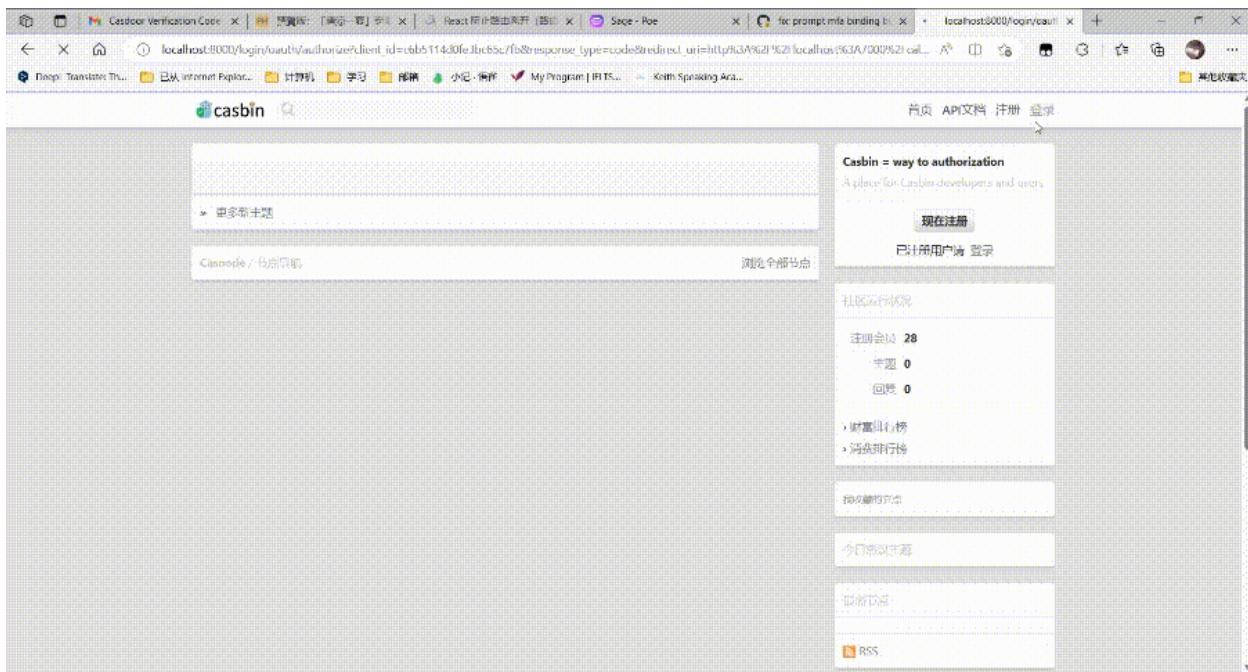
The screenshot shows the Casdoor MFA configuration page. It lists three MFA items: "Phone", "Email", and "App". The "Phone" item is set to "Prompt" rule, "Email" to "Optional", and "App" to "Required". There are also up/down arrows and delete icons for each row.

Name	Rule	Action
Phone	Prompt	
Email	Optional	
App	Required	

下面的图片显示了提示用户启用多因素认证的通知。

The screenshot shows the Casdoor dashboard with a modal dialog titled "Enable multi-factor authentication". The dialog contains the message: "To ensure the security of your account, it is recommended that you enable multi-factor authentication". It includes a "sms" button and two buttons at the bottom: "Later" and "Go to enable". The "Go to enable" button is highlighted with a red box.

此视频演示了当多因素认证方法设置为必需时，用户需要在完成登录过程之前启用多因素认证。



Remember Multi-Factor Authentication

When logging in to Casdoor, users can choose to have the Multi-Factor Authentication for this account remembered for a specific period. This means they won't be prompted to perform Multi-Factor Authentication for the account again during that time.

Multi-factor authentication

You have enabled Multi-Factor Authentication,
please enter the TOTP code

Remember this account for 12 hours

Next Step

Have problems? [Use a recovery code](#)

Powered by  Casdoor

You can set the duration for which Multi-Factor Authentication is remembered for an account in the organization settings. As shown, there is an "MFA remember time" option where you can specify the time (e.g., set it to 12 hours as in the example).

MFA remember time Hours



>

应用

应用

概览

Casdoor应用概述

术语参考

术语参考

应用程序配置

配置应用程序的身份验证

提供商

配置不同的提供商

登录方式

配置登录方式和登录方式的显示顺序

Exclusive Signin

Configure exclusive signin to allow only one active session per user

注册项目表

配置注册项目表以创建自定义注册页面

Signin Items Table

Configure the signin items table to create a custom signin page

自定义登录界面

自定义您的应用程序登录页面

指定登录组织

在登录页面上指定登录组织

标签

配置您的应用程序标签

应用邀请码

使用邀请码限制用户通过应用注册

Shared Application

Shared application across organizations

概览

Casdoor 中的每个应用都被称为“application”。它们之间没有关联，不会相互影响，这意味着只要你愿意，你可以单独部署或停止任何应用程序。

如果您想要使用Casdoor为您的网站提供登录服务，您可以将其添加为Casdoor应用。

这样用户在访问组织中的所有应用程序时就无需重复登录。

应用程序配置非常灵活和简单。您可以设置是否允许密码登录或第三方登录，配置您想要用户登录的第三方应用程序。您甚至可以自定义应用程序的注册项等。

在本章中，您将学习如何从头开始启动您自己的应用程序。

让我们一起探索吧！

术语参考

- `Name`: 创建的应用的名称。
- `CreatedTime`: 应用程序创建的时间。
- `DisplayName`: 应用程序向公众显示的名称。
- `Logo`: 应用程序的标志将会在登录和注册页面上显示。
- `HomepageUrl`: 应用程序主页的URL。
- `Description`: 描述应用程序。
- `Tags`: 只有在应用标签中列出标签的用户才能登录。
- `Organization`: 应用所属的组织。
- `EnableSignUp`: 如果用户可以注册。如果不是，应用程序的账户。
- `SigninMethods`: 登录方法的配置
- `SignupItems`: 用户注册时需要填写的字段。
- `Providers`: 为应用程序提供各种服务（如OAuth, 电子邮件, 短信服务）。
- `ClientId`: OAuth客户端ID。
- `ClientSecret`: OAuth客户端密钥。
- `RedirectUris`: 如果用户成功登录，Casdoor将导航到这些URI之一。
- `TokenFormat`: 生成的令牌的格式。它可以是以下格式：`JWT`（包含所有`User`字段），`JWT-Empty`（包含所有非空值）或`JWT-Custom`自定义访问令牌内的`User`字段。
- `ExpireInHours`: 登录将在几小时后过期。
- `SigninUrl`:
- `SignupUrl`: 如果您在Casdoor之外独立提供注册服务，请在此处填写URL。
- `ForgotUrl`: 与`SignupUrl`相同。
- `AffiliationUrl`:

应用程序配置

当你在你的服务器上部署你的casdoor并设置你的组织后，你可以现在就部署你的应用程序！

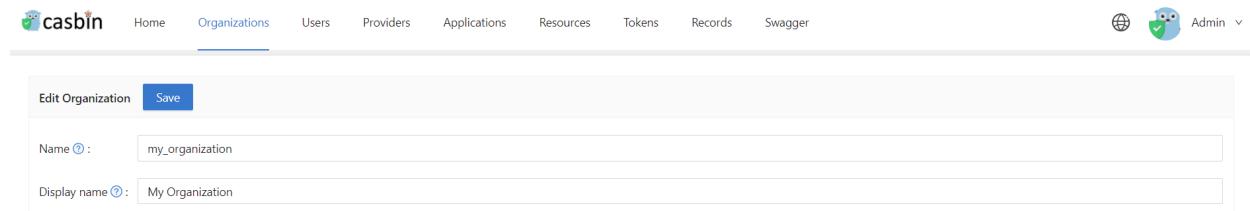
让我们看看如何使用Casdoor配置您的应用程序的身份验证！

① 备注

例如，我想要使用 Casnnode 设置我的论坛

我创建了我的应用程序并填写了必要的配置。

选择我创建的组织，以便组织中的用户也可以使用该应用程序。



The screenshot shows the Casdoor web interface. At the top, there is a navigation bar with links: Home, Organizations (which is highlighted), Users, Providers, Applications, Resources, Tokens, Records, and Swagger. On the far right, there is a user profile icon labeled "Admin". Below the navigation bar, the main content area has a title "Edit Organization" and a "Save" button. There are two input fields: "Name" (containing "my_organization") and "Display name" (containing "My Organization").

这个组织命名为 `my_organization`，我从下拉菜单中选择到它。

Edit Application Save

Name ? : my_forum

Display name ? : My Forum

Logo ? : URL: https://cdn.casbin.com/logo/logo_1024x256.png

Preview: 

Home ? :

Description ? :

Organization ? : built-in

Client ID ? : my_organization
built-in

接下来，我希望我的用户在注册时能够使用 Casdoor 作为认证。因此，我在这里填写重定向URL为 <https://your-site-url.com/callback>。

...警告

请注意，在提供商应用程序中的 `callback URL` 应该是Casdoor的回调 URL，而 Casdoor 中的 `Redirect URL` 应该是您网站的回调 URL 。

进一步了解

为了使认证过程发挥作用，详细步骤如下：

1. 用户将请求发送到Casdoor。

2. Casdoor 使用 `Client ID` (客户端ID) 和 `Client Secret` (客户端密钥) 获取 GitHub、谷歌或其他供应商的身份验证。
3. 如果认证成功, GitHub 会调用回到 Casdoor, 通知 Casdoor 已成功验证。因此, GitHub 认证回调 URL 应该是您的 Casdoor 的回调URL, 即 <http://your-casdoor-url.com/callback>
4. 接着, Casdoor 将认证成功通知应用程序。这意味着 Casdoor 回调 URL 应该是您的应用程序的回调 URL , 即 <http://your-site-url.com/callback>。

:::

You need to enable JavaScript to run this app.

Verification Code Settings

You can configure the **Code resend timeout** to control how long users must wait before requesting another verification code via email or SMS. Set the value in

seconds (default is 60). This setting determines the countdown timer duration shown to users on the login page. A value of 0 uses the global default.

:::提示

如果您想对应用程序的登录方式进行更个性化的配置，例如禁用某种登录方式或关闭某种登录方式，您可以参考[登录方式](#)

:::

提供商

您还可以通过添加提供商并设置其属性来添加第三方应用程序进行注册。

Name	Category	Type	Country/Region	Can signup	Can signin	Can unlink	Prompted	Signup group	Rule
provider_casbin_email	Email	M							
provider_tencent_sms	SMS	Cloud	All x						
provider_storage_aliyun_oss	Storage	Box							
provider_casdoor_github	OAuth	Github		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
provider_casdoor_google	OAuth	G		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		One Tap
provider_casdoor_facebook	OAuth	F		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
provider_casdoor_qq	OAuth	QQ		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
provider_casdoor_wechat	OAuth	WeChat		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
provider_casdoor_dingtalk	OAuth	DingTalk		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

我们的供应商可以区分不同的情况，您可以通过选择规则为不同的功能选择不同的供应商。有关各规则项目的详细解释，请参见下表。

规则	描述
注册	对于注册场景，您可以选择“注册”规则，供提供商发送相应的短信或电子邮件模板。
登录	对于登录场景，您可以为提供商选择“登录”规则。
忘记密码	当在应用程序中选择“忘记密码”场景的提供商时，您可以选择“忘记密码”规则。
重置密码	当在应用程序中选择“忘记密码”场景的提供商时，您可以选择“忘记密码”规则。

规则	描述
设置 MFA	对于 MFA 设置验证场景，可以选择“设置 MFA”规则。
MFA Auth	对于MFA Auth验证情景，您可以选择“MFA Auth”规则。欲了解更多关于mfa的信息，请参阅** MFA **
all	如果您想要为所有功能使用单个提供商，您可以选择“all”规则。这意味着同一个提供商将用于您的应用程序中提到的所有场景。

Providers :

Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Signup group	Rule	Action
provider_captcha_default	Captcha							Signup	
provider_xz5v54	SMS							All	
provider_clftfc	SMS							Signup	

Preview :

Copy signup page URL

Copy signin page URL

A dropdown menu is open on the right side of the interface, listing various actions:

- All
- Signup
- Login
- Forget Pa...
- Reset Pas...
- Set MFA
- MFA Auth

Providers :

Name	Category	Type	Country/Region	Can signup	Can signin	Can unlink	Prompted	Signup group	Rule	Action
provider_captcha_default	Captcha		+81 x +33 x +34 x						All	
forjp	SMS		+33 x +86 x						All	
forcn	SMS		+33 x +86 x						All	
forus	SMS		+34 x						All	
provider_01nwpa	SMS		All x						All	

登录方式

在应用配置页面上，我们可以配置登录项目表。 我们可以在表中添加和删除登录项目。

Signin methods ②:		Signin methods	Add
Name	Display name	Rule	Action
Password	Password	All	▲ ▼ ⏚
Verification code	Email	All	▲ ▼ ⏚
LDAP	LDAP		▲ ▼ ⏚
WebAuthn	WebAuthn		▲ ▼ ⏚

关于每个登录项目的详细解释，请参考下面的表格。 目前，只有 **密码**、**验证码**、**WebAuthn** 和 **LDAP** 登录方式可用。

列名	可选值	描述
名称	-	登录方式的名称。
DisplayName	-	登录方式向公众显示的名称。
规则项	规则项	选择一个规则来自定义这个登录方式。 详细规则在下表中描述。
操作	-	用户可以执行如移动此登录方式向上、向下或删除等操作。

目前，只有 **密码** 和 **验证码** 登录方式支持配置规则。

登录方式名称	可选规则	描述
密码	全部(默认) / 非 LDAP	选择用户可用的登录方式。选择全部，那么LDAP用户也可以登录。选择非LDAP，那么LDAP用户被禁止登录。
验证码	全部(默认) / 仅限电子邮件 / 仅限电话	选择用户可用的登录方式。选择全部，那么电子邮件和电话号码都可以用于登录验证。选择仅限电子邮件，那么只允许电子邮件登录。选择仅限电话，那么只允许电话号码进行登录验证。

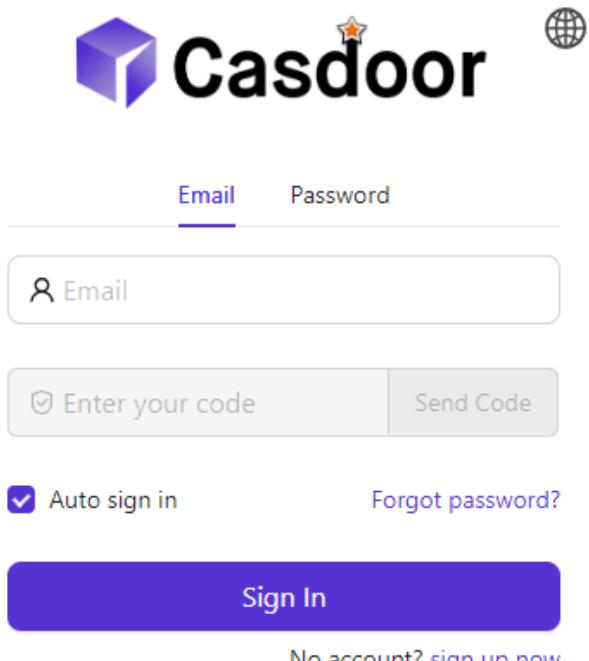
① 备注

例如，我们希望用户优先使用他们的电子邮件登录，如果他们不能使用电子邮件，那么考虑使用密码登录。

首先，我们配置两个登录选项，验证码和密码，并且验证码是第一个登录选项。然后我们将验证码规则更改为仅限电子邮件，这样用户只能通过电子邮件接收登录验证码。

Signin methods		Add	
Name	Display name	Rule	Action
Verification code	Email	Email only	^
Password	Password		^

为了让用户更容易理解，我们可以更改验证码登录方式的显示名称，这样用户就可以轻松理解这是电子邮件登录。



 提示

除LDAP外，所有登录选项默认都是启用的。并且要求至少添加一个登录方式。

这是一个登录方式如何工作的视频：

Exclusive Signin

Exclusive signin restricts users to maintaining only one active session at a time. When enabled, signing in from a new device or browser automatically terminates all previous sessions for that user.

Configuration

Enable exclusive signin in the application settings:

1. Navigate to Applications in Casdoor
2. Select your application
3. Toggle Enable exclusive signin

Once enabled, the system enforces single-session access for all users of that application.

Behavior

When a user with exclusive signin enabled signs in:

- Any existing active sessions are immediately terminated
- A new session is created for the current signin
- The user is logged out from all other devices or browsers

For example, if a user signs in on their laptop, then later signs in on their phone, the laptop session is automatically ended. Only the phone session remains active.

Security Implications

Exclusive signin prevents concurrent session abuse where multiple parties could access the same account simultaneously. This is particularly useful when users forget to sign out from shared or public computers, as the next signin automatically invalidates the previous session.

The feature also helps manage server resources by limiting the number of concurrent sessions, though users working across multiple devices will need to re-authenticate when switching between them.

Technical Implementation

When a user signs in with exclusive signin enabled:

1. Casdoor queries all existing sessions for that user and application
2. All found session IDs are destroyed in the backend
3. A new session is created and stored
4. Only the new session ID is maintained in the database

This per-application session management works independently for each application configured in Casdoor.

注册项目表

在应用配置页面上，我们可以配置注册项目表以创建自定义注册页面。我们可以在此注册项目表上添加或删除任何注册项目。

Signup items [?](#)

Name	Visible	Required	Prompted	Rule	Action
ID				Random	
Username	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Display name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		None	
Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Confirm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Normal	
Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Agreement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		None	

关于每个注册项目的详细解释，请参考下表。

列名	可选值	描述
名称	-	注册项目的名称。
可见	True / False	选择此注册项目是否在注册页面上可见。
必填	True / False	选择此注册项目是否为必填项。
提示	True /	选择是否在用户忘记填写此注册项目时提示。

列名	可选值	描述
	False	
Label	-	If this signup item start with Text, Label should be the html code for this field. If not it will repalce the label of this signup item.
Custom CSS	-	CSS code for this signup item.
规则	Rule Items	选择一个规则来自定义此注册项目。 详细规则在下表中描述。
操作	-	用户可以执行如移动此注册项目上移、下移或删除等操作。

目前，支持配置规则的注册项目包括 ID、显示名称、电子邮件和协议。

项目名称	可选规则	描述
ID	Random / Incremental	选择用户ID应该是随机生成还是递增。
显示名	None / Real name / First, last	选择显示名称应该如何呈现。 选择无将显示显示名称。 选择真实姓名将显示用户的实际姓名。 选择名, 姓将分别显示名和姓。

项目名称	可选规则	描述
称		
电子 邮 件	Normal / No verification	选择是否使用验证码验证电子邮件地址。选择正常将需要电子邮件验证。选择无验证将允许无需电子邮件验证即可注册。
协议	None / Signin / Signin (Default True)	选择用户在登录时是否需要确认使用条款。选择无将不显示任何使用条款，允许用户直接登录。选择登录将要求用户在登录前确认条款。选择登录（默认为真）将默认设置条款为已确认，允许用户直接登录。

① 备注

例如，假设我想设置我的注册页面包括一个电子邮件字段，但不需要电子邮件验证。

首先，我添加了一些注册所需的注册项目，如ID、用户名、密码和电子邮件。

Signup items		Add				
Name	Action	visible	required	prompted	rule	Action
ID	Incremental	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No verification	<input checked="" type="checkbox"/>
Username		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>
Password		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>
Email		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>

然后，我选择了电子邮件行的规则项目为无验证。结果，生成的预览注册页面将达到预期效果。



* Username:

* Password:

* Email:

Sign Up

Have account? [sign in](#)

now

Signin Items Table

On the application configuration page, we can configure the signin items table to create a customized registration page. We can add or delete any signin item on this signin items table.

Name	Visible	Label HTML	Custom CSS	Placeholder	Rule	Action
Back button	<input checked="" type="checkbox"/>		.back-button { top: 65 }			<input type="button"/> <input type="button"/> <input type="button"/>
Languages	<input checked="" type="checkbox"/>		.login-languages { top }			<input type="button"/> <input type="button"/> <input type="button"/>
Logo	<input checked="" type="checkbox"/>		.login-logo-box { }			<input type="button"/> <input type="button"/> <input type="button"/>
Signin methods	<input checked="" type="checkbox"/>		.signin-methods { }			<input type="button"/> <input type="button"/> <input type="button"/>
Username	<input checked="" type="checkbox"/>		.login-username { }			<input type="button"/> <input type="button"/> <input type="button"/>
Password	<input checked="" type="checkbox"/>		.login-password { }			<input type="button"/> <input type="button"/> <input type="button"/>
Agreement	<input checked="" type="checkbox"/>		.login-agreement { }			<input type="button"/> <input type="button"/> <input type="button"/>
Forgot password?	<input checked="" type="checkbox"/>		.login-forget-password { }			<input type="button"/> <input type="button"/> <input type="button"/>
Signin button	<input checked="" type="checkbox"/>		.login-button-box { ma }			<input type="button"/> <input type="button"/> <input type="button"/>
Signup link	<input checked="" type="checkbox"/>		.login-signup-link { ma }			<input type="button"/> <input type="button"/> <input type="button"/>
Providers	<input checked="" type="checkbox"/>		.provider-img { width: }			<input type="button"/> Small icon <input type="button"/>

For a detailed explanation of each signin item, please refer to the table below.

Column Name	Selectable Value	Description
Name	-	The name of the signin item.
Visible	True / False	Select whether this signin item is visible on the registration page.
Label HTML	-	If this signin item is added as a custom item, Label should be the html code for this field.

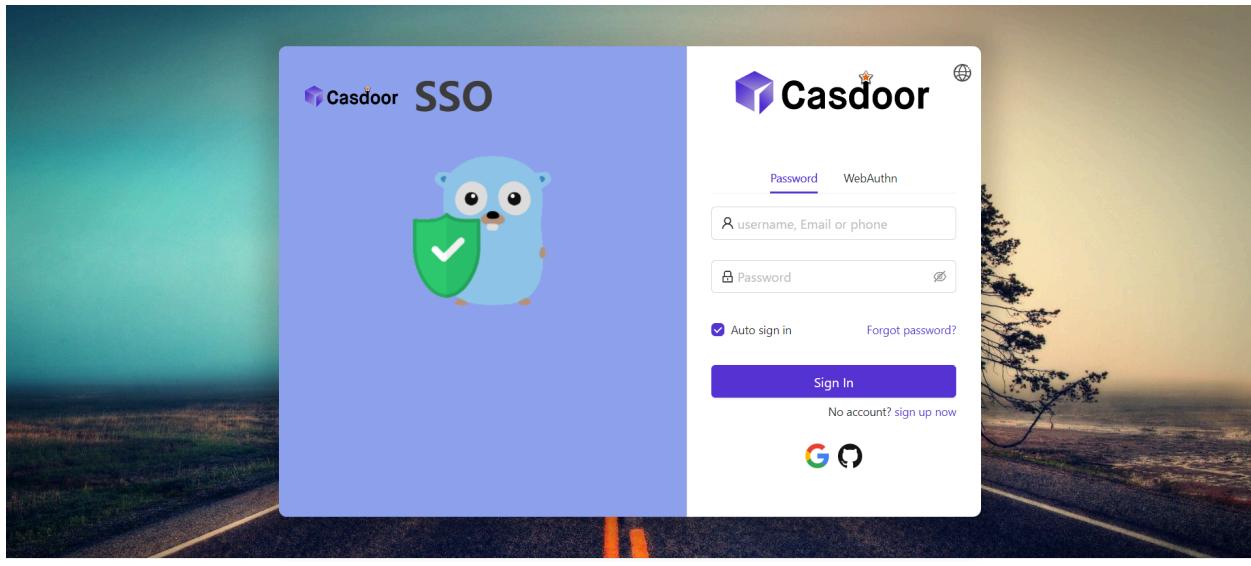
Column Name	Selectable Value	Description
Custom CSS	-	CSS code for this signin item.
Placeholder	-	The placeholder of the signin item.
Rule	<input type="button" value="Rule Items"/>	Select a rule to customize this signin item. Detailed rules are described in the table below.
Action	-	Users can perform actions such as moving this signin item up, moving it down, or deleting it.

The Captcha signin item supports configuration rules to control how verification is presented to users.

Item Name	Selectable Rules	Description
Captcha	<input type="button" value="Normal"/> / <input type="button" value="Inline"/>	Choose how captcha verification is displayed. <input type="button" value="Normal"/> shows a modal dialog when sending verification codes. <input type="button" value="Inline"/> displays the captcha directly on the signin page, streamlining the verification process.

自定义登录界面

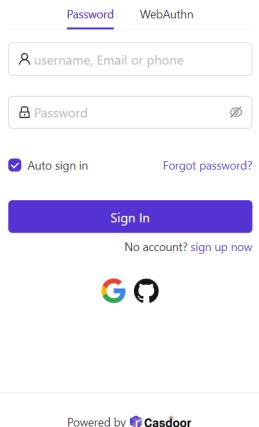
您已创建应用程序。现在，让我为你展示如何自定义应用的登录页面的UI。在这个指南中，我们将创建一个应用的自定义登录页面。



让我们开始吧

Part 1: 增加背景图片

首先，我们要添加背景图像。默认背景是白色的，看起来非常简单。



若要添加背景图像，请使用您喜欢的图像的 URL，填写 [背景 URL](#)。如果您填写了有效的URL，预览区域将会显示您所选择的图像。

Background URL ② :	URL ② : <input type="text" value=""/>
Preview:	
Form CSS ② :	<input type="text"/>
Form position ② :	<input type="radio"/> Left <input checked="" type="radio"/> Center <input type="radio"/> Right <input type="checkbox"/> Enable side panel

Part 2: 自定义登录面板

现在我们在第一步操作结束的页面：



Powered by Casdoor

为了让面板看起来很好，您需要添加一些CSS 代码。 复制下面的代码并粘贴到 **表单 CSS** 字段。

```
<style>
.login-panel{
    padding: 40px 30px 0 30px;
    border-radius: 10px;
    background-color: #ffffff;
    box-shadow: 0 0 30px 20px rgba(0, 0, 0, 0.20);
}
</style>
```

Background URL
URL : <https://static.runoob.com/images/demo/demo2.jpg>

Preview:



Form CSS :

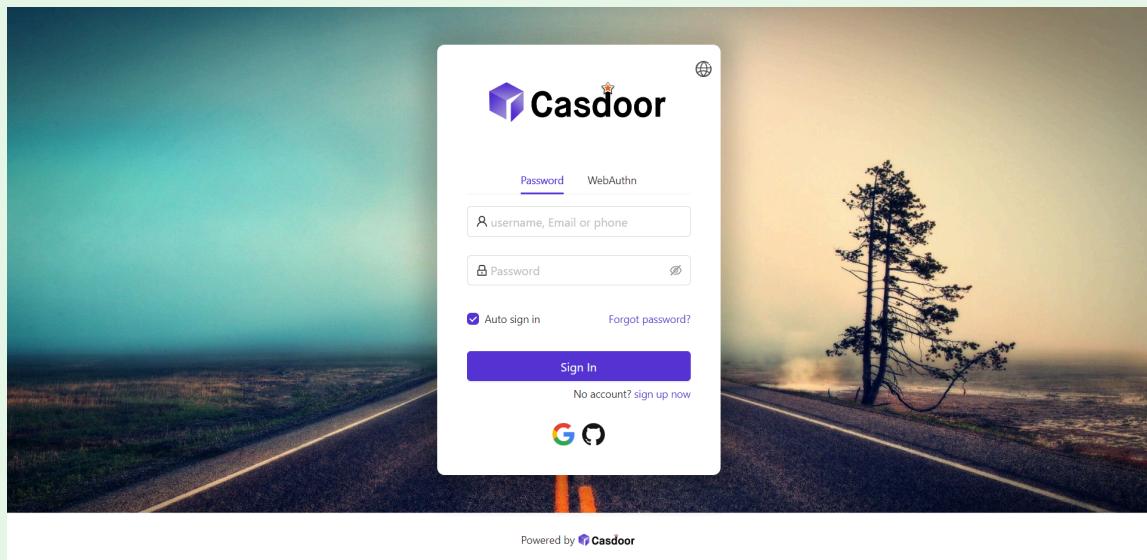
Form position :

💡 提示

当您编辑 `form CSS` 时，如果值为空，编辑器将显示默认值。然而，您仍然需要复制内容并将其粘贴到字段。

...

填写 `表单 CSS` 后，不要忘记在底部保存配置。好，让我们看看效果。



Part 3: 选择面板位置

现在登录页面就比刚开始的页面更为美观。 我们还为您提供了三个按钮，可以决定面板的位置。

Background URL
URL : <https://static.runoob.com/images/demo/demo2.jpg>

Preview:



Form CSS :

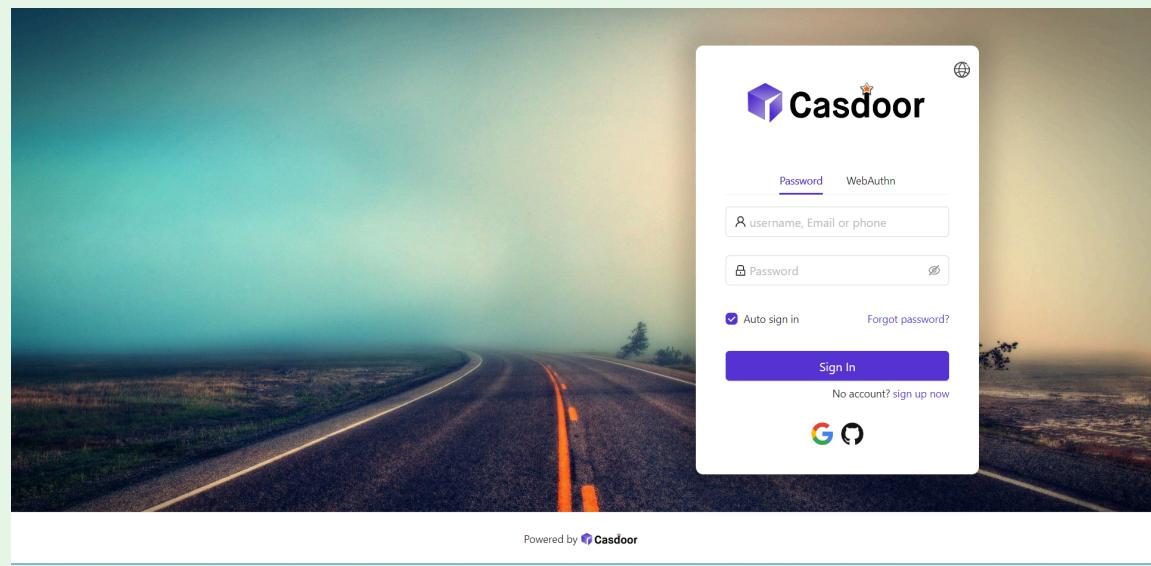
```
<style>.login-panel{ padding: 40px 30px 0 30px; border-radius: 10px; background-color: #fff; }</style>
```

Form position :

Left Center Right Enable side panel

The "Right" button is highlighted with a red box.

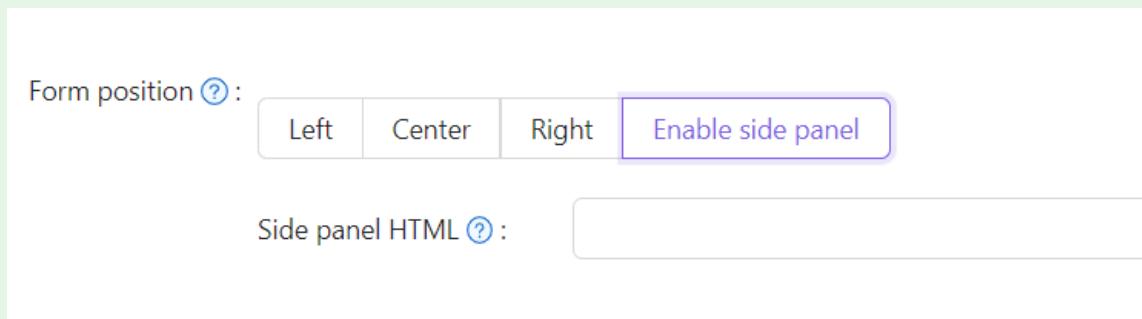
例如，选择 **Right** 按钮：



Part 4: 启用侧边面板

接下来，让我们看看如何启用侧边面板并自定义其样式。

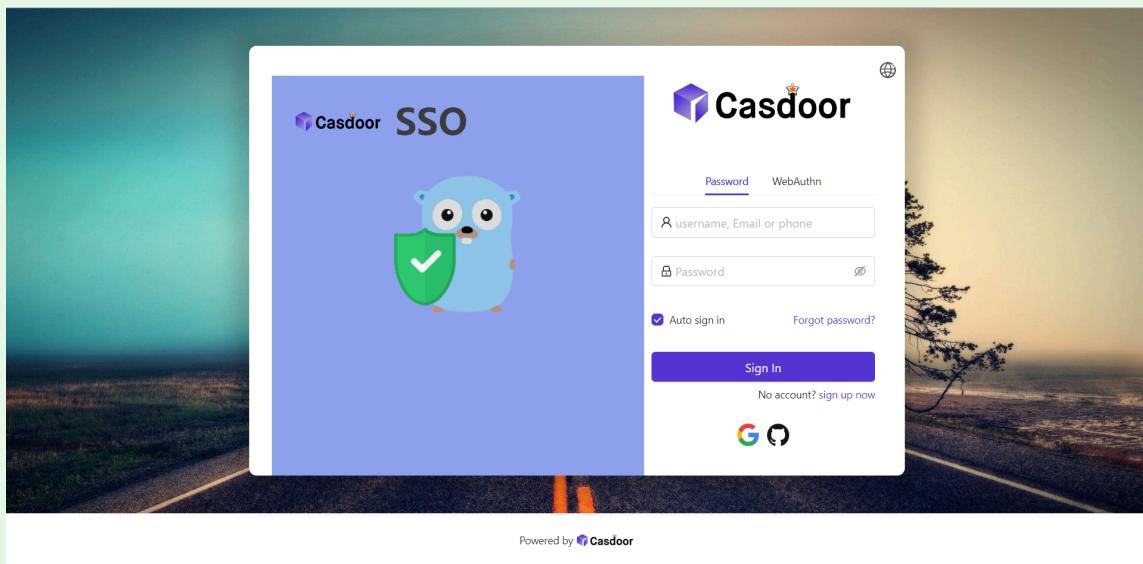
首先选择按钮。在 **启用侧边面板** 模式时，面板会在中间位置。



然后编辑 **侧边板 HTML**，它决定了将显示在侧边板中的内容。我们提供了一个默认模板，所以您可以简单地复制并粘贴它。

```
<style>
  .left-model{
    text-align: center;
    padding: 30px;
    background-color: #8ca0ed;
    position: absolute;
    transform: none;
    width: 100%;
    height: 100%;
  }
  .side-logo{
    display: flex;
    align-items: center;
  }
  .side-logo span {
    font-family: Montserrat, sans-serif;
    font-weight: 900;
```

好，让我们看看效果。 显示带有标志和图像的侧面板，但结果不能令人满意。



为了改进外观，您需要在 `表单 CSS` 中修改和添加一些CSS。

Background URL
② : URL ② : <https://static.runoob.com/images/demo/demo2.jpg>

Preview:

Form CSS ② : `<style> .login-panel{ padding: 40px 30px 0 30px; border-radius: 10px; background-color: #ffffff; box-shadow: 0 0 30px 20px rg`

Form position ② : [Left](#) [Center](#) [Right](#) [Enable side panel](#)

Side panel HTML ② : `<style> .left-model{ text-align: center; padding: 30px; background-color: #8ca0ed; position: absolute; left: -30px; top: 0; width: 30px; height: 100%; }`

Signup items ② : [Signup items](#) [Add](#)

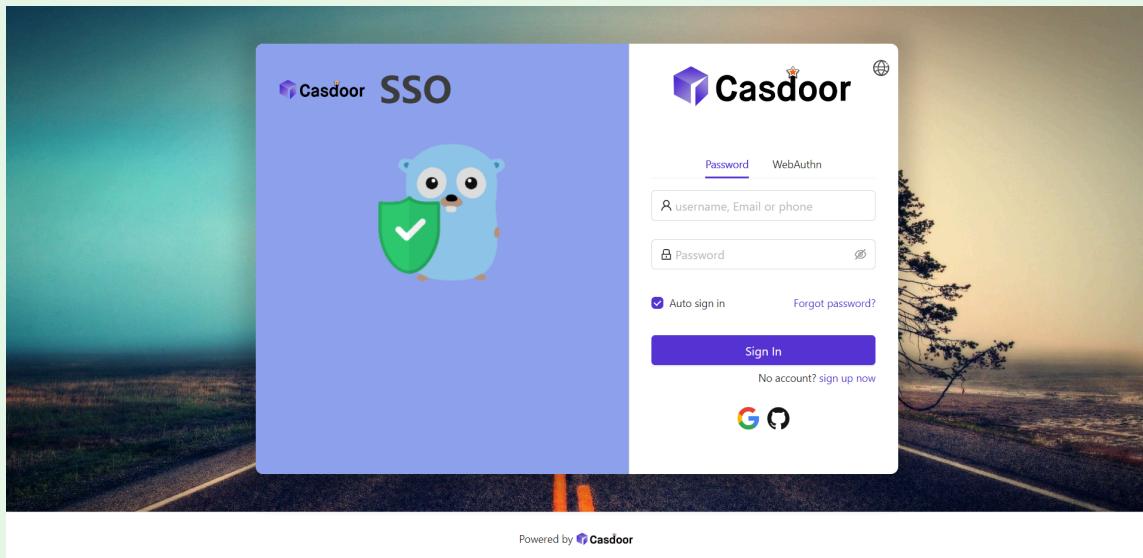
最后代码如下。

```
<style>
.login-panel{
```

① 信息

`.login-panel` 和 `.login-form` 是div的类名。它们对应于页面的不同区域。如果你想要进一步自定义登录页面，你可以在这里写CSS代码，目标是这些类名称。

最后，我们有了一个美丽的登录页面！



总结

我们来总结一下：我们已添加背景图像，自定义了登录面板的风格，并且启用了侧边板。

下面是一些关于定制Casdoor应用程序的额外资源：

- [自定义主题](#): 自定义主题，包括主颜色和边框半径。
- [注册项目表](#)
- [应用程序配置](#)

感谢你的阅读！

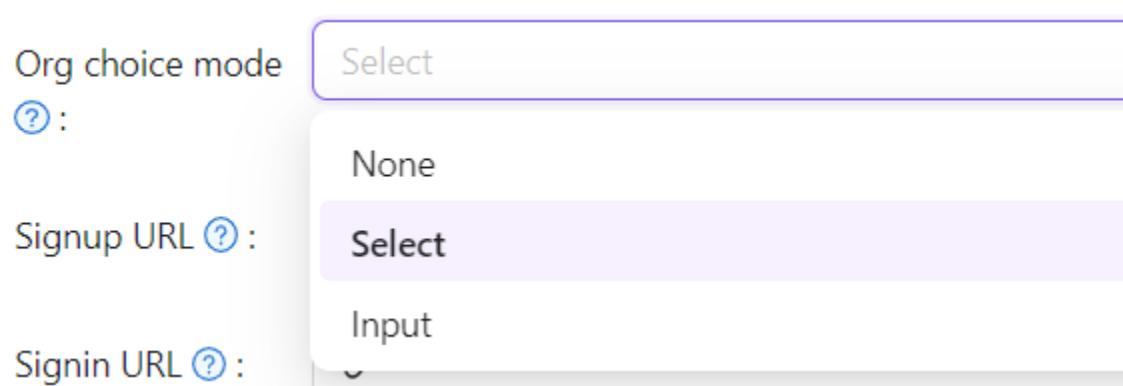
指定登录组织

在这里，我们将向您展示如何启用为应用指定登录组织的选项。

例如，端点 /login 是属于**内置组织**的账户的默认登录页面。然而，您可以在属于**内置组织**的**app-built-in**应用上启用指定登录组织的选项。这允许用户在登录时选择一个组织。用户选择组织后，他们将被重定向到 /login/<organization>。

配置

在应用编辑页面上，您可以找到 org select mode 配置选项。您可以从下拉列表中选择模式。



- 无：不会显示组织选择页面。
- 输入：用户可以在输入框中输入组织名称。
- 选择：用户可以从下拉列表中选择组织。



Please type an organization to sign in

built-in

Confirm



Please select an organization to sign
in

|



built-in

forum

test

Star

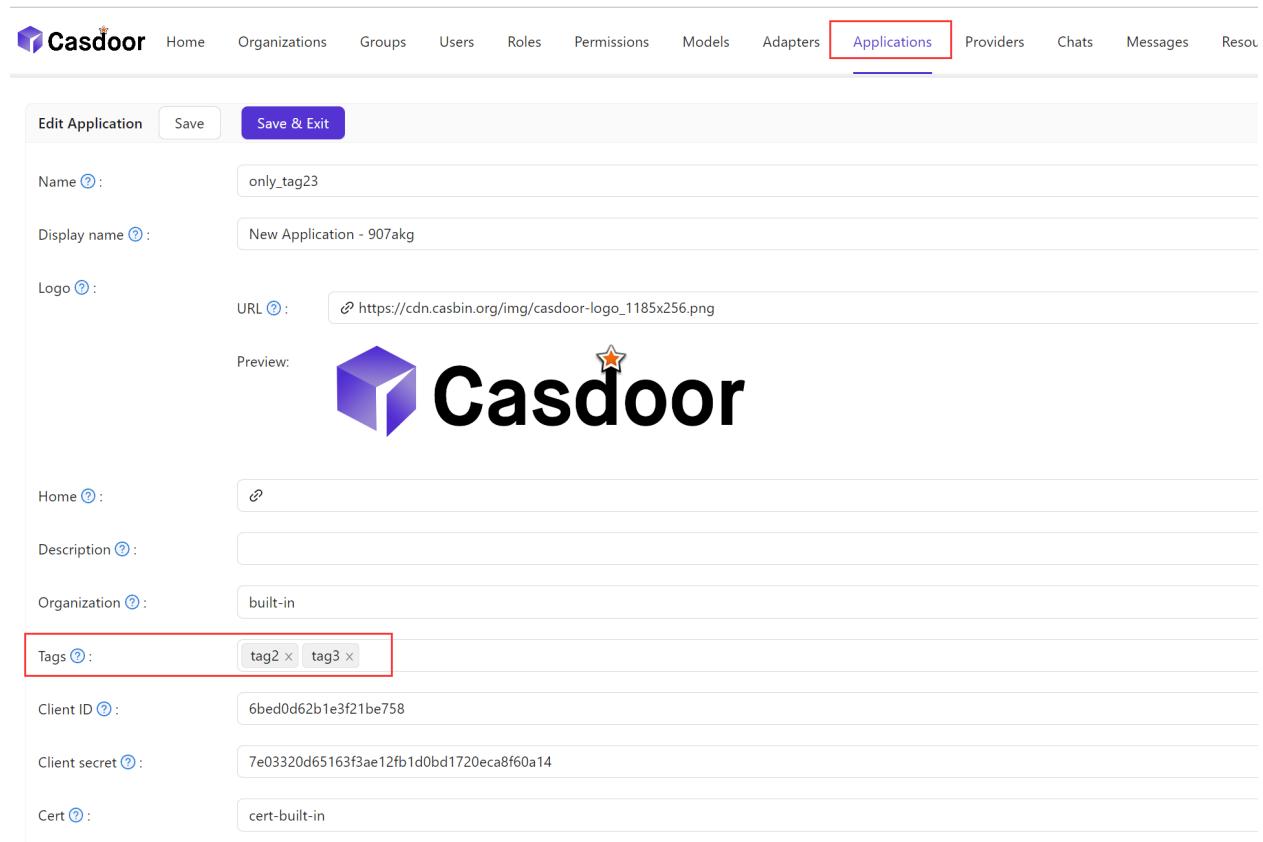
① 信息

The organization select page will only be shown when the route is `/login` or `<organization>/login`. 这意味着应用应该在组织或app-built-in中设置为默认应用。

标签

应用程序标签用于限制用户访问应用程序。具体来说，只有在应用程序标签中列出的标签的用户才被允许登录。例如，应用程序 dev_app 有标签 dev, prd。只有带有标签 dev 或 prd 的用户才能登录 dev_app。请注意，管理员和全局管理员用户不受应用程序标签的影响。

在应用程序编辑页面上，您可以找到 Tags 配置部分，您可以在那里添加标签。



The screenshot shows the Casdoor application configuration interface. The top navigation bar includes Home, Organizations, Groups, Users, Roles, Permissions, Models, Adapters, Applications (which is highlighted with a red box), Providers, Chats, Messages, and Resources. Below the navigation is a form for editing an application. The form fields include:

- Name: only_tag23
- Display name: New Application - 907akg
- Logo URL: https://cdn.casbin.org/img/casdoor-logo_1185x256.png
- Preview: Shows the Casdoor logo with a star icon.
- Home URL: (empty)
- Description: (empty)
- Organization: built-in
- Tags: tag2 x, tag3 x (highlighted with a red box)
- Client ID: 6bed0d62b1e3f21be758
- Client secret: 7e03320d65163f3ae12fb1d0bd1720eca8f60a14
- Cert: cert-built-in

这是一个演示应用程序标签如何工作的视频：

应用邀请码

简介

如果你想要限制用户通过应用注册，你可以使用邀请码。邀请码是能够用来允许用户通过应用注册的字符串。它由管理员生成并可重复使用。一个应用可以有多个邀请码。

配置

- 首先，将“邀请码”添加到应用的注册项中。
- 然后在应用的设置界面添加邀请码。

The screenshot shows the 'Signup items' configuration screen. At the top, there is a 'Signup items' section with a 'Add' button. Below it is a table with columns: Name, Visible, Required, Prompted, Rule, and Action. A new row has been added for 'Invitation code'. The 'Visible' and 'Required' checkboxes for this row are checked. A red box highlights this row. At the bottom of the table, there is an 'Add' button and a 'Copy' and 'Delete' button.

提示

Once the application has invitation codes, users can only sign up for the application with a valid invitation code. 无论“邀请码”在注册项中是否可见，用户都必须在注册时提供邀请码。因此，如果您想要使用邀请码，您需要将“邀请

码"添加到注册项表中。

以下是一个演示如何配置和使用邀请码的视频：

The screenshot shows a web-based configuration interface for a signup form. At the top, the URL is `localhost:7001/applications/built-in/app-built-in`. Below the header, there are two main sections: "Signup items" and "Invitation code".

Signup items: This section contains a table with columns: Name, Visible, Required, Prompted, Rule, and Action. The rows represent various fields:

Name	Visible	Required	Prompted	Rule	Action
ID	On	On	Off	Random	[Up/Down]
Username	On	On	Off	None	[Up/Down]
Display name	Off	Off	Off	None	[Up/Down]
Password	On	On	Off	Normal	[Up/Down]
ID card	Off	Off	Off	None	[Up/Down]
Email	Off	Off	Off	Normal	[Up/Down]
Phone	Off	Off	Off	None	[Up/Down]
Affiliation	Off	Off	Off	None	[Up/Down]
Country/Region	Off	Off	Off	None	[Up/Down]

Invitation code: This section has an "Add" button and a "No data" message.

Shared Application

Introduction

If you want to create an application that can be shared with other organizations, you can enable Is Shared field in application(for safety reasons, only built-in organization can create shared application). To specify the organization, you should add -org- and organization name after clientId / application name. For example, the clientId of application is `2dc94ccbec09612c04ac`, your organization name is `casbin`, the clientId for your organization is `2dc94ccbec09612c04ac-org-casbin` and the login url for oauth is `https://door.casdoor.com/login/oauth/authorize?client_id=2dc94ccbec09612c04ac-org-casbin&response_type=code&redirect_uri=http://localhost:9000&scope=read&state=casdoor`.

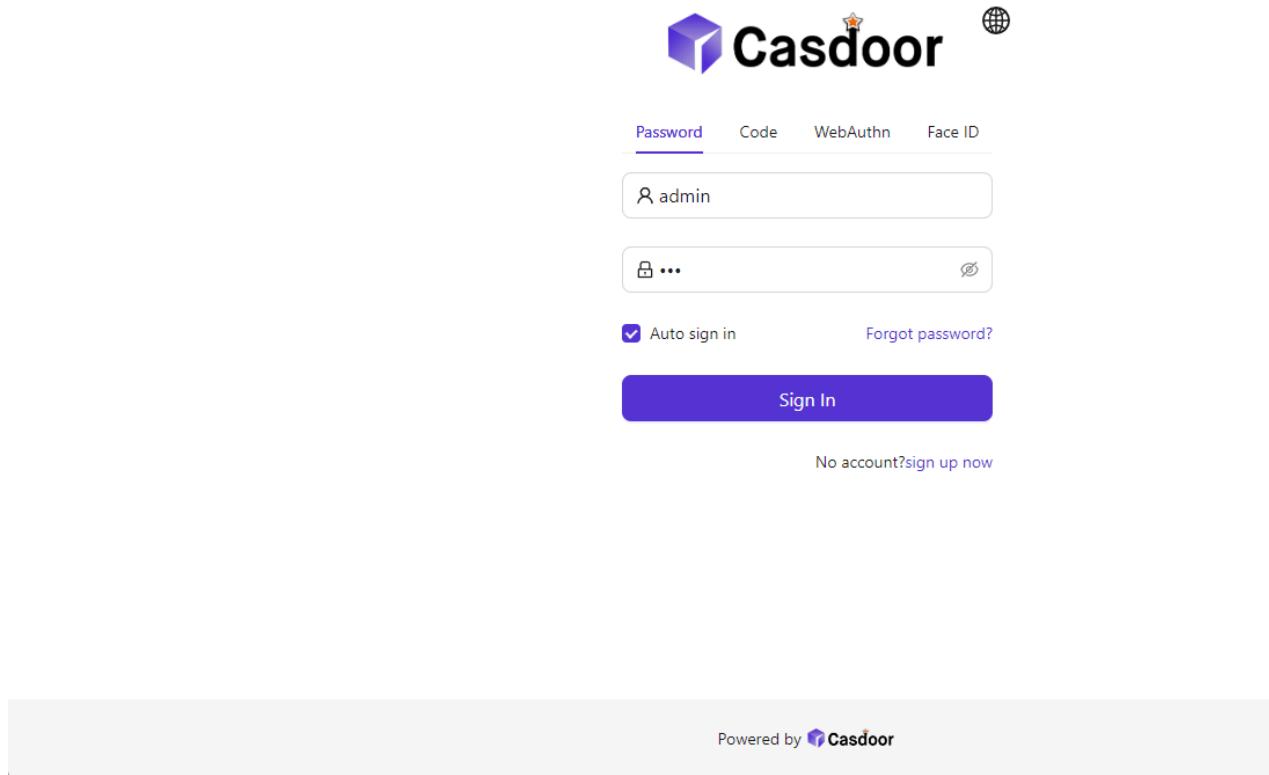
Configuration

1. First create a new application.
2. Enable Is Shared field.
3. add `-org-` to split organization and clientId / application name.

The screenshot shows the Casdoor application configuration interface. At the top, there is a navigation bar with links: Home, SaaS Hosting (highlighted in purple), User Management, Identity, Authorization, and Logging & Auditing. Below the navigation bar, there is a form titled "New Application". The form has the following fields:

- Name: application_f4gtqp
- Display name: New Application - f4gtqp
- Is shared: A toggle switch that is turned on (blue).
- Logo: URL: https://cdn.casbin.org/img/casdoor-logo_1185x256.png. It includes a preview image of the Casdoor logo, which features a purple geometric shape and the word "Casdoor" with a yellow star above the letter "o".

At the bottom of the form, there are "Save" and "Save & Exit" buttons.



注意事项

Once you shared an application, it can be used by all organizations, and cannot be disabled for a particular organization.

Here is a demo video that shows how to use shared application:



>

权限

权限

概述

在组织中使用Casbin管理用户访问权限

权限配置

使用公开的Casbin API来管理组织中用户的访问权限

开放的 Casbin API

使用公开的Casbin API来管理组织中的用户访问权限

适配器

配置适配器并对策略进行基本的增删改查操作

概述

Introduction

All users associated with a single [Casdoor organization](#) share access to the organization's applications. 然而，可能会有一些情况，你希望限制用户访问某些应用程序或应用程序内的特定资源。在这种情况下，您可以利用[Casbin](#)提供的[Permission](#)功能。

Understanding Casbin Concepts

Before delving deeper into the topic, it is important to have a basic understanding of how [Casbin](#) works and its related concepts:

- **Model:** Defines the structure of your permission policies and the criteria for matching requests against these policies and their outcomes. You can configure models in the [Models](#) page in Casdoor.
- **Policy:** Describes the specific permission rules (who can access what resources with what actions). You configure policies in the [Permissions](#) page in Casdoor.
- **Adapter:** An abstraction layer that shields Casbin's executor from the source of the Policy, allowing the storage of Policies in various locations like files or databases. Learn more about [Adapters](#).



Learn More About Casbin

Visit the [Casbin documentation](#) to learn more about access control models and patterns. You can also use the [Casbin Online Editor](#) to create and test Model and Policy files for your specific scenarios.

Configuring Permissions in Casdoor

Where to Configure

In the Casdoor Web UI, you'll work with two main pages:

1. **Models Page:** Navigate to Models in the sidebar to add or edit Models for your organization.

The screenshot shows the Casdoor Web UI with the 'Models' tab selected in the sidebar. The main area is titled 'Edit Model' and contains the following fields:

- Organization: built-in
- Name: model-built-in
- Display name: Built-in Model
- Model text:

```
[request_definition]
r = sub, obj, act

[policy_definition]
p = sub, obj, act

[policy_effect]
e = somewhere(p.eft == allow)

[matchers]
m = r.sub == p.sub && r.obj == p.obj && r.act == p.act
```
- Is enabled:

At the bottom are 'Save' and 'Save & Exit' buttons.

2. **Permissions Page:** Navigate to Permissions in the sidebar to configure permission policies.

The screenshot shows the 'Edit Permission' page in the Casdoor Web UI. The 'Permissions' tab is selected in the navigation bar. The main form has the following configuration:

- Organization: built-in
- Name: permission-built-in
- Display name: Built-in Permission
- Model: model-built-in
- Adapter: permission_rule_builtin
- Sub users: built-in/admin, built-in/seriouszyx, built-in/test
- Sub roles: (empty)
- Sub domains: (empty)
- Resource type: Application
- Resources: app-built-in
- Actions: Read, Write, Admin
- Effect: Allow
- Is enabled: checked
- Submitter: (empty)
- Approver: (empty)

How Permissions Work

Returning to the subject of permission configuration in Casdoor:

1. **Add a Model:** First, create a Model for your organization in the Models page within the Casdoor Web UI.
2. **Configure a Policy:** Then, add a Policy (permission rules) for your organization in the Permissions page.

Casbin在线编辑器可以为您提供针对您特定使用场景定制的模型和策略文件。您可以轻松地通过其Web UI将Model文件导入到Casdoor中，供内置的Casbin使用。For the Policy configuration (i.e., the Permissions page in the Casdoor Web UI), refer to the [Permission Configuration](#) guide for detailed instructions.

Using Permissions with Your Application

就像你的应用程序需要通过Casdoor内置的Casbin来执行权限控制一样，Casdoor本身

也利用自己的模型和策略通过Casbin来规范API接口的访问权限。尽管Casdoor可以从内部代码调用Casbin，但外部应用程序无法这样做。

作为一种解决方案，Casdoor为外部应用程序提供了一个API，以调用内置的Casbin。

See the [Exposed Casbin APIs](#) documentation for definitions of these API interfaces and instructions on how to use them.

Related Features

Account Item Permissions

Casdoor also provides fine-grained permission control at the user account field level through the [Edit Organization](#) page:

- **View rule:** Control who can view specific user account fields
- **Modify rule:** Control who can modify specific user account fields

These rules can be set to:

- **Public:** Everyone has permission
- **Self:** Each user has their own permission
- **Admin:** Only administrators have permission

Learn more in the [Account Customization](#) documentation.

Role-Based Access Control

Casdoor supports role-based permissions where you can assign [roles](#) to users and configure permission policies for these roles. This allows you to manage permissions at the role level rather than individual user level.

Next Steps

- [Permission Configuration](#): Learn how to configure each field in the Permission page
- [Exposed Casbin APIs](#): Use Casbin APIs in your external applications
- [Adapters](#): Configure adapters for policy storage
- [Account Customization](#): Configure field-level permissions for user accounts

让我们开始吧！

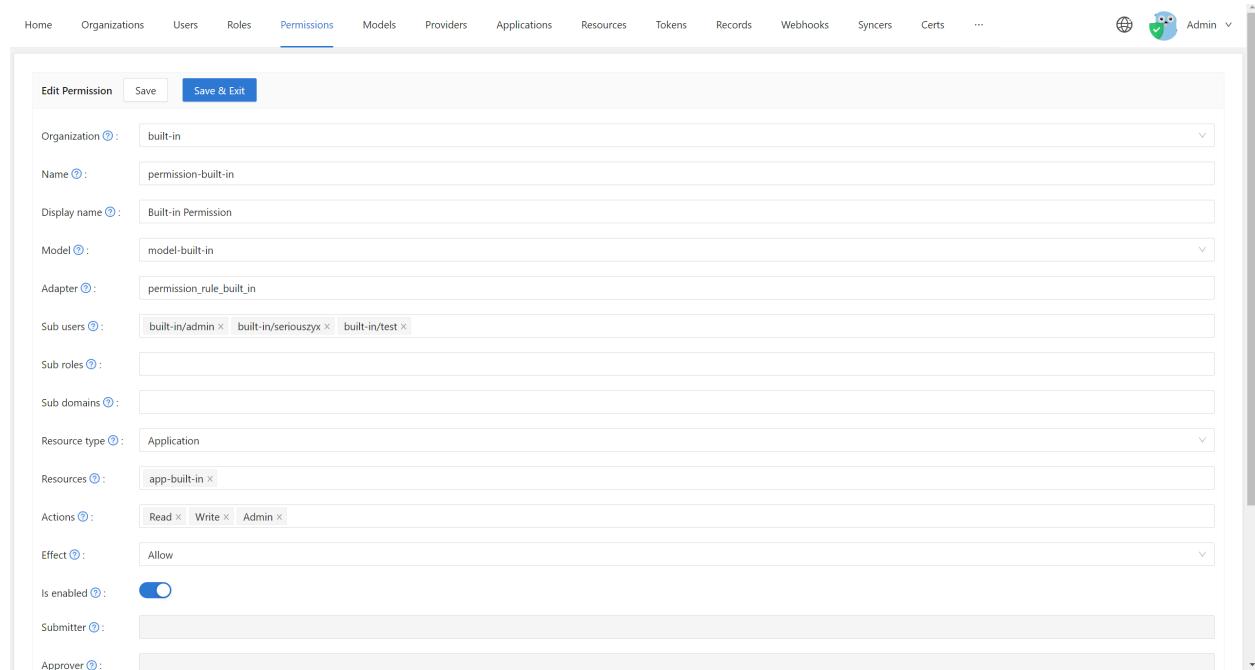
权限配置

This page explains each field in the Edit Permission page where you configure permission policies for your [organization](#).

Accessing the Permission Configuration

To access the permission configuration page:

1. Log in to your Casdoor instance
2. Navigate to **Permissions** in the sidebar
3. Click **Add** to create a new permission or click on an existing permission to edit it



The screenshot shows the 'Edit Permission' configuration page. At the top, there are buttons for 'Edit Permission', 'Save', and 'Save & Exit'. Below these are various input fields and dropdown menus for configuring a permission rule. The fields include:

- Organization: built-in
- Name: permission-built-in
- Display name: Built-in Permission
- Model: model-built-in
- Adapter: permission_rule_builtin
- Sub users: built-in/admin, built-in/seriouszyx, built-in/test
- Sub roles: (empty)
- Sub domains: (empty)
- Resource type: Application
- Resources: app-built-in
- Actions: Read, Write, Admin
- Effect: Allow
- Is enabled:
- Submitter: (empty)
- Approver: (empty)

On the right side of the header, there are icons for globe, shield, and user, followed by the text 'Admin' and a dropdown arrow.

Configuration Fields

Basic Information

Organization

The name of the [organization](#) to which the policy belongs. 一个组织可以拥有多个权限策略文件。 You can select the organization from the dropdown menu in the [Edit Permission](#) page.

Name

The globally unique name of the permission policy in the organization. 它用于识别策略文件。

- Must be unique within the organization
- Used as the identifier when calling [Casbin APIs](#)

Display name

A user-friendly name for the permission policy. This is shown in the Casdoor Web UI for better readability.

Model and Storage Configuration

Model

The name of the model file that describes the structure and matching patterns of the permission policy. You can configure models in the [Edit Model](#) page.

Models define how permission checks are performed. For example:

- Simple ACL (Access Control List)
- RBAC (Role-Based Access Control)
- ABAC (Attribute-Based Access Control)

Learn more about models in the [Casbin documentation](#).



提示

Use the [Casbin Online Editor](#) to create and test your model before adding it to Casdoor.

Adapter

Attention! In the current version, this field describes the name of the database table that stores the permission policy, rather than the name of the adapter configured in the [Adapters](#) page in the Casdoor Web UI.

Casdoor uses its own database to store configured permission policies:

- If this field is empty, the permission policy will be stored in the `permission_rule` table
- If specified, it will be stored in the specified database table
- If the specified table name does not exist in the database used by Casdoor, it will be created automatically



注意事项

Important

We strongly recommend specifying different adapters (table names) for different models, as keeping all policies in the same table may cause conflicts.

Learn more about adapters in the [Adapter documentation](#).

Subject Configuration

These fields define who the permission policy applies to.

Sub users

Which **users** will the permission policy be applied to. You can select specific users from the [Edit Permission](#) page.

Examples:

- Select specific users like `alice`, `bob`
- Leave empty to not restrict by user

Sub roles

If the RBAC (Role-Based Access Control) model is used, you can select which **roles** will be applied to the permission policy. You configure roles in the [Edit Role](#) page.

This will add permission policies such as `g, user, role` for every user in this role.

Examples:

- Select roles like `admin`, `editor`, `viewer`
- All users with these roles will inherit the permissions



Role-Based Permissions

Using roles is a powerful way to manage permissions at scale. Instead of assigning permissions to individual users, you assign them to roles, and then assign roles to users.

Sub domains

Which domains will the permission policy be applied to. This is useful for multi-tenant scenarios.

Examples:

- `domain1`, `domain2`
- Leave empty if not using domain-based access control

Object and Action Configuration

These fields define **what** resources and **what actions** are controlled by the policy.

Resource type

In the current version, Casdoor does not use this field for external applications that want to authenticate. You can ignore it for now or use it for your own categorization purposes.

Resources

This field describes the resources for which you wish to enforce permission control.

 备注

Note that the resources here are not those configured in the Resources page of the Casdoor Web UI. You can add any string you want here, such as:

- A URL: `/api/users`, `/admin/dashboard`
- A file name: `document.pdf`, `config.yaml`
- A resource identifier: `project:123`, `database:users`

You can add multiple resources, and Casdoor will create permission rules for each combination of resource and action.

Actions

This field describes the actions to operate on resources. Similar to resources, it can be any string you want, such as:

- HTTP methods: `GET`, `POST`, `PUT`, `DELETE`
- CRUD operations: `read`, `write`, `update`, `delete`
- Custom actions: `view`, `edit`, `approve`, `publish`

⚠ 注意事项

Please note that Casdoor will convert all these strings to lowercase before storing them. Additionally, Casdoor will apply all actions to each resource. You cannot specify that an action only takes effect on certain resources in this configuration page.

If you need fine-grained control over action-resource combinations, you should define this in your Model file.

Effect Configuration

Effect

This option takes effect for Casdoor itself to control application access.

① 信息

If you want an external application to enforce permission controls using the interface Casdoor exposes, this field won't do anything. You should describe the effect of pattern matching in the Model file using `allow` or `deny` rules.

Example Configuration

As you can see, this configuration page is almost tailor-made for the `(sub, obj, act)` model, which is one of the most common permission models.

Here's an example configuration:

- Model: `rbac_model` (Role-Based Access Control)
- Sub roles: `admin`, `editor`
- Resources: `/api/users`, `/api/posts`
- Actions: `read`, `write`

This would allow users with the `admin` or `editor` role to perform `read` and `write` actions on the `/api/users` and `/api/posts` resources.

Related Topics

- [Permission Overview](#): Understand the basics of permissions in Casdoor
- [Exposed Casbin APIs](#): Use permissions in your external applications
- [Adapters](#): Configure policy storage adapters
- [Account Customization](#): Configure View rule and Modify rule for user account fields
- [User Roles](#): Manage user roles in the Edit Role page

开放的 Casbin API

介绍

假设你的应用程序的前端已经获取了已登录用户的 `access_token`，现在想要对用户进行一些访问的认证。你不能简单地将 `access_token` 放入HTTP请求头来使用这些API，因为Casdoor使用 `Authorization` 字段来检查访问权限。像Casdoor提供的其他API一样，`Authorization` 字段由应用客户端id和密钥组成，使用 [基本的HTTP认证方案](#)。它看起来像 `Authorization: Basic <Your_Application_ClientId><Your_Application_ClientSecret>`。因此，Casbin API 应当被应用的后端服务器调用。以下是如何操作的步骤。

以演示站点中的[app-vue-python-example](#)应用为例，授权头应该是：

```
Authorization: Basic 294b09fbc17f95daf2fe  
dd8982f7046ccba1bbd7851d5c1ece4e52bf039d。
```

1. 前端通过HTTP请求头将 `access_token` 传递给后端服务器。
2. 后端服务器从 `access_token` 中检索用户id。

提前说明，这些接口也是为 `(sub, obj, act)` 模型设计的（目前）。正文是由Casbin模型定义的权限请求格式，通常分别代表 `sub`、`obj` 和 `act`。

除了请求强制执行权限控制的 API 接口以外，Casdoor 也提供了其它一些有助于外部应用获取权限策略信息的接口，也一并列在此处。

Enforce

The Enforce API supports multiple query parameters to specify which permission(s) to enforce against. Only one parameter should be provided at a

time:

- `permissionId`: The identity of a specific permission policy (format: `organization name/permission name`)
- `modelId`: The identity of a permission model (format: `organization name/model name`) - enforces against all permissions using this model
- `resourceId`: The identity of a resource - enforces against all permissions for this resource
- `enforcerId`: The identity of a specific enforcer
- `owner`: The organization name - enforces against all permissions in this organization

Request using `permissionId`:

```
curl --location --request POST 'http://localhost:8000/api/enforce?permissionId=example-org/example-permission' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic <Your_Application_ClientId><Your_Application_ClientSecret>' \
--data-raw '["example-org/example-user", "example-resource", "example-action"]'
```

Request using `modelId`:

```
curl --location --request POST 'http://localhost:8000/api/enforce?modelId=example-org/example-model' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic <Your_Application_ClientId><Your_Application_ClientSecret>' \
--data-raw '["example-org/example-user", "example-resource", "example-action"]'
```

Request using `resourceId`:

```
curl --location --request POST 'http://localhost:8000/api/enforce?resourceId=example-org/example-resource' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic <Your_Application_ClientId><Your_Application_ClientSecret>' \
--data-raw '[{"example-org/example-user", "example-resource", "example-action"}'
```

Response:

```
{
  "status": "ok",
  "msg": "",
  "sub": "",
  "name": "",
  "data": [
    true
  ],
  "data2": [
    "example-org/example-model/example-adapter"
  ]
}
```

Note: When using `modelId`, `resourceId`, `enforcerId`, or `owner` parameters, the response `data` array may contain multiple boolean values (one for each permission that was checked), and `data2` contains the corresponding model and adapter identifiers.

BatchEnforce

The BatchEnforce API supports multiple query parameters to specify which

permission(s) to enforce against. Only one parameter should be provided at a time:

- `permissionId`: The identity of a specific permission policy (format: organization name/permission name)
- `modelId`: The identity of a permission model (format: organization name/model name) - enforces against all permissions using this model
- `enforcerId`: The identity of a specific enforcer
- `owner`: The organization name - enforces against all permissions in this organization

Request using `permissionId`:

```
curl --location --request POST 'http://localhost:8000/api/batch-enforce?permissionId=example-org/example-permission' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>' \
--data-raw '[[{"example-org/example-user", "example-resource",
"example-action"}, ["example-org/example-user2", "example-
resource", "example-action"], ["example-org/example-user3",
"example-resource", "example-action"]]
```

Request using `modelId`:

```
curl --location --request POST 'http://localhost:8000/api/batch-enforce?modelId=example-org/example-model' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>' \
--data-raw '[[{"example-org/example-user", "example-resource",
"example-action"}, ["example-org/example-user2", "example-
resource", "example-action"]]]'
```

响应:

```
{  
    "status": "ok",  
    "msg": "",  
    "sub": "",  
    "name": "",  
    "data": [  
        [  
            true,  
            true,  
            false  
        ]  
    ],  
    "data2": [  
        "example-org/example-model/example-adapter"  
    ]  
}
```

Note: When using `modelId`, `enforcerId`, or `owner` parameters, the response `data` array may contain multiple arrays of boolean values (one array for each permission that was checked), and `data2` contains the corresponding model and adapter identifiers.

GetAllObjects

This API retrieves all objects (resources) that a user has access to. It accepts an optional `userId` parameter. If not provided, it uses the logged-in user's session.

Request with `userId` parameter:

```
curl --location --request GET 'http://localhost:8000/api/get-all-objects?userId=example-org/example-user' \
```

Request using session (userId determined from session):

```
curl --location --request GET 'http://localhost:8000/api/get-all-objects' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

响应:

```
{
  "status": "ok",
  "msg": "",
  "data": [
    "app-built-in",
    "example-resource"
  ]
}
```

GetAllActions

This API retrieves all actions that a user can perform. It accepts an optional `userId` parameter. If not provided, it uses the logged-in user's session.

Request with `userId` parameter:

```
curl --location --request GET 'http://localhost:8000/api/get-all-actions?userId=example-org/example-user' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

Request using session (userId determined from session):

```
curl --location --request GET 'http://localhost:8000/api/get-all-actions' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

响应:

```
{  
    "status": "ok",  
    "msg": "",  
    "data": [  
        "read",  
        "write",  
        "admin"  
    ]  
}
```

GetAllRoles

This API retrieves all roles assigned to a user. It accepts an optional `userId` parameter. If not provided, it uses the logged-in user's session.

Request with `userId` parameter:

```
curl --location --request GET 'http://localhost:8000/api/get-all-roles?userId=example-org/example-user' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

Request using session (userId determined from session):

```
curl --location --request GET 'http://localhost:8000/api/get-all-roles' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

响应：

```
{  
  "status": "ok",  
  "msg": "",  
  "data": [  
    "role_kcx66l"  
  ]  
}
```

RunCasbinCommand

This API executes Casbin CLI commands and returns their output. It's designed for running language-specific Casbin command-line tools through Casdoor's backend, supporting languages like Java, Go, Node.js, Python, and others.

The API includes an in-memory cache that stores command results for 5 minutes. When the same command is executed with identical parameters, the cached result is returned immediately without re-executing the command, improving response times and reducing server load.

Request:

```
curl --location --request GET 'http://localhost:8000/api/run-casbin-command?language=go&args=["-v"]' \
--header 'Authorization: Basic <Your_Application_ClientId>
<Your_Application_ClientSecret>'
```

Parameters:

- `language`: The programming language for the Casbin CLI (e.g., `go`, `java`, `node`, `python`)
- `args`: A JSON-encoded array of command-line arguments (e.g., `["-v"]` for version, `["new"]` for creating new files). Note: URL-encode the JSON array when using it as a query parameter

Response:

```
{  
  "status": "ok",  
  "msg": "",  
  "data": "casbin version 2.x.x"  
}
```

The cache key is generated from the language and arguments, so different commands are cached independently. Expired entries are automatically cleaned up to prevent memory growth.

适配器

Casdoor支持使用UI连接适配器并管理策略规则。在Casbin中，策略规则的存储是作为一个适配器实现的，它充当Casbin的中间件。Casbin用户可以使用适配器从存储中加载策略规则或将策略规则保存到存储中。

适配器

- **类型**：适配器类型。目前支持数据库适配器。
- **主机**
- **端口**
- **用户**
- **密码**
- **数据库类型**：目前支持MySQL, PostgreSQL, SQL Server, Oracle, SQLite 3。
- **数据库**：数据库的名称。
- **表**：表的名称。如果表不存在，将会被创建。

Edit Adapter Save Save & Exit

Organization ② :	built-in
Name ② :	casdoor_adapter
Type ② :	Database
Host ② :	localhost
Port ② :	3306
User ② :	root
Password ② :	123456
Database type ② :	MySQL
Database ② :	casdoor
Table ② :	casbin_rule

① 信息

填写完所有字段后，请记得**保存配置**。然后点击**同步**按钮来加载策略规则。策略规则将显示在下面的表格中。

Policies ② : Sync Add

Rule Type	V0	V1	V2	V3	V4	V5	Option
p	built-in	*	*	*	*	*	
p	app	*	*	*	*	*	
p	*	*	POST	/api/signup	*	*	
p	*	*	POST	/api/get-email-and-phone	*	*	
p	*	*	POST	/api/login	*	*	
p	*	*	GET	/api/get-app-login	*	*	
p	*	*	POST	/api/logout	*	*	
p	*	*	GET	/api/logout	*	*	
p	*	*	GET	/api/get-account	*	*	
p	*	*	GET	/api/userinfo	*	*	

< 1 2 3 4 5 >

Is enabled ② : Toggle Reset

基本的增删改查操作

如果您已成功连接适配器，您可以对策略规则进行基本的增删改查操作。

- 添加

Policies ⓘ: Sync Add

Rule Type	V0	V1	V2	V3	V4	V5	Option
p	built-in	*	*	/api/signup	*	*	
p	*	*	POST	/api/get-email-and-phone	*	*	
p	*	*	POST	/api/login	*	*	
p	*	*	GET	/api/get-app-login	*	*	
p	*	*	POST	/api/logout	*	*	
p	*	*	GET	/api/logout	*	*	
p	*	*	GET	/api/get-account	*	*	
p	*	*	GET	/api/userinfo	*	*	
p	*	*	POST	/api/webhook	*	*	

< 1 2 3 4 5 >

提示

您一次只能添加一条策略。 新添加的策略将作为表格中的第一行出现，但实际上将保存在最后一行。 所以，当你下次同步策略时，它们将出现在表格的最后一行。

- 编辑

Table ⓘ: casbin_rule

Model ⓘ: casbin_rule

Policies ⓘ: Sync Add

Rule Type	V0	V1	V2	V3	V4	V5	Option
p	built-in	*	POST	*	*	*	
p	app	*	*	*	*	*	
p	*	*	POST	/api/signup	*	*	
p	*	*	POST	/api/get-email-and-phone	*	*	
p	*	*	POST	/api/login	*	*	
p	*	*	GET	/api/get-app-login	*	*	
p	*	*	POST	/api/logout	*	*	
p	*	*	GET	/api/logout	*	*	
p	*	*	GET	/api/get-account	*	*	
p	*	*	GET	/api/userinfo	*	*	

< 1 2 3 4 5 >

- 删除

User [?](#):

Password [?](#):

Database type [?](#): MySQL

Database [?](#): casdoor

Table [?](#): casbin_rule

Model [?](#): casbin_rule

Policies [?](#): Sync Add

Rule Type	V0	V1	V2	V3	V4	V5	Option
p	*	*	GET	/api/get-default-application	*	*	
p	test	*	*	*	*	*	

< 1 2 3 4 5 >



>

提供商

提供商

概述

添加第三方服务到您的应用程序

OAuth

24 个项目

电子邮箱

6 个项目

短信

5 个项目



通知

8 个项目



存储

9 个项目



SAML

4 个项目



支付

6 个项目



验证码

7 个项目



Web3

2 个项目



Face ID

2 个项目



MFA

2 个项目

概述

Casdoor 利用提供商为平台提供第三方服务。 在本章中，您将学习如何向Casdoor添加提供商。

我们拥有的

Currently, we have seven types of providers:

- **OAuth 提供商**

允许用户通过其他 OAuth 应用程序登录。 您可以将GitHub, Google, QQ等许多其他OAuth应用程序添加到Casdoor。 有关更多详细信息，请参阅[OAuth](#)部分。

- **短信提供商**

当用户想要验证他们的电话号码时，Casdoor将发送短信给他们。 短信提供者被用来发送Casdoor短信。

- **电子邮件提供商**

电子邮件提供者与短信提供者类似。

- **存储提供商**

Casdoor允许用户使用本地文件系统或云OSS服务存储文件。

- **支付提供商**

Casdoor 可以添加付款提供者，用于在产品页面上添加付款方法。 目前，支持的支

付提供商包括支付宝，微信支付，PayPal和GC。

- **验证码提供商**

Casdoor支持在用户流程中配置验证码。目前，支持的验证码提供商包括默认验证码，reCAPTCHA，hCaptcha，阿里巴巴云验证码，以及Cloudflare Turnstile。

- **MFA Providers**

Casdoor supports external authentication servers for multi-factor authentication. Currently supports RADIUS servers for authenticating users as a second factor during login.

如何配置和使用

范围

提供者有不同的范围，这由创建者决定。只有管理员有权限添加和配置提供商。

Casdoor中有两种类型的管理员：

- **全球管理员：**所有在 `built-in` 组织下的用户以及启用 `IsGlobalAdmin` 的用户。由全局管理员创建的提供者可以被所有应用程序使用。
- **组织管理员：**启用 `IsAdmin` 的用户。由组织管理员创建的提供者只能被该组织下的应用程序使用（正在开发中...）。

添加到应用程序

按照以下步骤将提供者添加到您的应用程序中。请注意，除非您已添加它，否则您不能在应用程序中使用该提供者。

1. 转到应用程序编辑页面并添加一个新的提供商。

Providers :

Name	Category	Type
provider_storage_aliyun_oss	Storage	
provider_casdoor_github	OAuth	
provider_casdoor_google	OAuth	
provider_casdoor_qq	OAuth	
provider_casdoor_wechat	OAuth	
Please select a provider		

2. 选择您想要添加到应用程序的提供商。您将看到应用程序可以使用的所有提供商。

Providers :

Name	Category	Type	canSignUp
provider_storage_aliyun_oss	Storage		
provider_casdoor_github	OAuth		<input checked="" type="checkbox"/>
provider_casdoor_google	OAuth		<input checked="" type="checkbox"/>
provider_casdoor_qq	OAuth		<input checked="" type="checkbox"/>
provider_casdoor_wechat	OAuth		<input checked="" type="checkbox"/>
Please select a provider			

Preview :

- provider_email_submail
- provider_4olfdm
- provider_casdoor_bilibili
- provider_casdoor_okta
- provider_casdoor_alipay
- provider_casdoor_slack
- provider_casdoor_steam
- provider_casdoor_infoflow

3. 对于OAuth和Captcha提供商，您可以配置它们的使用方式。请参阅 [OAuth](#) 和 [验证码](#) 以获取更多信息。

Type	canSignUp	canSignIn	canUnlink	prompted	Rule
					Always ▾
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

最后，**保存配置**。您现在可以尝试在您的应用程序中使用该提供程序。

OAuth

概述

将 OAuth 提供商添加到您的应用程序

User Mapping

Map OAuth provider claims to Casdoor user fields

谷歌

将Google OAuth提供商添加到您的应用程序

Google One Tap

学习如何在您的应用程序中添加Google One Tap支持

 GitHub

将GitHub OAuth提供商添加到您的应用程序

 LinkedIn

将LinkedIn OAuth提供商添加到您的应用程序

 Facebook

将Facebook OAuth提供商添加到您的应用程序中。

 Apple

Add the Apple Sign in OAuth provider to your application.

 AD FS

将AD FS添加为第三方服务以完成身份验证。

 **Azure AD**

将 Azure AD 添加为第三方服务以完成身份验证

 **Azure AD B2C**

将 Azure AD B2C 添加为第三方服务以完成身份验证

 **自定义OAuth**

将您的自定义OAuth提供商添加到Casdoor

 **Okta**

将 Octa OAuth 提供商添加到您的应用程序

 **Twitter**

添加Twitter OAuth 提供商到您的应用程序

 **微博**

将 Weibo OAuth 提供商添加到您的应用程序

 **微信**

将微信 OAuth 提供商添加到您的应用程序

 **企业微信**

将 WeCom OAuth 提供商添加到您的应用程序

 **腾讯 QQ**

添加腾讯QQ OAuth提供商到您的应用程序。

 **钉钉**

添加钉钉 OAuth 到您的应用程序

 Steam

将Steam OAuth提供商添加到您的应用程序中

 Gitee

添加Gitee OAuth 提供商到您的应用程序

 百度

向您的应用程序添加 Baidu OAuth 提供商

 Infoflow

在应用程序中添加 Infoflow OAuth 提供商

 Lark

将Lark OAuth提供商添加到您的应用程序

概述

Casdoor允许使用其他OAuth应用程序作为登录方法。

目前，Casdoor支持多个OAuth应用程序提供商。一旦这些提供商被添加到Casdoor中，它们的图标将会在登录和注册页面上显示。以下是Casdoor支持的提供商：

提供者	Logo	提供者	Logo	提供者	Logo	提供者	Logo
ADFS		支付宝		亚马逊		苹果	
Auth0		Azure AD		Azure AD B2C		百度	
Bilibili		Bitbucket		盒子		Casdoor	
Cloud Foundry		Dailymotion		Deezer		DigitalOcean	
钉钉		Discord		Tiktok		Dropbox	
Eve Online		Facebook		Fitbit		Gitea	
Gitee		GitHub		GitLab		Google	
Heroku		InfluxCloud		信息流		Instagram	

提供者	Logo	提供者	Logo	提供者	Logo	提供者	Logo
Intercom		Kakao		Lark		Lastfm	
线		LinkedIn		Mailru		Meetup	
微软		Naver		Nextcloud		Okta	
OneDrive		Oura		Patreon		PayPal	
QQ		Salesforce		Shopify		Slack	
SoundCloud		Spotify		Steam		Strava	
Stripe		TikTok		Tumblr		Twitch	
Twitter		TypeTalk		Uber		VK	
微信		WeCom		微博		WePay	
Xero		Yahoo		Yammer		Yandex	
Zoom		电子邮件		短信		Battle.net	

我们将向您展示如何申请第三方服务并将其添加到Casdoor。

申请成为开发者

在此之前，你需要理解一些概念。

- **RedirectUrl**, 认证后重定向地址, 填写您的应用程序地址, 例如 `https://forum.casbin.com/`
- **Scope**, 用户授予您的权限, 如基本个人资料, 电子邮件地址和帖子及其他。
- **ClientId/AppId, ClientKey/AppSecret**, 这是最重要的信息 而且这是您在申请开发者帐户后需要得到的信息。您无法与任何人共享 的密钥。

添加 OAuth 提供商

1. 前往您的Casdoor首页。
2. 点击顶部栏中的 `Providers`。
3. 点击 `Add`，您将会看到新的提供商被添加到顶部的列表中。
4. 点击新的提供商以对其进行更改。
5. 在 `Category` 部分中, 选择 `OAuth`。
6. 从 `Type` 下拉菜单中选择您需要的特定OAuth提供商。
7. 填写必要的信息, 例如 `Client ID` 和 `Client Secret`。

User Field Mapping

OAuth providers often return additional user information beyond the standard profile fields. Casdoor's `User Mapping` feature allows you to automatically populate user profile fields from OAuth claims returned by your identity provider. This is particularly useful when integrating with enterprise identity providers like Okta, Azure AD, or other custom OAuth services that provide rich user metadata.

Automatic Account Linking

When users authenticate via OAuth, Casdoor automatically attempts to link accounts using

multiple strategies: existing OAuth links, email/phone matching (if enabled), and case-insensitive username matching. This is particularly useful for enterprises with existing users who want to enable OAuth authentication without requiring manual account linking.

应用程序设置

1. 点击顶部栏中的 **Application**，然后选择要编辑的应用程序。
2. 点击提供商添加按钮，并选择新添加的提供商。
3. 修改提供商的权限，例如启用注册、登录和解绑。
4. 你已经准备好了！

User Mapping

When users sign in through OAuth providers, Casdoor automatically captures their basic profile information like username, email, and avatar. However, identity providers often return additional claims in their OAuth responses that contain valuable user data. The User Mapping feature allows you to map these extra claims to specific user profile fields in Casdoor.

Supported Fields

You can map OAuth provider claims to the following user fields:

- **phone** - Phone number
- **countryCode** - Country calling code
- **firstName** - First name
- **lastName** - Last name
- **region** - Geographic region
- **location** - Full location or address
- **affiliation** - Organization or company affiliation
- **title** - Job title or position
- **homepage** - Personal website URL
- **bio** - Biography or description
- **tag** - Custom tag or category
- **language** - Preferred language
- **gender** - Gender identity
- **birthday** - Date of birth

- `education` - Educational background
- `idCard` - ID card number
- `idCardType` - Type of ID card

Standard fields (`id`, `username`, `displayName`, `email`, `avatarUrl`) are handled automatically and don't need mapping configuration.

Configuration

To configure user mapping for an OAuth provider:

1. Navigate to **Providers** in the top menu
2. Select or create an OAuth provider (e.g., Okta, Azure AD B2C, Google)
3. Scroll to the **User mapping** section
4. Add mappings by specifying:
 - **User field:** The Casdoor user field you want to populate
 - **Claim name:** The exact claim name from your OAuth provider's response

For example, if your identity provider returns a claim named `given_name` and you want to map it to the user's first name in Casdoor:

- User field: `firstName`
- Claim name: `given_name`

Provider-Specific Examples

Okta

Okta returns claims like `given_name`, `family_name`, and `locale`. You might

configure:

- `firstName` → `given_name`
- `lastName` → `family_name`
- `language` → `locale`

Azure AD B2C

Azure AD B2C can return custom claims configured in your user flows. For instance:

- `phone` → `extension_PhoneNumber`
- `title` → `jobTitle`
- `location` → `city`

Generic OAuth Providers

Most OAuth providers following standard protocols return claims in their userinfo endpoint. Check your provider's documentation to find available claim names.

Behavior

The mapping works with these characteristics:

- **Non-destructive:** Existing user field values are preserved. Mapping only updates empty fields.
- **Automatic sync:** When users sign in via OAuth, the mapping is applied automatically.
- **Flexible:** Each provider can have its own unique mapping configuration.
- **Extra claims:** All claims from the provider are stored in the user's extra data,

even if not explicitly mapped.

Common Scenarios

Enterprise SSO

When integrating with enterprise identity providers like Okta or Azure AD, you often want to sync organizational data:

```
title → jobTitle  
affiliation → companyName  
region → officeLocation
```

Social Login Enhancement

Social providers like Google or Facebook provide basic profile data, but you can capture additional details:

```
location → location  
homepage → website  
bio → about_me
```

Multi-Provider Setup

Different providers may use different claim names for the same data. Configure each provider independently:

Google OAuth:

- `firstName` → `given_name`

- `lastName` → `family_name`

GitHub OAuth:

- `location` → `location`
- `homepage` → `blog`
- `bio` → `bio`

Technical Details

When a user authenticates through OAuth:

1. Casdoor receives the OAuth token and fetches user info from the provider
2. The provider response includes standard fields plus extra claims
3. Standard fields (username, email, etc.) are processed first
4. User mapping rules are applied to populate additional fields from extra claims
5. All raw claims are stored in the user's OAuth extra data for reference

This ensures that user profiles in Casdoor stay synchronized with your identity provider while maintaining flexibility in how data is structured.

谷歌

要设置Google OAuth提供商，请转到[Google API控制台](#)并使用您的Google帐户登录。

Project name *

My Casdoor



Project ID: my-casdoor. It cannot be changed later. [EDIT](#)

Location *

 No organization

[BROWSE](#)

Parent organization or folder

[CREATE](#)

[CANCEL](#)

接下来，导航到[OAuth 同意屏幕](#)选项卡以配置 OAuth 同意屏幕。

API APIs & Services

OAuth consent screen

Dashboard

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

User Type

 Internal

Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

 External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

CREATE

按照以下步骤注册您的Google应用：

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *

The name of the app asking for consent

User support email *

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

之后，转到凭证选项卡。

Credentials

[+ CREATE CREDENTIALS](#) [DELETE](#)

Create credentials to access your enabled APIs. [Learn more](#)

API Keys

<input type="checkbox"/>	Name	Creation date
No API keys to display		

OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date
No OAuth clients to display		

Service Accounts

<input type="checkbox"/>	Email	Name
No service accounts to display		

为您的应用创建凭证：

[←](#) Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *



! 请确保您正确设置了授权重定向URI

在Google OAuth配置中, `Authorized redirect URIs` 必须设置为您的 Casdoor 的回调URL, 而在Casdoor中的 `Redirect URL` 应设置为您的应用程序的回调URL。

有关更多详细信息, 请参阅[应用配置](#)。

创建Client ID后, 您将获得 `Client ID` 和 `Client Secret`。

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services



OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Your Client ID

487708653175-11oih9gfqb2u3tvfp6684qaes5ujjdca.apps.googleusercontent.com



Your Client Secret

HbxoqxxkGSs1lCVRuMTVvK57



DOWNLOAD JSON

OK

将Google OAuth提供商添加进来，并在你的Casdoor中输入Client ID和Client Secret。

[Edit Provider](#) [Save](#)

Name <small>?</small> :	my_google_provider
Display name <small>?</small> :	Google provider
Category <small>?</small> :	OAuth
Type <small>?</small> :	Google
Client ID <small>?</small>	487708653175-11oih9gfqb2u3tvfp6684qaes5ujjdca.apps.googleusercontent.com
Client secret <small>?</small>	*****
Provider URL <small>?</small> :	https://console.cloud.google.com/apis/credentials/oauthclient/498643462012-46

If Get password is enabled, you should enable google people api first and add scope <https://www.googleapis.com/auth/user.phonenumbers.read>



Google People API

Google Enterprise API

Provides access to information about profiles and contacts.

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged if you run out of credits. [Learn more](#)

≡ Google Cloud My Project 32397 Search (/) for resources, docs, products, and more

API APIs & Services Edit app registration

Enabled APIs & services OAuth consent screen Scopes Test users Summary

Library Credentials OAuth consent screen Page usage agreements

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API	Scope	User-facing description
openid	Associate you with your personal info on Google	
People API	.../auth/user/phonenumbers.read	See and download your personal phone numbers
People API	.../auth/userinfo.email	See your primary Google Account email address
People API	.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

Update selected scopes

Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter https://www.googleapis.com/auth/user.phonenumbers.read Enter property name or value

API	Scope	User-facing description
API	.../auth/user.phonenumbers.read	See and download your personal phone numbers

Manually add scopes

If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with "https://"). When you are finished, click "Add to table".

ADD TO TABLE

UPDATE

您现在可以使用Google作为第三方服务来完成身份验证。

Google One Tap

步骤1：配置您的应用程序

如果您想通过Google One Tap允许登录，您需要在您的应用程序中添加Google OAuth提供者。有关如何做到这一点的信息，请参考[Google的文档](#)。

一旦您添加了Google OAuth提供者，导航到应用程序编辑页面，添加Google OAuth提供者，并将Rule从Default切换到One Tap。

The screenshot shows the configuration interface for an application. At the top, there is a large text area containing SAML metadata XML. Below this, there is a 'Providers' section with a table listing various providers. The 'Google' provider is highlighted with a red border. In the 'Action' column for the Google provider, there is a dropdown menu with options: 'Default' (selected) and 'One Tap'. Other providers listed include 'Storage', 'Oauth', 'Email', 'Web3', and 'Oauth' again. There are also buttons for 'Copy SAML metadata URL' and 'Copy sign-in page URL'.

步骤2：使用Google One Tap登录

设置完成后，用户现在可以使用Google One Tap登录。

GitHub

GitHub OAuth支持网页应用流程和设备流程。请继续阅读以获取OAuth凭据。

首先，请访问[GitHub开发者设置](#)以注册一个新的GitHub应用。

⚠ 注意事项

小技巧：我们建议您使用GitHub Apps来替换OAuth Apps，因为GitHub Apps可以添加多个重定向URLs，这在部署测试和生产环境时可以带来便利。[GitHub](#)官方也推荐使用GitHub Apps而不是OAuth Apps。

Settings / Developer settings

 GitHub Apps

 OAuth Apps

 Personal access tokens

然后填写GitHub应用名称、主页URL、描述和回调URL。

GitHub App name *

Casdoor

The name of your GitHub App.

Write

Preview

Markdown supported

A UI-first centralized authentication / Single-Sign-On (SSO) platform supporting OAuth 2.0, OIDC and SAML, integrated with Casbin RBAC and ABAC permission management

Homepage URL *

http://door.casdoor.com

The full URL to your GitHub App's website.

Add Callback URL

Callback URL

http://localhost:7001/callback

Delete

Callback URL

https://door.casdoor.com/callback

Delete

❗ 正确设置授权回调URL

在GitHub App配置中，`Callback URL`必须是你的Casdoor的回调URL，并且Casdoor中的`Redirect URL`应该是你的应用程序的回调URL。

有关更多详细信息，请阅读[应用配置](#)。

在注册了您的GitHub应用程序后，您现在可以生成您的`Client Secret`了！

About

Owned by: [REDACTED]

App ID: [REDACTED]

Client ID: lv1 [REDACTED] d2e

[Revoke all user tokens](#)

GitHub Apps can use OAuth credentials to identify users. Learn more about identifying users by reading our [integration developer documentation](#).

Client secrets

[Generate a new client secret](#)



*****dba81954

Added 5 minutes ago by [REDACTED]

[Client secret](#)

[Delete](#)

Last used within the last week



*****15822f89

Added on 15 Feb by [REDACTED]

[Client secret](#)

[Delete](#)

Last used within the last week

添加一个GitHub OAuth提供商，并在您的Casdoor中填写 [Client ID](#) 和 [Client Secret](#)。

Edit Provider

[Save](#) [Save & Exit](#)

Name <small>②</small> :	provider_github_localhost
Display name <small>②</small> :	provider_github_localhost
Category <small>②</small> :	OAuth
Type <small>②</small> :	GitHub
Client ID <small>②</small> :	lv` [REDACTED] .2e
Client secret <small>②</small> :	***
Provider URL <small>②</small> :	https://github.com/organizations/xxx/settings/applications/1234567

[Save](#)

[Save & Exit](#)

现在您可以使用GitHub作为第三方服务来完成身份验证。

LinkedIn

要设置LinkedIn OAuth提供商，请转到[LinkedIn Developer](#)页面创建一个新的应用程序。

 DEVELOPERS Products Docs and tools ▾ Resources ▾ My apps ▾

Create an app

* indicates required

App name*

LinkedIn Page*
ⓘ This action can't be undone once the app is saved.

The LinkedIn Company Page you select will be associated with your app. Verification can be done by a Page Admin. Please note this cannot be a member profile page. [Learn more](#)

[+ Create a new LinkedIn Page ↗](#)

Privacy policy URL

App logo*
This is the logo displayed to users when they authorize with your app

 [Upload a logo](#)

在填写上述表格并创建您的应用程序后，您需要验证与应用程序关联的LinkedIn页面。



Identity Cloud Login

Client ID: 860t47n8b4jh7w | Created: Sep 4, 2020

Settings

Auth

Products

Analytics

Team members

App settings

[Delete app](#)

Company:



Identity Cloud Documentation

Computer Software; 1-10 employees

[Verify](#)



This app is not verified as being associated with this company.

[Learn more](#)

① 备注

只有公司页面管理员才能验证您的应用并授予其权限。

一旦您的应用程序通过验证，您就可以继续：

 Identity Cloud Login
Client ID: 860t47n8b4jh7w | Created: Sep 4, 2020

Settings Auth **Products** Analytics Team members

Products

Additional available products

 **Marketing Developer Platform**
Build marketing experiences to reach the right audiences [Select](#)
[View docs ↗](#)

 **Share on LinkedIn**
Amplify your content by sharing it on LinkedIn [Select](#)
[View docs ↗](#)

 **Sign In with LinkedIn**
Let users easily sign in with their professional identity [Select](#)
[View docs ↗](#)

为您的应用添加授权重定向URL，作为您的Casdoor回调URL。

Authorized redirect URLs for your app

No redirect URLs added

+ Add redirect URL

 正确设置授权的重定向 URL

在LinkedIn OAuth配置中，`authorized redirect URLs`必须是你的Casdoor的回调URL，并且Casdoor中的`Redirect URL`应该是你的应用程序的回调URL。

有关更多详细信息，请阅读[应用配置部分](#)。

然后，您可以获取您的`Client ID`和`Client Secret`。

Application credentials

Authentication keys

Client ID:

860t47n8b4jh7w

Client Secret:

..... 

在Casdoor中添加一个LinkedIn OAuth提供商，并填写`Client ID`和`Client Secret`。

Edit Provider

Save

Name [?](#) : my_linkedin_provider

Display name [?](#) : Linkedin provider

Category [?](#) : OAuth

Type [?](#) : LinkedIn

Client ID [?](#) : 860t47n8b4jh7w

Client secret [?](#) : ****

现在您可以使用LinkedIn作为第三方服务来完成身份验证!

Facebook

要设置Facebook OAuth提供商，请转到[Facebook Developer](#)网站并创建一个新的应用程序。

选择您要创建的应用类型。

Select an app type



The app type can't be changed after your app is created.



Create or manage business assets like Pages, Events, Groups, Ads, Messenger and Instagram Graph API using the available business permissions, features and products.



Consumer

Connect consumer products, and permissions, like Facebook Login and Instagram Basic Display to your app.



Instant Games

Create an HTML5 game hosted on Facebook.



Gaming

Connect an off-platform game to Facebook Login.



Workplace

Create enterprise tools for Workplace from Facebook.



None

Create an app with combinations of consumer and business permissions and products.

[Learn More About App Types](#)

Cancel

Continue

在输入您的姓名和联系电子邮件后，您将被带到Facebook开发者仪表板。

FACEBOOK for Developers

Docs Tools Support My Apps Search developer documentation

Casdoor App ID: 1231340483981478 In development ?

Dashboard Settings Roles Alerts App Review Products Add Product

Add a Product

Facebook Login
The world's number one social login product.
[Read Docs](#) [Set Up](#)

Audience Network
Monetize your app and grow revenue with ads from Facebook advertisers.
[Read Docs](#) [Set Up](#)

App Events
Understand how people engage with your business across apps, devices, platforms and websites.
[Read Docs](#) [Set Up](#)

Messenger
Customize the way you interact with people on
[Read Docs](#)

Webhooks
Subscribe to changes and receive updates in real time.
[Read Docs](#)

Instant Games
Create a cross-platform HTML 5 game hosted on
[Read Docs](#)

接下来，设置Facebook登录：



Facebook Login

The world's number one social login product.

[Read Docs](#)

[Set Up](#)

为此应用选择Web平台：

Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.



iOS



Android



Web



Other

在填写网站URL后，转到Facebook登录 > 设置，并输入有效的OAuth重定向URI。

Client OAuth Settings

Client OAuth Login
Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URLs are allowed with the options below. Disable globally if not used. [?]

Web OAuth Login
Enables web-based Client OAuth Login. [?]

Enforce HTTPS
Enforce the use of HTTPS for Redirect URLs and the JavaScript SDK. Strongly recommended. [?]

Force Web OAuth Reauthentication
When on, prompts people to enter their Facebook password in order to log in on the web. [?]

Embedded Browser OAuth Login
Enable webview Redirect URLs for Client OAuth Login. [?]

Use Strict Mode for Redirect URLs
Only allow redirects that exactly match the Valid OAuth Redirect URLs. Strongly recommended. [?]

Valid OAuth Redirect URIs
A manually specified redirect_uri used with Login on the web must exactly match one of the URLs listed here. This list is also used by the JavaScript SDK for in-app browsers that suppress popups. [?]

Valid OAuth redirect URIs:

❗ 正确设置授权的 REDIRECT URL

在Facebook OAuth配置中，**Valid OAuth Redirect URIs**必须是你的Casdoor的回调URL，并且Casdoor中的**Redirect URL**应该是你的应用程序的回调URL。

有关更多详细信息，请阅读[应用配置部分](#)。

基本的应用配置几乎完成了！

将顶部工具栏中的模式从开发中切换到实时。



现在您可以在Casdoor中使用您的App ID和App Secret。

App ID	App Secret
<input type="text" value="1231340483981478"/>	<input type="text" value="*****"/> Show

添加Facebook OAuth提供商，并填写Client ID和Client Secret，用你的Casdoor中的App ID和App Secret。

修改提供商 [保存](#)

名称 ? :	my_facebook_provider
显示名称 ? :	Facebook provider
分类 ? :	OAuth
类型 ? :	Facebook
Client ID ?	1231340483981478
Client secret ?	*****

您现在可以使用Facebook作为第三方服务进行身份验证！

Apple

To set up the Apple Sign in provider, please go to the [Apple Developer](#) website. An active Apple Developer Program membership is required.

Step 1: Configure App ID

Create a new App ID or configure an existing one, and ensure Sign in with Apple is enabled for it.

The screenshot shows a list of services under 'Edit your App ID Configuration'. The 'Sign In with Apple' option has a red arrow pointing to its checkbox, which is checked. Another red arrow points to the 'Edit' button next to the service name. A third red arrow points to the 'Enable as a primary App ID' link at the end of the row. The other services listed are Push to Talk, Sensitive Content Analysis, Shallow Depth and Pressure, Shared with You, Siri, and System Extension. There are 'Remove' and 'Save' buttons at the top right.

Edit your App ID Configuration	
<input type="checkbox"/>	Push to Talk ⓘ
<input type="checkbox"/>	Sensitive Content Analysis ⓘ
<input type="checkbox"/>	Shallow Depth and Pressure ⓘ
<input type="checkbox"/>	Shared with You ⓘ
<input checked="" type="checkbox"/> #	Sign In with Apple ⓘ
<input type="checkbox"/>	Siri ⓘ
<input type="checkbox"/>	System Extension ⓘ

Step 2: Create a Services ID

Next, create a new identifier, making sure to select the Services IDs type. (The Identifier you set here will be your Client ID in Casdoor).

[« All Identifiers](#)

Register a new identifier

App IDs

Register an App ID to enable your app, app extensions, or App Clip to access available services and identify your app in a provisioning profile. You can enable app services when you create an App ID or modify these settings later.

Services IDs

For each website that uses Sign in with Apple, register a services identifier (Services ID), configure your domain and return URL, and create an associated private key.

Pass Type IDs

Register a pass type identifier (Pass Type ID) for each kind of pass you create (i.e. gift cards). Registering your Pass Type IDs lets you generate Apple-issued certificates which are used to digitally sign and send updates to your passes, and allow your passes to be recognized by Wallet.

Order Type IDs

Register an order type identifier (Order Type ID) to support signing and distributing order bundles with Wallet and Apple Pay. Registering your order type ID lets you generate certificates to digitally sign and send updates to your orders in Wallet.

Website Push IDs

Register a Website Push Identifier (Website Push ID). Registering your Website Push IDs lets you generate

Then, configure this Services ID. Enable Sign in with Apple and click Configure.

[« All Identifiers](#)

Edit your Services ID Configuration

[Remove](#)

[Continue](#)

Description

Identifier

You cannot use special characters such as @, &, *, "

ENABLED NAME

Sign In with Apple

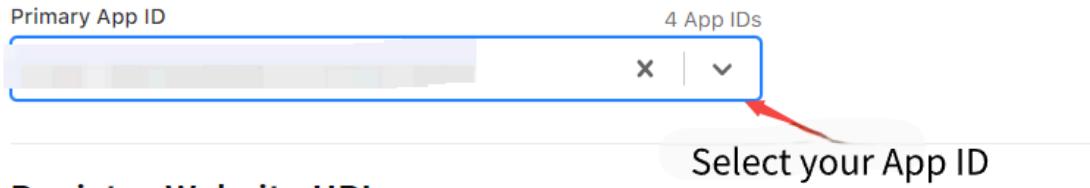
[Configure](#)

Step 3: Configure Redirect URLs

In the configuration screen, set up the Return URLs (callback URLs). You need to enter the Redirect URL shown on the Casdoor provider page here.

Web Authentication Configuration

Use Sign in with Apple to let your users sign in to your app's accompanying website with their Apple ID. To configure web authentication, group your website with the existing primary App ID that's enabled for Sign in with Apple.



Register Website URLs

Provide your web domain and return URLs that will support Sign in with Apple. Your website must support TLS 1.2 or higher. All Return URLs must be registered with the https:// protocol included in the URI string. After registering new website URLs, confirm the list you'd like to add to this Services ID and click Done. To complete the process, click Continue, then click Save.

Domains and Subdomains

A screenshot of an input field labeled "Domains and Subdomains". To the right of the field is the text "Your domain" with a red arrow pointing to it. Below the input field is the placeholder text "Enter a comma delimited list of domains and subdomains."

Return URLs

A screenshot of an input field labeled "Return URLs". To the right of the field is the text "Full callback URL" with a red arrow pointing to it. Below the input field is the placeholder text "Enter a comma delimited list of Return URLs."

⚠ SET RETURN URLs CORRECTLY

The `Return URLs` on Apple must exactly match the `Redirect URL` shown on your Casdoor Apple provider configuration page (e.g., `https://your-casdoor-domain.com/callback`).

Step 4: Create a Key

After configuring the Services ID, create a Key. When creating the Key, enable Sign in with Apple and associate it with your App ID.

Certificates, Identifiers & Profiles

[« All Keys](#)

Configure key

[Continue](#)

Key Name

You cannot use special characters such as @, &, *, %, -, .

ENABLE	NAME	DESCRIPTION
<input type="checkbox"/>	Apple Push Notifications service (APNs)	Establish connectivity between your notification server and the Apple Push Notification service. One key is used for all of your apps. Learn more
<input type="checkbox"/>	DeviceCheck	Access the DeviceCheck and AppAttest APIs to get data that your associated server can use in its business logic to protect your business while maintaining user privacy. Learn more
<input type="checkbox"/>	Media Services (MusicKit, ShazamKit)	Access the Apple Music catalog and make personalized requests for authorized users, and check audio signatures against the Shazam music catalog. <small>(There are no Identifiers available that can be associated with the key.)</small>
<input checked="" type="checkbox"/>	Sign in with Apple	Enable your apps to allow users to authenticate in your application with their Apple ID. Configuration is required to enable this feature.
<input type="checkbox"/>	Account & Organizational Data Sharing	Configure your apps and websites with Account & Organizational Data Sharing to securely request access to your users' Apple ID account information.
<input type="checkbox"/>	ClassKit Catalog	Publish all of your ClassKit app activities to teachers creating Handouts in Apple Schoolwork. Learn more

[Configure](#) [Edit](#)

Red arrows point to the "Edit" button for the "Sign in with Apple" service and the "Edit" button for the "Sign in with Apple" row in the table.

After registering the Key, note down the Key ID and download the **.p8** file immediately. (This file can only be downloaded once, save it securely!)

Certificates, Identifiers & Profiles

[« All Keys](#)

View Key Details

[Download](#) [Revoke](#) [Edit](#)

Name: StudyXAppleLogin

Key ID: Y kid

Enabled Services

NAME	CONFIGURATION
Sign in with Apple	5R.com

Red arrows point to the "kid" label under the Key ID and the "teamId" label under the "Sign in with Apple" configuration.

Important: Find and note down your **Team ID** from the **Membership** page on the Apple Developer Portal.

Step 5: Configure Casdoor Provider

1. Client ID: Enter the Apple Services ID **Identifier** you created earlier.
2. Team ID: Enter your Apple Team ID (found on the Membership page).
3. Key ID: Enter the Apple Key ID you noted down.
4. Key Text: Open the downloaded **.p8** file with a text editor. Copy its entire content (including the **-----BEGIN . . .** and **-----END . . .** lines) and paste it here.
5. Check Redirect URL: Verify that the **Redirect URL** shown here in Casdoor has been correctly added to the **Return URLs** in your Apple Services ID configuration.

Service ID identifier <small>(?)</small> :	<input type="text"/>
Team ID <small>(?)</small> :	<input type="text"/>
Key ID <small>(?)</small> :	<input type="text"/>
Key text <small>(?)</small> :	<input type="text"/>
Provider URL <small>(?)</small> :	<input type="text"/> <small>✓ https://github.com/organizations/xxx/settings/applications/1234567</small>

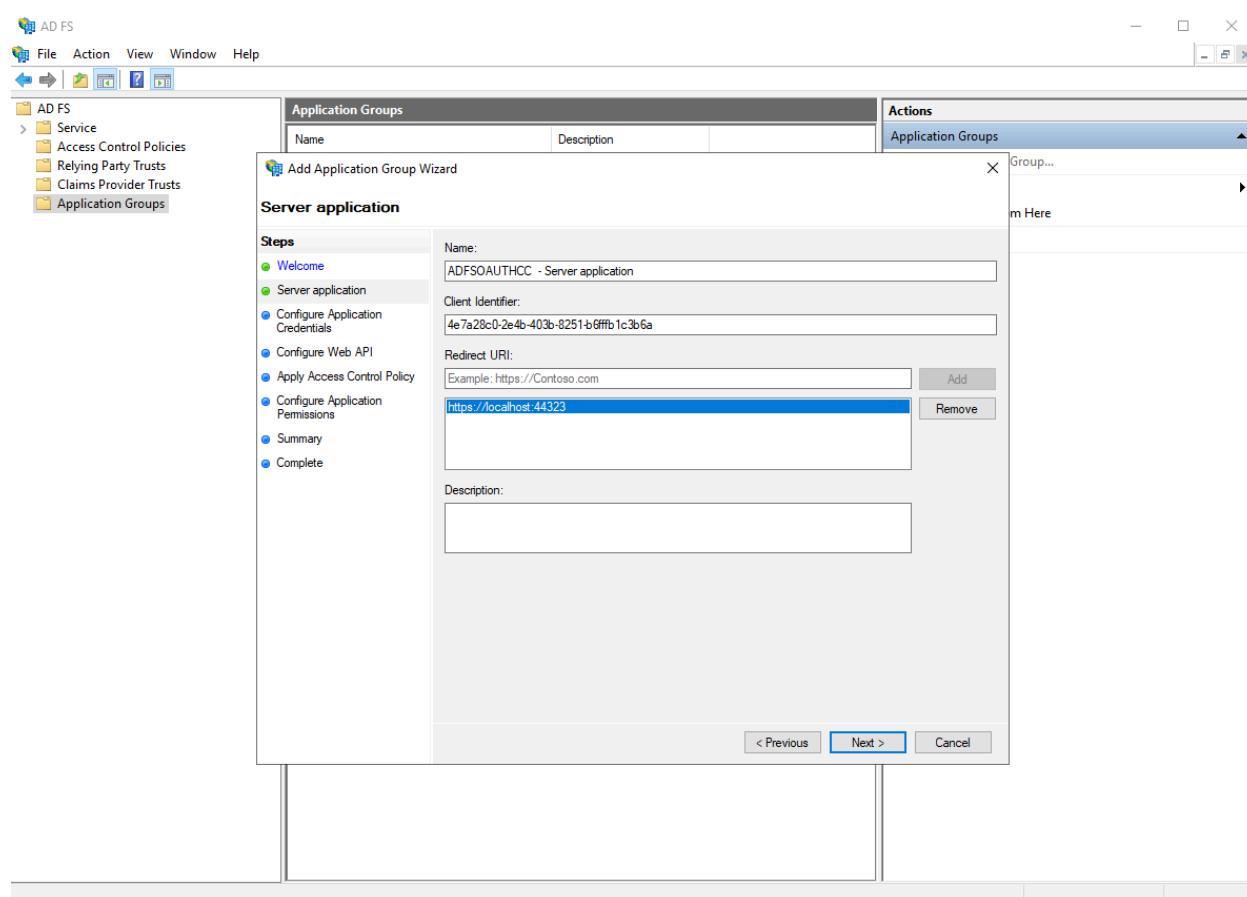
AD FS

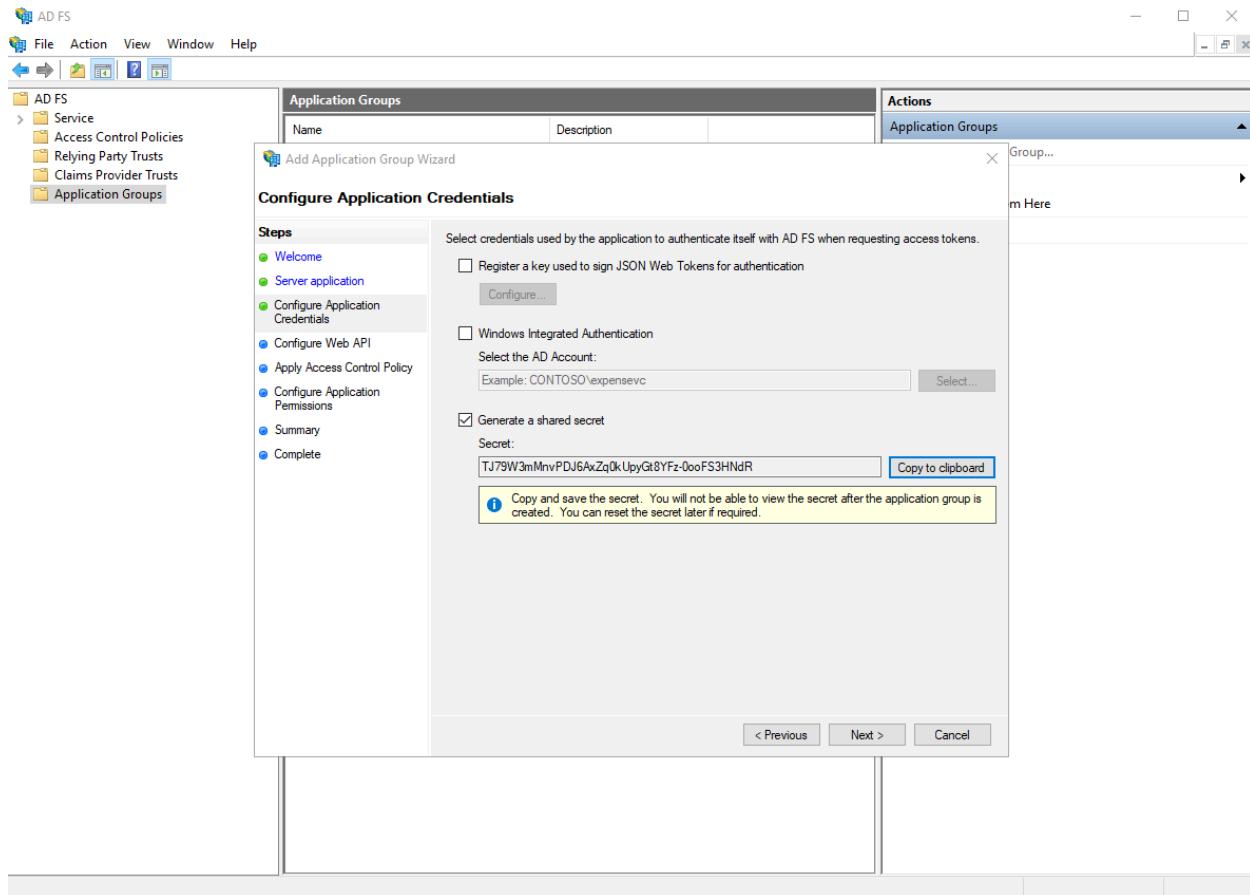
要设置 Active Directory 联合服务，请参考[AD FS 文档](#)以基本了解 ADFS，并查阅[AD FS 部署指南](#)以获取设置 AD FS 服务器的指导。确保在进行下一步操作之前，你已经拥有一个完全可操作的AD FS服务器。

步骤1：通过AD FS启用OAuth

有关逐步创建应用程序的详细说明，请参阅[启用AD FS的OAuth机密客户端指南](#)。

到了这一步的末尾，您应该已经获得了客户端ID和客户端密钥，如下面的截图所示：





第一张图片中的客户端标识符和第二张图片中的秘密应作为OAuth设置中的客户端ID和客户端秘密使用。

启用Casdoor AD FS提供商

在您的Casdoor设置中添加一个AD FS提供商，并输入"Client ID"和"Client Secret"。

Edit Provider [Save](#) [Save & Exit](#)

Name ②:

Display name ②:

Category ②: OAuth

Type ②: Adfs 

Client ID ②

Client secret ②

Domain ②:

Provider URL ② <https://openhome.alipay.com/platform/appManage.htm#/app/2021003111697088/overview>

[Save](#) [Save & Exit](#)

Azure AD

介绍

Azure Active Directory (Azure AD) 通过为云和本地应用程序提供单一的身份系统，简化了应用程序管理。软件即服务 (SaaS) 应用程序，本地应用程序和业务线 (LOB) 应用程序可以添加到 Azure AD 中。然后用户可以一次登录来安全和无缝地访问这些应用程序。以及微软公司提供的办公室365项和其他商业应用程序。

如何使用？

注册应用程序的步骤如下所示。

步骤1：注册一个应用程序

首先，[注册](#)一个应用程序，并根据需要选择账户类型。演示站使用下面显示的类型。

[Home](#) >

Register an application

* Name

The user-facing display name for this application (this can be changed later).



Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

By proceeding, you agree to the [Microsoft Platform Policies](#) 

[Register](#)

步骤2：创建客户端密钥

创建一个 `client secret` 并保存其值，因为稍后会用到。

The screenshot shows the Casdoor interface for managing certificates and secrets. On the left, a sidebar lists various management options like branding, authentication, and certificates. The 'Certificates & secrets' option is highlighted with a red box. The main content area displays a table of client secrets. One row is selected, showing details: Description 'casdoor', Expires '1/8/2023', Value '3Xr8Q~dFau2Hwyhg6y8Upb53PCFbuF...', and Secret ID 'f3c7d37c-1def-4e29-b75f-457fa7c081e8'. The 'Value' field is also highlighted with a red box.

步骤3：添加重定向URI

按照图片中的示例为Casdoor添加重定向URI。

The screenshot shows the Casdoor 'Authentication' configuration page. The left sidebar has 'Authentication' selected with a red box. In the main area, there's a section for 'Platform configurations' with a 'Add a platform' button highlighted with a red box. To the right, under 'All platforms', there's a 'Redirect URLs' section with a red box around it. It contains the URL 'http://localhost:8000/callback'. Below this are sections for 'Front-channel logout URL' (with an example URL) and 'Implicit grant and hybrid flows'.

步骤4：授予管理员同意

`user.read` API 默认是打开的。您可以根据自己的需要添加更多的作用域。最后，记得 给予管理员权限。

The screenshot shows the Casdoor API permissions page. The left sidebar has sections for Overview, Quickstart, Integration assistant, Manage (with Branding & properties, Authentication, Certificates & secrets, Token configuration, and API permissions), Expose an API, App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting (Troubleshooting and New support request). The main area shows a message: "Successfully granted admin consent for the requested permissions." A warning message states: "Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)". Another message says: "The 'Admin consent required' column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your org app will be used. [Learn more](#)". The "Configured permissions" section shows a table for Microsoft Graph (5 permissions: email, offline_access, openid, profile, User.Read) with "Admin consent reqd" set to No for all. A red box highlights the "Grant admin consent for Default Directory" button. A red box also highlights the list of granted permissions on the right.

API / Permissions name	Type	Description	Admin consent reqd	Status
email	Delegated	View users' email address	No	Granted for Default Dir...
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Default Dir...
openid	Delegated	Sign users in	No	Granted for Default Dir...
profile	Delegated	View users' basic profile	No	Granted for Default Dir...
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Dir...

步骤5：在Casdoor中创建AzureAD提供商

最后一步是添加一个AzureAD OAuth提供者，并在您的Casdoor中填写 `Client ID` 和 `Client Secret`。

Edit Provider

Save

Save & Exit

Name ? : provider_casdoor_azuread

Display name ? : Casdoor AzureAD

Category ? : OAuth

Type ? : AzureAD

Client ID ? : 621cc0f0-055f-433f-9894-bfa1bfde169d

Client secret ? : ***

Provider URL ? : https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/Applications列表

Save

Save & Exit

Azure AD B2C

介绍

Azure AD B2C 是一种客户身份访问管理解决方案，支持 OpenID Connect、OAuth 2.0 和 SAML 等标准。它允许将面向消费者的应用程序与可扩展和可定制的身份管理解决方案集成。

如何使用？

下面显示了设置 Azure AD B2C 用于身份验证的步骤。

步骤 1：创建 B2C 租户

首先，在您的 Azure 门户中创建一个 B2C 租户。

步骤 2：注册应用程序

在您的 B2C 租户内注册应用程序。

[Home](#) >

Register an application

* Name

The user-facing display name for this application (this can be changed later).



Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

By proceeding, you agree to the [Microsoft Platform Policies](#) 

[Register](#)

步骤 3：创建客户端密钥

为您的应用程序创建一个 `client secret` 并保存该值，因为稍后将使用它。

casdoor | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Description	Expires	Value	Secret ID
casdoor	1/8/2023	3Xr8Q~dFau2Hwyhg6y8Upb53PCFbuF...	f3c7d37c-1def-4e29-b75f-457fa7c081e8

步骤 4：添加重定向 URIs

在 Azure AD B2C 设置中为您的应用程序添加重定向 URIs。

casdoor | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration redirect URLs, specific authentication settings, or fields specific to the platform.

Add a platform

Supported account types

Who can use this application or access this API?

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

All users with a work or school, or personal Microsoft account can use your application. Office 365 subscribers.

To change the supported accounts for an existing registration, use the manifest editor. Take properties may cause errors for personal accounts. [Learn more about these restrictions.](#)

Save Discard

Configure Cancel

Front-channel logout URL

This is where we send a request to have the application sign-out. It is required for single sign-out to work correctly.

e.g. <https://example.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint (SPA) and doesn't use the auth code flow. If your application is a page architecture (SPA) and doesn't use the auth code flow, select both access tokens and ID tokens. Other web apps that use hybrid authentication must obtain tokens.

步骤 5：定义用户流程

在 Azure AD B2C 中定义用户流程，以管理用户如何注册、登录以及管理他们的个人资料。

步骤 6：在 Casdoor 中创建 Azure AD B2C 提供商

最后，在 Casdoor 中添加一个 Azure AD B2C OAuth 提供商，使用来自您的 B2C 租户的 `Client ID` 和 `Client Secret`。

Edit Provider Save Save & Exit

Name <small>?</small> :	provider_casdoor_azuread
Display name <small>?</small> :	Casdoor AzureAD
Category <small>?</small> :	OAuth
Type <small>?</small> :	AzureAD
Client ID <small>?</small> :	621cc0f0-055f-433f-9894-bfa1bfde169d
Client secret <small>?</small> :	***
Provider URL <small>?</small> :	https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade

Save Save & Exit

自定义OAuth

ⓘ 备注

Casdoor支持自定义提供商。然而，自定义提供商必须遵循3-legged OAuth的标准流程，[Token URL](#)和[UserInfo URL](#)的返回值必须符合Casdoor指定的格式。

Overview

Custom OAuth providers allow you to integrate any OAuth 2.0 compliant authentication service with Casdoor, even if it's not officially supported. This is useful when you want to integrate with:

- Internal enterprise OAuth servers
- Self-hosted authentication systems
- Third-party services not yet officially supported by Casdoor

Multiple Custom Providers Support

Casdoor supports up to 10 different custom OAuth providers simultaneously. When creating custom providers, you can choose from the following types:

- Custom - The first custom provider
- Custom2 through Custom10 - Additional custom providers

This allows you to integrate multiple custom OAuth services without conflicts. Each custom provider maintains its own separate configuration and user data fields.

Creating a Custom Provider

To create a new custom provider, navigate to the provider page of Casdoor, and select one of the custom types ("Custom", "Custom2", "Custom3", etc.) in the Type field. 然后，您需要填写[Client ID](#)、[Client Secret](#)、[Auth URL](#)、[Scope](#)、[Token URL](#)、[UserInfo URL](#)和[Favicon](#)。

Type [?](#) :

Auth URL [?](#)

Scope [?](#)

Token URL [?](#)

Userinfo URL [?](#)

Favicon [?](#) :

URL [?](#) :

Preview:

Client ID [?](#)

Client secret [?](#)

- Auth URL 是自定义提供商的 OAuth 登录页面地址。

如果你在 Auth URL 中填写 `https://door.casdoor.com/login/oauth/authorize`, 那么, 当用户使用这个自定义提供者登录时, 浏览器将首先重定向到

```
https://door.casdoor.com/login/oauth/
authorize?client_id={ClientID}&redirect_uri=https://{{your-casdoor-
hostname}}/callback&state={State_generated_by_Casdoor}&response_type=code&scope={Scope}`
```

授权完成后, 自定义提供商应该重定向到

```
https://{{your-casdoor-hostname}}/callback?code={code}
```

经过这一步, Casdoor将会识别URL中的code参数。

- Scope 是访问 Auth URL 时携带的范围参数, 您应根据自定义提供商的要求进行填写。

- **Token URL** 是获取accessToken的API端点。

一旦你在前一步获取了代码，Casdoor应该使用它来获取accessToken。

如果你在**Token URL**中填入https://door.casdoor.com/api/login/oauth/access_token，那么Casdoor将使用以下命令来访问它

```
curl -X POST -u "{ClientID}:{ClientSecret}" --data-binary
"code={code}&grant_type=authoritiation_code&redirect_uri=https://your-casdoor-
hostname/callback" https://door.casdoor.com/api/login/oauth/access_token
```

自定义提供者应至少返回以下信息：

```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IxXXXXXXXXXXXX",
  "refresh_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IxXXXXXXXXXXXX",
  "token_type": "Bearer",
  "expires_in": 10080,
  "scope": "openid profile email"
}
```

- **UserInfo URL** 是通过accessToken获取用户信息的API端点。

如果你在**UserInfo URL**中填入<https://door.casdoor.com/api/userinfo>，那么Casdoor将使用以下命令来访问它

```
curl -X GET -H "Authorization: Bearer {accessToken}" https://door.casdoor.com/api/
userinfo
```

自定义提供者应至少返回以下信息：

```
{
  "name": "admin",
  "preferred_username": "Admin",
  "email": "admin@example.com",
  "picture": "https://casbin.org/img/casbin.svg"
}
```

- **Favicon** 是自定义提供商的标识URL。

此标志将与其他第三方登录提供商一起在Casdoor的登录页面上显示。

Okta

要设置Okta OIDC提供商，首先访问[Okta Developer](#)并注册以获取开发者账户。

导航到应用程序 > 应用程序选项卡，点击创建应用集成，选择登录方法为OIDC - OpenID Connect，并选择应用类型为Web应用程序，然后点击下一步。

Create a new app integration

Sign-in method

[Learn More](#)

OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.NET, Node.js, PHP)

Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)

输入登录重定向URI，例如 `https://door.casdoor.com/callback`。

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URLs

[Learn More](#)

Allow wildcard * in sign-in URL redirect.

[+ Add URI](#)

在任务部分，为您的应用定义受控访问的类型，然后点击保存以创建应用集成。

现在你将拥有 **Client ID**, **Client secret** 和 **Okta domain**。

Client Credentials

[Edit](#)

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings

[Edit](#)

Okta domain

在Casdoor仪表板中添加一个Okta OAuth提供商，输入您的 **客户端ID**, **客户端密钥** 和 **域**。

Edit Provider Save Save & Exit

Name ?: provider_casdoor_okta

Display name ?: Casdoor Okta

Category ?: OAuth

Type ?: Okta

Client ID ?: 0oa4we8u8iivyscpb5d7

Client secret ?: ***

Domain ?: <https://dev-53555475.okta.com/oauth2/default>

Provider URL ?: <https://dev-53555475.okta.com>

:

Save

Save & Exit

❗ 正确设置域名

请注意, **Domain**不仅仅是**Okta domain**; 应该在其后追加**/oauth2/default**。

在授权服务器上访问 [Okta 文档](#) 获取更多详情。

现在您可以使用Okta作为第三方服务来完成身份验证。

Twitter

Twitter (进行中

由于官方限制严格，申请Twitter的开发者账号可能会有些繁琐。与其他第三方平台相比，这可能更具挑战性。

首先，访问[开发者门户](#)，如果你还没有账号，就创建一个。Twitter要求你为开发者账号的申请提供详细的应用信息。确保准确填写信息，以避免在审查过程中出现任何问题。

一旦你的申请被批准，你就可以开始创建应用了。你需要在**认证设置**部分完成两项重要任务：

1. 手动启用**3-legged OAuth**。这对于“使用Twitter登录”和代表其他账户发布推文等功能是必要的。
2. 启用**向用户请求电子邮件地址**以获取用户的电子邮件地址。

确保仔细填写应用的回调地址和其他必要信息。

微博

Weibo ✓

申请微博开发者账户并不困难，但过程可能会慢，大约需要2-3天。

首先，访问[开发者网站](#)并填写所需的基本信息。然后，你需要等待一个彻底的审查...

一旦你的申请被批准，你将收到客户端ID和客户端密钥。

微信

WeChat ✓

Add WeChat OAuth Provider

若要将微信OAuth提供商添加到你的应用，请遵循以下步骤

1. 访问 [微信开放平台](#) 并注册成为开发者。
2. 在你的网站应用或移动应用获得批准后，您将得到您的 App ID 和 App Secret。

Name ②: provider_casdoor_wechat

Display name ②: Casdoor WeChat

Organization ②: admin (Shared)

Category ②: OAuth

Type ②: WeChat

Client ID ②: wx049c70e6c2027b0b

Client secret ②: ***

Client ID 2 ②: wxe933a9cd81c396d1

Client secret 2 ②: ***

服务器配置(已启用)

Use WeChat

Media Platform in PC ②:

令牌(Token) 123

Access token ②:

Follow-up action Use WeChat Open Platform to login Use WeChat Media Platform to login

Provider URL ②: <https://open.weixin.qq.com/>

WeChat 提供商提供两套不同的密钥：

- 第一组密钥对 (`Client ID`, `Client Secret`) 是 `WeChat Open Platform` (微信开放平台) 的，并且适用于PC登录场景。它允许你在PC浏览器显示二维码，让用户能够使用微信APP扫描此二维码进行登录。
- 第二组密钥对(`Client ID 2`, `Client Secret 2`) 以及 `Access Token` 是 `WeChat Media Platform` (微信公众平台) 的，目的是让用户能在微信APP内进行

登录。Access Token 是你在 WeChat Media Platform (微信公众平台) 的服务器配置中填写的 Token。它允许用户使用微信内部的浏览器进行登录，他会将用户重定向到你的 WeChat Official Account (微信公众号) 以实现登录。请注意：微信不支持在除微信APP之外的任何移动浏览器或者APP进行登录。这一限制是由 WeChat 而不是 Casdoor 施加的。

如果您填写了第二对密钥 (Client ID 2, Client Secret 2)，填写了 Access Token 字段并启用了 Enable QR code 开关，那么您可以选择直接使用微信公众平台的信息扫描二维码后登录，或者使用微信开放平台的信息登录，如果您选择 使用微信开放平台登录，在用户关注微信公众号后，用户将被要求扫描微信开放平台的二维码进行登录。当用户点击微信按钮进行登录时，Casdoor 会要求用户在继续登录过程之前关注微信公众号。值得注意的是，这只能在PC登录场景中使用，因为手机无法自行扫描二维码。当在移动场景中使用时(即WeChat App的内置浏览器)，Casdoor 将自动跳过这一步。

You can choose whether to enable the WeChat QR code login option on the setting page. To do so, add the WeChat provider in your application configuration and add the WeChat option in your signin methods. Once added, the login page will display a "WeChat" tab as a login option, allowing users to log in by scanning the QR code.

The QR code login process is as follows:

1. On the login page, after selecting the "WeChat" tab, a WeChat QR code will be automatically loaded and displayed.
2. The user scans the QR code using the WeChat app and completes the authorization to log in.
3. If the QR code expires or needs to be refreshed, the user can click the "Refresh" link below the QR code to obtain a new one.

The screenshot shows the 'Signin methods' configuration screen in Casdoor. At the top left, there is a 'Signin methods' dropdown and an 'Add' button. Below this is a table with columns: 'Name', 'Display name', 'Rule', and 'Action'. The table contains five rows: 'Password' (Display name: Password, Rule: All), 'Verification code' (Display name: Verification code, Rule: All), 'WebAuthn' (Display name: WebAuthn, Rule: All), 'Face ID' (Display name: Face ID, Rule: All), and an empty row. At the bottom left, there is an 'Org choice mode' section with 'LDAP' and 'WeChat' options, where 'WeChat' is highlighted with a red box.

💡 提示

我们建议同时设置两套密钥对用来在 [WeChat Open Platform \(微信开放平台\)](#) 内部连接你的 [WeChat Open Platform \(微信开放平台\)](#) 账号与 [WeChat Media Platform \(微信公众平台\)](#) 账号。从而让Casdoor将通过PC和手机登录的用户视为同一用户。

ⓘ 备注

由于WeChat OAuth的限制，目前没有任何方法通过微信登录除微信APP以外的任何第三方手机APP或移动浏览器。目前移动端登录只能在微信APP中进行。

更多细节请浏览 [微信开放平台](#)。

Enable WeChat QR Code Login

You can choose whether to enable the WeChat QR code login option on the setting page. To do so, add the WeChat provider in your application configuration and add the WeChat option in your signin methods. Once added, the login page will display a "WeChat" tab as a login option, allowing users to log in by scanning the QR code.

The QR code login process is as follows:

1. On the login page, after selecting the "WeChat" tab, a WeChat QR code will be automatically loaded and displayed.
2. The user scans the QR code using the WeChat app and completes the authorization to log in.
3. If the QR code expires or needs to be refreshed, the user can click the "Refresh" link below the QR code to obtain a new one.

Signin methods

① :

Name	Display name	Rule	Action		
Password	Password	All			
Verification code	Verification code	All			
WebAuthn	WebAuthn				
Face ID	Face ID				

Org choice mode ② :

LDAP

WeChat



Password [WeChat](#)



[Refresh](#)

Powered by Casdoor

企业微信

介绍

WeCom提供了一种使用OAuth的授权登录方法，这使您可以直接从WeCom终端打开的网页中获取成员的身份信息，从而无需登录过程。

有两种类型的应用程序：**内部应用程序**和**第三方应用程序**。

基本配置

要配置WeCom提供商，您需要提供以下参数：

参数描述:

参数	描述
Sub type	内部或第三方
Method	静默或正常模式
Client ID	企业CorpID
Client secret	企业CorpSecret
Agent ID	应用程序Agentid

① 信息

WeCom支持两种授权方法：**静默授权**和**普通授权**。

静默授权：用户点击链接后，页面将重定向到`redirect_URI?code=CODE&state=STATE`

普通授权：用户点击链接后，会显示一个中间页面供用户选择是否授权。用户确认授权后，他们将被重定向到`redirect_uri?code=CODE&state=STATE`

有关更多详细信息，请参阅[官方文档](#)。

更多信息

有关内部应用的更多信息，请参阅[内部应用](#)文档。

有关第三方应用的信息，请参阅[第三方应用](#)文档。

腾讯 QQ

腾讯QQ ✓

要将腾讯QQ OAuth提供商添加到您的应用程序中，请访问QQ的认证平台 - [Connect QQ](#)。

首先，您需要申请成为开发者。在您的申请获得批准后，按照平台的指示获取您的客户端ID和客户端密钥。

钉钉

钉钉 ✓

配置钉钉

要配置钉钉，请访问[钉钉开发者平台](#)并使用您的钉钉账户登录。一旦你在平台上，按照提供的指示获取你的[客户端 ID](#)和[客户端密钥](#)。钉钉中的对应术语如下：

术语	钉钉名称
Client ID	AppKey
Client secret	AppSecret

在钉钉中，你可以在应用信息中找到[Appkey](#)和[AppSecret](#)。

基础信息

应用信息

开发管理

权限管理

应用功能

机器人与消息推送

事件与回调

登录与分享

酷应用

安全与监控

监控中心

部署与发布

版本管理与发布

应用信息



casdoor

document

应用凭证

AgentId

2687194261

AppKey

ding6dposoornm8u4t2g5

AppSecret

hE4cwQ4PjKDSp_ucHTBTqjAAfZfsNGkxwNg1q1FCiiTRW7apxJhzjFOjw46NfFWn

删除应用

删除操作不可逆，该应用所有信息将被删除，请谨慎操作。

删除

确保添加重定向域，它应该是你的Casdoor域。

基础信息

应用信息

开发管理

权限管理

应用功能

机器人与消息推送

事件与回调

登录与分享

酷应用

安全与监控

监控中心

部署与发布

接入登录

添加重定向 URL 作为免登授权码跳转地址。[了解更多](#)

* 回调域名

请填写 HTTP/HTTPS 开头的 URL

添加

微应用回调的URL

http://localhost:7001

重定向

接入分享

嵌入分享SDK，实现一键登录后内容分享。[了解更多](#)

iOS 分享

更多详细信息，请参考[钉钉开发者文档](#)。

此外，你需要向钉钉应用添加以下权限：

The screenshot shows the DingTalk Developer Platform interface. The top navigation bar includes '首页', '应用开发' (which is highlighted with a red box), '开放能力', '开发工具', '阿里云', '基本信息', and '开发文档'. Below the navigation is a search bar and a '批量申请' button. The left sidebar contains sections like '基础信息', '应用信息', '开发管理', '权限管理' (which is also highlighted with a red box), '应用功能', '事件与回调', '登录与分享', '安全与监控', '监控中心', '部署与发布', and '版本管理与发布'. The main content area displays a table of permissions. The first two rows of the table are highlighted with red boxes:

权限信息	接口	权限点code	全部状态	操作
个人手机号信息	获取用户个人信息	Contact.User.mobile	已开通	移除权限
个人支付宝绑定信息	获取支付宝绑定信息	Contact.User.alipayAccount	未开通	申请权限
签到	签到			
日历应用中日程写权限	修改日程	Calendar.Event.Write	未开通	申请权限
智能人事	分页获取参与人列表			
日志	查看单个日程的签到详情	Calendar.Event.Read	未开通	申请权限
签到	查询日程列表			
钉钉运动	通讯录个人信息读权限	Contact.User.Read	已开通	移除权限
应用管理	获取用户忙闲信息	Calendar.EventSchedule.Read	未开通	申请权限
身份验证	查询日历本	Calendar.Calendar.Read	未开通	申请权限

配置Casdoor

这是钉钉的最终配置：

Name [?](#) : dingding

Display name [?](#) : dingding

Organization [?](#) : admin (Shared)

Category [?](#) : OAuth

Type [?](#) : DingTalk

Client ID [?](#) : ding6dposoonm8u4t2g5

Client secret [?](#) : ***

Provider URL [?](#) : <https://github.com/organizations/xxx/settings/applications/1234567>

Steam

Steam ✓

要将Steam OAuth提供商添加到您的应用程序中，请按照以下步骤操作：

1. 访问[Steam WebAPI平台](#)并使用您的Steam账户登录。
2. 为您的Casdoor域名或IP申请一个API密钥。
3. 将您的API密钥作为客户端密钥填入Casdoor。客户端ID不需要填写。
4. 确保您的Steam账户有游戏，以便申请API。

如需获取更详细的信息，请访问[Steam WebAPI文档](#)。

Gitee

要设置 Gitee OAuth 提供商, 请转到 [Gitee 开发者](#) 网站。如果你以前没有创建过应用程序, Gitee 工作台将会是这样的:

The screenshot shows the Gitee developer console interface. At the top, there is a navigation bar with links for '特惠', '企业版', '高校版', '私有云', '博客', and '我的'. On the right side of the top bar are icons for notifications, location, and account settings. Below the top bar, there is a search bar labeled '搜开源' and a button with a plus sign. The main area has tabs for '我的应用' (selected) and '已授权应用'. A message '无数据' (No data) is displayed below the tabs.

然后, 您可以创建您的Gitee应用。

创建第三方应用

应用名称 *

应用名称

应用描述

应用描述

应用主页 *

你的应用主页

应用回调地址 * +

用户授权后, 重定向的地址, 例如: <https://gitee.com/login>

输入名称、描述、主页和回调URL, 并仔细选择权限。

① 正确设置授权回调URL

在 Gitee OAuth 配置中, `authorization callback URL` 必须是 你的 Casdoor 的回调 URL, 并且 Casdoor 中的 `Redirect URL` 应该是 你的应用程 序的回调 URL。

有关更多详细信息, 请阅读[应用配置指南](#)。

创建Gitee应用后, 您可以获取`Client ID`和`Client Secrets`!

Casdoor (今日请求次数: 0 次)

应用名称 *

Casdoor

Client ID

300ff94d994a7597850bbafb2d5dc67929676dd8e7176b029e067dc6966ef9c4

Client Secret

60be2e4e0f3fb8286cfe9f129ab0c3d6b40718a964dade150a8095eb2748730c

[重置 Client Secret](#)

[移除已授权用户的有效 Token](#)

在您的Casdoor中添加一个Gitee OAuth提供商, 并输入`client ID`和`client Secrets`。

Edit Provider

Save

Name ③ :

my_gitee_provider

Display name ③ :

Gitee provider

Category ③ :

OAuth

Type ③ :

Gitee

Client ID ③

300ff94d994a7597850bbafb2d5dc67929676dd8e7176b029e067dc6966ef9c4

Client secret ③

现在您可以使用 Gitee 作为第三方服务来完成身份验证！

⚠ 注意事项

由于Casdoor需要获取用户的电子邮件，因此必须勾选电子邮件选项；否则，将会导致范围授权错误。

Permissions (Be careful to select scopes, users might deny authorization when there are too many scopes.)

All

- | | |
|---|--|
| <input checked="" type="checkbox"/> user_info | Access and update user data, activities, etc |
| <input type="checkbox"/> projects | Full control of user projects |
| <input type="checkbox"/> pull_requests | Full control of user pull requests |
| <input type="checkbox"/> issues | Full control of user issues |
| <input type="checkbox"/> notes | Access, create and edit user comments |
| <input type="checkbox"/> keys | Full control of user public keys |
| <input type="checkbox"/> hook | Full control of user webhook |
| <input type="checkbox"/> groups | Full control of user orgs and teams |
| <input type="checkbox"/> gists | Access, create and update user gists |
| <input type="checkbox"/> enterprises | Full control of user enterprises and teams |
| <input checked="" type="checkbox"/> emails | Access user emails data |

Submit

Delete

百度

要设置Baidu OAuth提供商，请阅读[Baidu文档](#)并按照他们的步骤完成[应用创建](#)。

开发者服务管理

📍 提示：
轻应用平台不再支持创建直达号，如需开通直达号请登录<http://zhida.baidu.com>

创建工作

* 应用名称: CasdoorTest 11/32

传统接入扩展: 合作网站

解决方案: 使用BAE

创建

在创建应用程序后，应在以下位置设置重定向URL：

Casdoor

基本信息

接入类型 —————

其他应用

开发者服务 ————— ✎

Oauth2.0

安全设置

基本信息

名称: Casdoor

Icon: 

ID: 25547043

API Key: Hn'...yQmAp61

在以下位置添加您的 Casdoor 域名：

Casdoor

ID API Key Secret Key

基本信息

接入类型

其他应用

开发者服务

Oauth2.0

安全设置

安全设置

Implicit Grant授权方式 启用 禁用

授权回调页:

不配置OAuth授权回调地址，会存在用户授权信息被窃取风险，强烈建议配置该项。授权回调地址的校验规则请参考：[帮助文档](#)

根域名绑定: door.casbin.com

应用服务器IP地址:

应用在访问OpenAPI时须带有Referer信息，且其域名被限制在“根域名绑定”的设置项中

15/255

限制访问OpenAPI的Referer

0/500

同时绑定访问OpenAPI服务器IP

确定 取消

⚠ 注意事项

这部分与百度文档中提供的信息有很大的不同：

1. 将URL添加到回调URL设置中很可能导致URL验证失败，并导致登录失败，因此我们将我们的域名添加到域设置中。
2. 只能添加一个URL或域名，这与文档中的描述非常不同。

然后，您可以获取 `Client ID` 和 `Client Secrets`。

基本信息

名称: Casdoor

Icon:

ID: [redacted]

Client ID API Key: HnhK7...QmAp61

Client Secret Secret Key: DTgBZ...ls1bLm1Gha 重置

创建时间: 2022-01-22 16:20:05

更新时间: 2022-01-23 15:45:06

在您的Casdoor中添加一个百度OAuth提供商，并填写 **Client ID** 和 **Client Secrets**。

casbin

Home Organizations Users Roles Permissions Providers Applications Resources Tokens

Edit Provider Save Save & Exit

Name: Baidu

Display name: Baidu

Category: OAuth

Type: Baidu

Client ID: HsM...nWT

Client secret: ***

Provider URL: https://github.com/organizations/xxx/settings/applications/1234567

Save Save & Exit

现在您可以使用百度作为第三方服务来完成身份验证！

① 一般故障排除

如果你遇到百度提示说你的重定向URL是错误的，以下是一些可能的解决方法：

1. 将您的域名添加到适当的位置，然后重置Secret（百度重置Secret有一个bug，它会提示您一个错误，但刷新页面后Secret已经被刷新）。
2. 如果以上方法都不能解决问题，我们建议您删除应用程序并创建一个新的应用程序，并先设置您的域名。

另一个问题是，百度返回的用户名被掩码处理，这与他们的文档显示的用户名和显示名称不同。因此，我们目前只能使用掩码名称作为用户名。

Infoflow

要设置Infoflow OAuth提供商，请按照以下步骤操作：

1. 请前往[信息流{:target="_blank"}并使用您的信息流账户登录。](#)
2. 访问[信息流应用{:target="_blank"}页面。](#)

如流 Infoflow

首页 通讯录 应用中心 数据统计 设置

应用(5)

新建应用 应用分组/排序 应用宣传栏

3. 注册您的Infoflow应用。

返回 Casdoor 基本信息 保存 取消

应用logo: 建议使用640*640, 2M以内的jpg、png图片

应用名称: Casdoor

应用介绍: Casdoor单点登录系统

功能:

应用 (在客户端应用面板中, 为用户提供访问内部系统的入口, [查看客户端示例](#))

机器人 (在企业群聊中, 为用户提供机器人服务, [查看客户端示例](#))

服务号 (以双人会话方式, 为用户提供交流服务, [查看客户端示例](#))

4. 获取AgentID。

< 返回

Casdoor

| 基本信息

应用logo:



应用名称: Casdoor

应用介绍: Casdoor单点登录系统

功能: 应用

AgentID

应用ID: 55

5. 导航至设置选项卡并创建一个新的管理组。

6. 将您的结构添加到地址簿权限，并赋予它必要的权限。另外，将您刚刚创建的应用添加到指定位置。

通讯录权限

修改

组织架构

查看

管理 ?

对部门仅有查看权限时，只可查看被授权的成员资料信息；对部门有管理权限时，可查看成员的所有资料信息

成员ID

姓名

部门

头像

手机号

邮箱

登录帐号

应用权限

修改

应用权限

发消息

配置应用

Casdoor



7. 按照所示添加敏感接口权限。

敏感接口权限

修改

接口名称	权限开放
获取部门成员	<input checked="" type="checkbox"/>
获取部门列表	<input type="checkbox"/>
获取成员信息	<input checked="" type="checkbox"/>
获取标签成员	<input type="checkbox"/>
维护通信录	<input type="checkbox"/>
获取成员群组列表	<input type="checkbox"/>
获取群组成员列表	<input type="checkbox"/>
维护群组成员	<input type="checkbox"/>
发送群组消息	<input type="checkbox"/>
维护群组话题	<input type="checkbox"/>
维护勋章	<input type="checkbox"/>
通讯录搜索	<input type="checkbox"/>

8. 在同一页面上，你会找到 `CorpID` 和 `Secret`。

开发者凭据

Client ID

CorpID	hir...1
Secret	HgH...NB
Client Secret	

9. 在Casdoor中添加一个Infoflow OAuth提供商，并填写 Client ID、Client Secret 和 Agent ID。

Edit Provider Save Save & Exit

Name ② :	Infoflow
Display name ② :	Infoflow
Category ② :	OAuth
Type ② :	Infoflow
Sub type ② :	Internal
Client ID ②	CorpID
Client secret ②	Secret
Agent ID ② :	AgentID

您现在可以将Infoflow用作第三方服务进行身份验证。

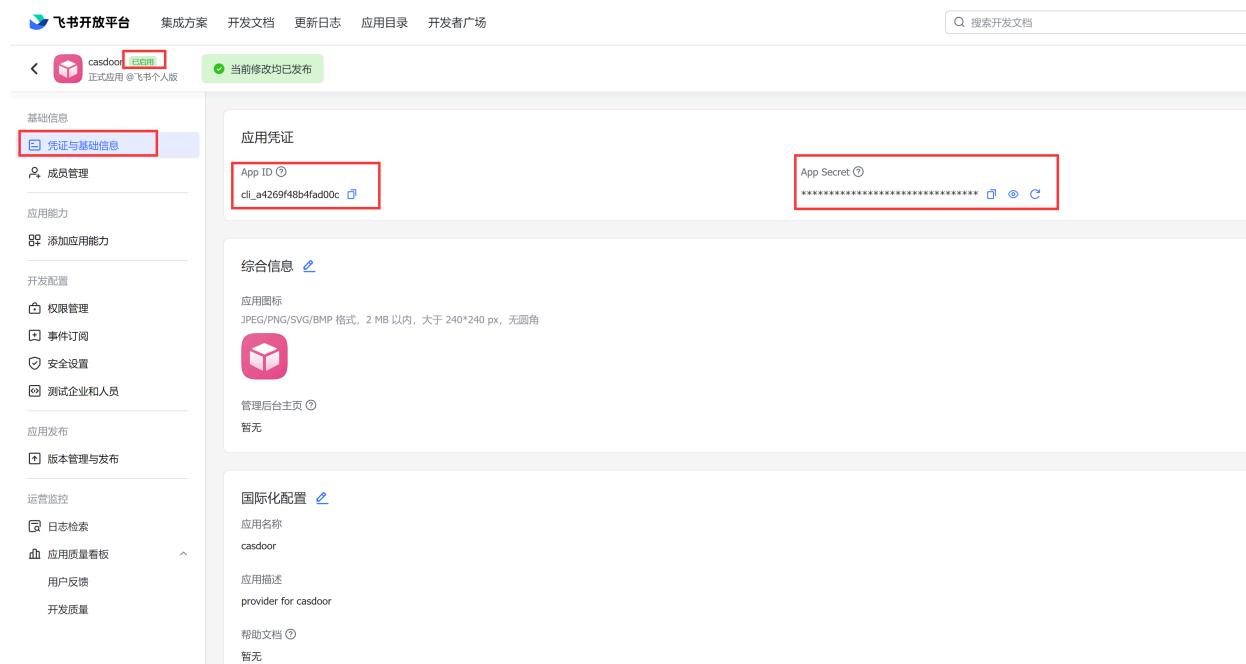
Lark

① 备注

这是一个如何配置Lark OAuth提供商的示例。

步骤1：创建一个Lark应用程序

首先，您需要在[Lark开放平台](#)上创建一个新的应用程序并启用它。 您可以在应用程序的基本信息中找到App ID和App Secret。



The screenshot shows the Lark Open Platform application configuration interface. On the left is a sidebar with various settings like basic information, application capabilities, development configuration, monitoring, and logs. The main panel shows the application details for 'casdoor'. The '凭证与基础信息' tab is selected, highlighting the '凭证' section. It displays the 'App ID' (cl_a4269f48b4fad00c) and 'App Secret' (a series of asterisks). Both fields are highlighted with red boxes.

接下来，在您的应用程序的安全设置中添加重定向URL `<your-casdoor-domain>/callback`（例如，<http://localhost:7001/callback>）。

The screenshot shows the Feishu Open Platform developer console interface. On the left, there is a sidebar with various application management options. The '安全设置' (Security Settings) option is highlighted with a red box. The main content area is titled '重定向 URL IP 白名单' (Redirection URL IP Whitelist). It contains two sections: '重定向 URL' (Redirection URL) and 'IP 白名单' (IP Whitelist). In the '重定向 URL' section, a URL 'http://localhost:7001/callback' is listed with '添加' (Add) and '批量修改' (Batch Modify) buttons. In the 'IP 白名单' section, there is a note about enabling it for API calls. A '添加' (Add) button is present here as well. On the right side of the main content area, there are '操作' (Operations) buttons for editing and deleting, and a '技术支持' (Technical Support) button.

步骤2：创建一个Lark OAuth提供商

现在在Casdoor中创建一个Lark OAuth提供商。 填写必要的信息。

名称	Lark中的名称
Category	Choose OAuth
Type	Choose Lark
Client ID	App ID obtained from Step 1
Client secret	App Secret obtained from Step 1

The screenshot shows two side-by-side interfaces. On the left is the 'Edit Provider' form in Casdoor, where 'lark' is selected as the provider type. On the right is the Feishu Open Platform application configuration page, showing the 'App ID' and 'App Secret' fields. Red arrows indicate the mapping between the 'Client ID' and 'Client secret' fields in Casdoor and the corresponding fields in the Feishu application configuration.

现在您可以使用Lark作为第三方服务来完成身份验证。

Username Handling

Casdoor uses a fallback mechanism to ensure user accounts are created successfully even when Lark's OAuth response has incomplete data. The username field follows this priority:

1. UserId - Primary identifier used when available
2. UnionId - Links users across multiple Lark organizations
3. OpenId - Always present, used as final fallback

This ensures authentication succeeds reliably since OpenId is guaranteed in Lark's OAuth response.

电子邮箱

概述

使用电子邮件进行身份验证

SendGrid

Using SendGrid as an Email Provider

Azure ACS

使用Azure ACS作为电子邮件提供商

Brevo

使用 Brevo 作为SMTP 服务器

 **MailHog**

使用MailHog作为SMTP服务器

 **Mailpit**

Using Mailpit as the SMTP server

概述

Adding an Email provider

1. Click on **Add** to add a new provider.
2. Select **Email** under the **Category** section.

Name  :	email provider
Display name  :	My Email
Category  :	Email
Type  :	Default

3. Fill in the fields for **Username**, **Password**, **Host**, and **Port** for your SMTP service.

Username ?	no-reply@casbin.com
Password ?	***
Host ? :	smtp.qiye.aliyun.com
Port ? :	465

4. Customize the `Email Title` and `Email Content`, then save the changes.

Proxy configuration

If your server cannot directly access the SMTP service (such as Gmail), you can enable the proxy option. When enabled, email traffic will be routed through the SOCKS5 proxy configured in Casdoor's configuration file.

To enable proxy support, toggle the `Enable proxy` switch in the provider settings. This is particularly useful when connecting to external email services from restricted network environments.

Modify email content

You can use the following placeholders to display some variables.

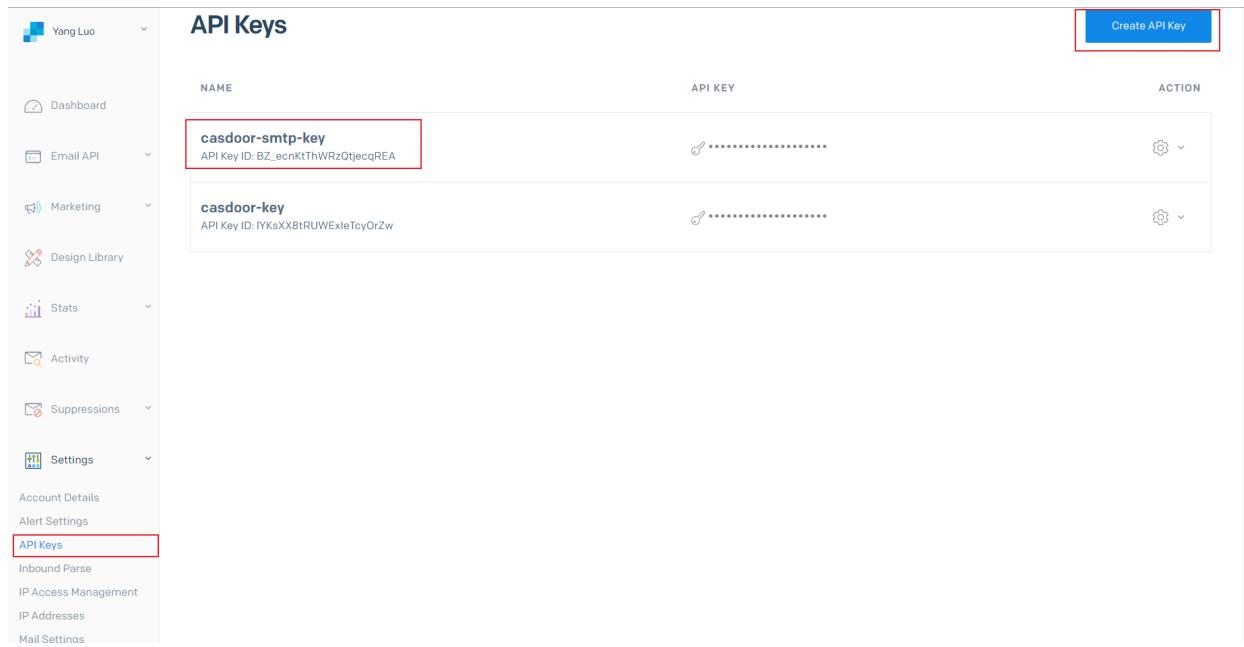
1. `%{user.friendlyName}` is the Display name of user.
2. `%link` is the reset link for forget password function. (You should put `%link` in the `<reset-link></reset-link>` label)

SendGrid

In this guide, we will use SendGrid as an email provider.

Step 1: Create an API Key for Your SendGrid Account

Expand **Settings** from the left navigation bar, then click on **API Keys**. Here, you will see all previously generated API keys. To create a new one, click on **Create API Key** and configure the necessary permissions.



The screenshot shows the SendGrid dashboard with the 'API Keys' page open. On the left, there's a sidebar with various navigation options like Dashboard, Email API, Marketing, Design Library, Stats, Activity, Suppressions, Settings, and several account-specific sections. The 'API Keys' option is highlighted with a red box. The main area displays a table of API keys:

NAME	API KEY	ACTION
casdoor-smtp-key API Key ID: BZ_ecnKtThWRzQtjecdREA	copy ······	⚙️ 🔍
casdoor-key API Key ID: IYKsXX8tRUWExleTcyOrZw	copy ······	⚙️ 🔍

A red box also highlights the 'Create API Key' button at the top right of the table area.

Step 2: Sender Verification

To verify your email sender, choose between Single Sender Verification or Domain Authentication by referring to the official documentation:

[Sender Identity](#)

Step 3: Configure Casdoor as an Email Provider

Create a SendGrid email provider in Casdoor and fill in the following fields:

Required Fields

Field	Description
Secret Key	Your SendGrid API key
发件人地址	Your verified email address (or domain)

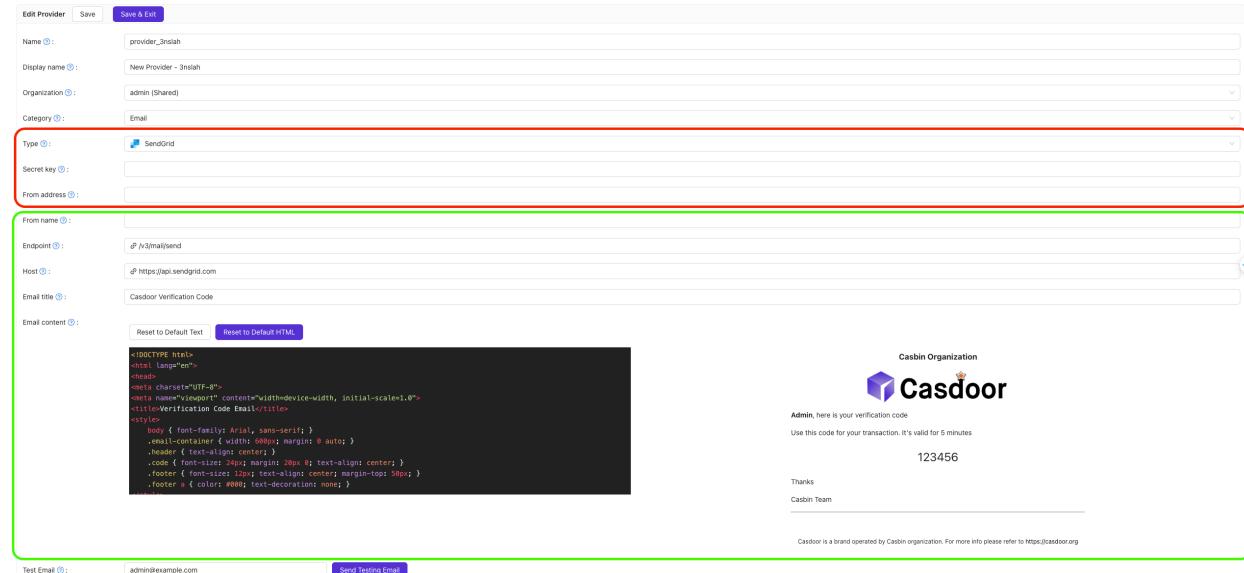
Default Fields

Field	Description
Endpoint	Default: /v3/mail/send

Field	Description
主机	Default: <code>https://api.sendgrid.com</code>

Email Fields

Field	Description
From Name	The display name of the email sender
Email Title	The subject of the email
Email Content	Supports HTML templates
Test Email	The recipient's email address for testing



Provider Configuration (SendGrid)

Name: provider_3instah
Display name: New Provider - 3instah
Organization: admin (Shared)
Category: Email

Type: SendGrid
Secret key:
From address:

From name:
Endpoint: `/v3/mail/send`
Host: `https://api.sendgrid.com`
Email title: Casdoor Verification Code
Email content:

```

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Verification Code Email</title>
<style>
body { font-family: Arial, sans-serif; }
.messageContainer { width: 600px; margin: 0 auto; }
.header { text-align: center; }
.code { font-size: 24px; margin: 20px 0; text-align: center; }
.footer { font-size: 12px; text-align: center; margin-top: 50px; }
.footer a { color: #000; text-decoration: none; }

```

Test Email: admin@example.com
Send Testing Email

Casbin Organization
Casdoor
Admin, here is your verification code
Use this code for your transaction. It's valid for 5 minutes
123456
Thanks
Casdoor Team

Casdoor is a brand operated by Casbin organization. For more info please refer to <https://casdoor.org>

Finally, click on the **Send Testing Email** button and check your **Test Email** address for the test email.

Azure ACS

在本指南中，我们将使用ACS作为电子邮件提供商。

步骤1：配置ACS

按照下面的文档完成配置。

- [创建和管理电子邮件通信服务](#)
- [获取一个免费的Azure托管域或添加一个自定义域](#)
- [连接域](#)

复制你的 `Endpoint` 和 `Private Key` 以供使用

The screenshot shows the Azure portal interface for managing access keys. On the left, there's a sidebar with various service icons and a 'Keys' tab which is currently selected. The main area displays the 'casdoor' communication service settings. Under the 'Keys' section, there are two sets of fields: 'Primary key' and 'Secondary key'. Each set includes a 'Key' input field (which is redacted here) and a 'Connection string' input field (also redacted). Above these fields, there are 'Regenerate primary key' and 'Regenerate secondary key' buttons, along with 'Show values' links. A note at the top of the page says: 'Use access keys to authorize your API calls when you use the Communication Services SDKs. Store your access keys securely – for example, using Azure Key Vault – and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connects using one key while regenerating the other.' The 'Endpoint' field is explicitly highlighted with a red box.

步骤2：配置Casdoor电子邮件提供商

现在在Casdoor中创建一个电子邮件提供商，填写必要的信息。字段与Azure ACS之间

的关系如下：

① 备注

From Address 必须是一个经过验证的电子邮件域。

名称	在Azure ACS中的名称
发件人地址	
密钥	私钥
主机	端点

Name ⓘ :

Display name ⓘ :

Organization ⓘ :

Category ⓘ :

Type ⓘ :  Azure ACS

Secret key ⓘ :

From address ⓘ :

Host ⓘ :

Email title ⓘ :

Email content ⓘ :

Test Email ⓘ :

Provider URL ⓘ :

Brevo

在本指南中，我们将使用 Brevo 作为SMTP 服务器。

第 1 步：请求激活您的 Brevo SMTP 帐户

请参阅文档以激活 Brevo SMTP: [发送交易电子邮件使用Brevo SMTP](#)

在我的案例下，当我创建一个工单来激活我的smtp帐户时，我得到了这个答复：



Rafael Guimaraes

Last Response: 2 days ago



Hi there,

Thank you for reaching out!

I've activated your account's SMTP/Transactional capabilities.

You can find your account's SMTP credentials by clicking [here](#).

To get you started, I'll include some useful links about our SMTP/Transactional services:

- [Our complete library of help articles related to SMTP](#)
- [Troubleshooting common issues with SMTP](#)

The SMTP port listed by default, Port 587, will be used without a secure connection. If you want to use a secure connection (SSL or TLS), please use Port 465.

Please be sure to let me know if you have more questions or if you need any help.

Best regards,

步骤 2: 获取 Brevo SMTP 配置

在你的 Brevo 看板中, 找到 SMTP&API, 查看 **SMTP 服务器**, **端口**, **登录**, **SMTP 验证 Key** 信息

第 3 步：配置 Casdoor 邮件提供商

在 Casdoor 中创建一个新的提供商。 填写必要的信息.

单击 **测试SMTP连接** 按钮。 如果您看到 **提供商：SMTP连接成功**, 这意味着您的 Casdoor 服务可以访问 Brevo 服务。

接下来，点击 **发送测试电子邮件** 按钮。 如果你看到**邮件发送成功**，意味着测试邮件已经成功的从**发件地址** 发送至 **测试接收邮箱**

MailHog

在本指南中，我们将使用MailHog作为SMTP服务器。MailHog是一个使用假SMTP服务器操作的电子邮件测试工具。

步骤1：部署MailHog服务

MailHog服务的IP地址是192.168.24.128，SMTP服务端口是1025。

```
http:// Binding to address: 0.0.0.0:8025
2023/07/13 03:06:43 Serving under http://0.0.0.0:8025/
Creating API v1 with WebPath:
Creating API v2 with WebPath:
[APIv1] KEEPALIVE /api/v1/events
[HTTP] Binding to address: 0.0.0.0:8025
Creating API v1 with WebPath:
Creating API v2 with WebPath:
2023/07/13 03:10:36 Using maildir message storage
2023/07/13 03:10:36 Maildir path is /tmp/mailhog641072855
2023/07/13 03:10:36 [SMTP] Binding to address: 0.0.0.0:1025
2023/07/13 03:10:36 Serving under http://0.0.0.0:1025/
[APIv2] GET /api/v2/jim
[APIv2] GET /api/v2/messages
2023/07/13 03:10:50 [HTTP] Connection closed by client: 127.0.0.1:641072855
```

步骤2：创建电子邮件提供商

提供必要的信息并保存设置。

Category ? :	Email
Type ? :	Default
Username ? :	
Password ? :	
From address ? :	notification@casdoor.com
From name ? :	Casdoor Notification
Host ? :	192.168.24.128
Port ? :	1025
Disable SSL ? :	<input checked="" type="checkbox"/>
Email title ? :	Casdoor Verification Code (Test)
Email content ? :	You have requested a verification code at Casdoor (Test) . Here is your code: <u>%s</u> , please enter in 5 minutes.
Test Email ? :	admin@example.com
	Test SMTP Connection
	Send Testing Email
Save	Save & Exit

步骤3：发送测试电子邮件

首先，点击[测试SMTP连接](#)按钮。如果你看到[provider: SMTP connected successfully](#)，这意味着你的Casdoor服务可以访问MailHog服务。

接下来，点击[发送测试电子邮件](#)按钮。如果你看到[电子邮件发送成功](#)，这意味着测试电子邮件已经从[From](#)地址成功发送到[测试电子邮件](#)。

Name ?: email_provider provider:SMTP connected successfully

Display name ?: Email Provider Email sent successfully

Organization ?: admin (Shared)

Category ?: Email

Type ?: Default

Username ?:

Password ?:

From address ?: notification@casdoor.com

From name ?: Casdoor Notification

Host ?: 192.168.24.128

Port ?: 1025

Disable SSL ?:

Email title ?: Casdoor Verification Code (Test)

Email content ?: You have requested a verification code at Casdoor (Test). Here is your code: 123456, please enter in 5 minutes.

Test Email ?: admin@example.com **Test SMTP Connection** **Send Testing Email**

Provider URL ?: <https://github.com/organizations/xxx/settings/applications/1234567>

 MailHog

Connected

Inbox (4)

From "Casdoor Notification" <notification@casdoor.com>
Subject Casdoor Verification Code (Test)
To admin@example.com

HTML Plain text Source

Jim
Jim is a chaos monkey.
[Find out more at GitHub.](#)

[Enable Jim](#)

You have requested a verification code at Casdoor (Test). Here is your code: 123456, please enter in 5 minutes.

Mailpit

Mailpit

In this guide, we will be using Mailpit as the SMTP server. [Mailpit](#) is an email-testing tool that operates with a fake SMTP server.

Step 1: Deploy the Mailpit service

The IP address for the Mailpit service is `127.0.0.1`. By default, the Mailpit SMTP server listens on port 1025 and does not use encryption or authentication.

```
> { home } * mailpit.exe
time="2025/07/19 16:13:51" level=info msg="[smtpd] starting on [::]:1025 (no encryption)"
time="2025/07/19 16:13:51" level=info msg="[http] starting on [::]:8025"
time="2025/07/19 16:13:51" level=info msg="[http] accessible via http://localhost:8025/"
```

Step 2: Create an email provider

Provide the necessary information and save the settings.

Edit Provider

Name ⓘ: mailpit

Display name ⓘ: mailpit

Organization ⓘ: admin (Shared)

Category ⓘ: Email

Type ⓘ:  Default

Username ⓘ:

Password ⓘ:

From address ⓘ: 2707138687@qq.com

From name ⓘ: attack825

Host ⓘ: 127.0.0.1

Port ⓘ: 1025

Disable SSL ⓘ:

Step 3: Send a test email

First, click on the button. If you see , it means that your Casdoor service can access the Mailpit service.

Next, click on the button. If you see , it means that the test email has been sent successfully from the address to the .

Test Email ⓘ:

Provider URL ⓘ:

Mailpit

Mark unread Delete Download ▶ ▷

Return to inbox

From: attack825 <2707138687@qq.com>
To: <admin@example.com>
Subject: Casdoor Verification Code
Date: Sat, 19 Jul 2025, 4:37 pm (1.7 kB)
Tags: Add tags...

attack825 5 minutes ago
To: admin@example.com
Casdoor Verification Code

attack825 13 minutes ago
To: 2707138687@qq.co
Casdoor Verification Code

attack825 15 minutes ago
To: 2707138687@qq.co
Casdoor Verification Code

attack825 17 minutes ago
To: admin@example.com
Casdoor Verification Code

sender@example.com 29 minutes ago
To: recipient@example.com
Email Subject

HTML HTML Source Text Headers Raw HTML Check 91% Link Check

Casbin Organization

 Casdoor

Admin, here is your verification code
Use this code for your transaction. It's valid for 5 minutes
123456

Thanks
Casbin Team

Casdoor is a brand operated by Casbin organization. For more info please refer to <https://casdoor.org>

短信

概述

使用短信进行身份验证

Twilio

使用Twilio作为Casdoor的SMS提供商

Amazon SNS

使用Amazon SNS作为Casdoor的SMS提供商

Azure ACS

使用ACS作为Casdoor的SMS提供商

 阿里云

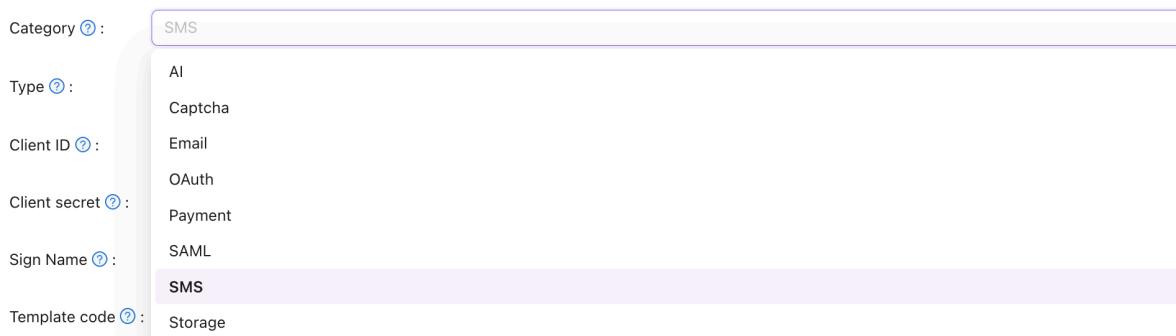
将阿里云作为Casdoor的短信提供商

概述

We use [casdoor/go-sms-sender](#) to send SMS for Casdoor. The `go-sms-sender` library currently supports Twilio, Submail, SmsBao, Alibaba Cloud, Tencent Cloud, Huawei Cloud, and Volc SMS APIs. If you want to add support for other SMS providers, you can either raise an issue or submit a pull request.

Adding an SMS provider

1. 点击 `添加` 来添加一个新的提供商。
2. 在 `类别` 部分选择 `短信`。



3. 选择你的提供商的类型。

Category [?](#): SMS

Type [?](#): Aliyun SMS

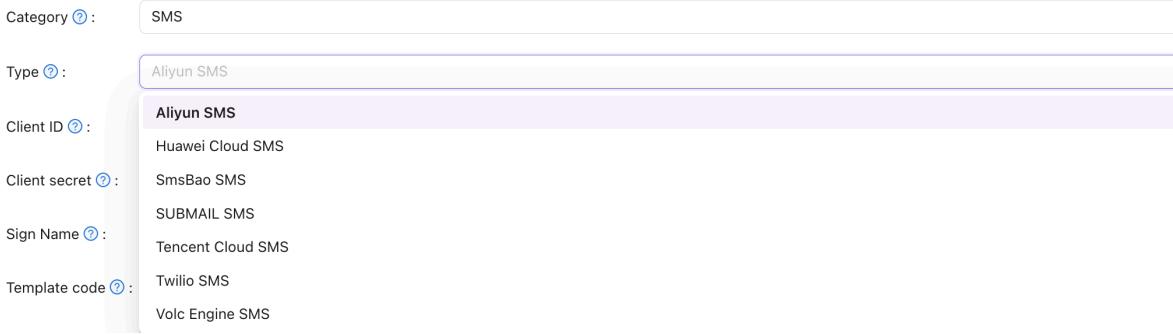
Client ID [?](#):

- Aliyun SMS
- Huawei Cloud SMS
- SmsBao SMS
- SUBMAIL SMS
- Tencent Cloud SMS
- Twilio SMS
- Volc Engine SMS

Client secret [?](#):

Sign Name [?](#):

Template code [?](#):



4. 从你的短信提供商处获取必要的信息，并填写相应的字段。

Proxy configuration

For SMS providers that use HTTP APIs (such as Custom HTTP SMS), you can enable proxy support if your server cannot directly access the SMS service. When enabled, SMS traffic will be routed through the SOCKS5 proxy configured in Casdoor's configuration file.

To enable proxy support, toggle the `Enable proxy` switch in the provider settings. This option is available for Custom HTTP SMS providers and helps when operating in restricted network environments.

Twilio

在Casdoor中填写必要的信息

有四个必填字段：[客户端ID](#)，[客户端密钥](#)，[发送者号码](#)和[模板代码](#)。与Twilio帐户的对应关系如下：

名称	Twilio中的名称	必填
Client ID	Account SID	必填
Client secret	Auth Token	必填
Sender number	Twilio电话号码	必填
Template code		必填

Twilio信息

- 帐户SID，授权令牌和Twilio电话号码

Step 4: invite and upgrade

The screenshot shows the Twilio developer console interface. On the left, there's a sidebar with 'Develop' selected. Below it are links for Phone Numbers, Messaging, Studio, Verify, and Video. A 'Explore Products' section is also present. The main content area is titled 'Step 4: invite and upgrade'. It includes sections for 'Invite teammates' (with a button to 'Invite teammates') and 'Upgrade your account' (with a 'Upgrade' button). Below these are sections for 'Account Info' (containing fields for Account SID, Auth Token, and My Twilio phone number) and 'Helpful links' (with links to 'How does Twilio work?', 'SMS Quickstart guides', and 'Support help center'). A 'Show' button is visible next to the Auth Token field.

配置Casdoor提供商

您可以根据您的需求配置**模板代码**，然后在**SMS测试**中输入您的电话号码进行测试。

Name <small>②</small> :	twilio
Display name <small>②</small> :	twilio
Organization <small>②</small> :	admin (Shared)
Category <small>②</small> :	SMS
Type <small>②</small> :	Twilio SMS
Client ID <small>②</small> :	AC06b73d65c8ee67ce8e448edcc64b6ec6
Client secret <small>②</small> :	***
Sender number <small>②</small> :	+12186751069
Template code <small>②</small> :	get the message
SMS Test <small>②</small> :	+1 <small>▼</small> <input type="text" value="Input your phone num..."/> <input type="button" value="Send Testing SMS"/>
Provider URL <small>②</small> :	<input type="text" value=""/>

Amazon SNS

在Amazon中获取必要的信息

有四个必填字段: Access Key, Secret Access Key, Region 和 Template code。我将向您展示如何从Amazon SNS获取此信息。

- Access Key和Secret Access Key

在身份和访问管理 (IAM) 中, 您可以创建一个Access Key和Secret Access Key。

The screenshot shows two parts of the AWS IAM console. On the left, the 'Identity and Access Management (IAM)' navigation pane is visible with options like Dashboard, Access management, and Access reports. The 'Access management' section is expanded, showing 'Access keys (1)' and 'CloudFront key pairs (0)'. The 'Access keys' section displays a table with one row:

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
AKIAYOMMXHVZLH4LYKGL	16 days ago	None	N/A	N/A	Active

The 'CloudFront key pairs' section shows a table with one entry: 'No CloudFront key pairs'.

- 区域

Region 与您创建的主题有关。

The screenshot shows the AWS Amazon SNS Dashboard. On the left, there's a sidebar with 'Amazon SNS' at the top, followed by 'Dashboard', 'Topics', 'Subscriptions', and a 'Mobile' section with 'Push notifications', 'Text messaging (SMS)', and 'Origination numbers'. The main area is titled 'Dashboard' and shows a summary: 'Resources for ap-southeast-1'. It displays 1 Topic, 0 Platform applications, and 0 Subscriptions. Below this, there's a section titled 'Overview of Amazon SNS' with a sub-section 'Application-to-application (A2A)' which describes Amazon SNS as a managed messaging service for decoupling publishers from subscribers.

配置Casdoor提供商

Template code 是您想要发送的消息。在 SMS Test 中输入您的电话号码进行测试。

Name ② : amazon_sns

Display name ② : amazon_sns

Organization ② : admin (Shared)

Category ② : SMS

Type ② : Amazon SNS

Access key ② : AKIAYOMMXHVZACW5RFMX

Secret access key ② : ***

Region ② : ap-southeast-1

Template code ② : enter the message you want to send

SMS Test ② : +1 Input your phone num...

Provider URL ② : <https://github.com/organizations/xxx/settings/applications/1234567>

Azure ACS

在Azure中获取必要的信息

有四个必填字段：客户端密钥，发送者号码，模板代码和提供商Url。我将向你展示如何从Azure ACS获取这些信息。

- 客户端密钥

在通信服务中，你可以创建一个用户访问令牌，这就是Casdoor中的客户端密钥。

The screenshot shows the Azure Communication Services - casdoor Identity & User Access Tokens page. The URL is [https://communication.azure.com/CommunicationServices/casdoor/IdentitiesAndUserAccessTokens](#). The page title is "casdoor | Identities & User Access Tokens". On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Quick start, Sample applications, Events, Settings, Keys, and a selected tab: Identities & User Access Tokens. Under the "Identity" section, there's a "Generate" button and two text input fields: "Identity" containing "8:acs:7f19cba5-66d0-4194-b061-1e1a3ac6d68c_0000001a-6b97-e8f5-2c8a-08482200600c" and "User Access token" containing "eyJhbGciOiJSUzI1NiIsImtpZCI6IjVFDQ4MjE0Qzc3MDczQUU1QzJCREU1Q0NENTQ0ODIiREYyQzRDODQjLCJ4NXQiOiJyb1NDRk1kd2M2N...". A note below says "User Access Tokens let your client applications authenticate directly against Azure Communication Services. Easily generate User Access tokens for trying ACS features. Identities generated are kept permanently." The "Services" section has checkboxes for "Voice and video calling (VOIP)" and "Chat", both of which are checked.

- 发送者号码

发送者号码是你在通信服务中创建的电话号码。

Communication Service

Search (Cmd+/) Get Port Release Give feedback

LOCKS

Tools

- Keys
- Identities & User Access Tokens
- Push notifications

Voice Calling - PSTN

- # Phone numbers
- Direct routing (Preview)

SMS

- Short Codes (Preview)

Monitoring

- Insights (preview)
- Metrics
- Diagnostic settings
- Logs

	Number	Status	Cost (monthly)
<input checked="" type="checkbox"/>	1-833-920-3625 	Active	\$2

- 提供商Url

提供商Url是通信服务中的端点。

Communication Service

Search (Cmd+/) Move Delete Give feedback

Overview

Activity log Resource group (move) : casdoor

Access control (IAM) Status : Active

Tags Location : Global

Diagnose and solve problems Subscription (move) : 免费试用

Quick start Subscription ID : e054e27a-96e8-4cca-a1cf-32717dcd303c 

Sample applications Tags (edit) : Add tags

Events

Settings

- Keys
- Identities & User Access Tokens

Endpoint : <https://casdoor.unitedstates.communication.azure.com>
 Data location : United States
 Manage keys : [Click here to manage keys](#)

Build engaging communication experiences at scale

Azure Communication Services brings rich communication APIs to all of your apps across any device, on any platform, using the same reliable and secure infrastructure that powers Microsoft Teams.

[Learn more](#)

配置Casdoor提供商

模板代码就是你想发送的消息。在SMS测试中输入你的电话号码进行测试。

Name ? :	azure_acs
Display name ? :	azure_acs
Organization ? :	admin (Shared)
Category ? :	SMS
Type ? :	 Azure ACS
Client ID ? :	
Client secret ? :	***
Sender number ? :	+18339203625
Template code ? :	enter the message you want to send
SMS Test ? :	+1 <input type="button" value="▼"/> Input your phone num... <input type="button" value="Send Testing SMS"/>
Provider URL ? :	https://casdoor.unitedstates.communication.azure.com

阿里云

在Casdoor中填写必要的信息

有四个必填字段：[客户端ID](#)，[客户端秘密](#)，[签名名称](#)，和[模板代码](#)。与阿里云账户的对应关系如下：

名称	在阿里巴巴中的名称	是必需的
Client ID	AccessKey ID	必需的
Client secret	AccessKey Secret	必需的
Sign Name	Signature	必需的
Template code	Template code	必需的

阿里巴巴信息

- AccessKey ID和AccessKey Secret

登录我的阿里云工作台后，我点击“AccessKey”创建ID和Secret。

The screenshot shows the Alibaba Cloud SMS service interface. At the top, there's a search bar and navigation links for '费用' (Cost), '工单' (Work Orders), 'ICP 备案' (ICP Registration), '企业' (Enterprise), '支持' (Support), 'App', and '帮助中心'. A user profile icon is also present. Below the header, a banner reads '【有奖调研】阿里云短信服务易用性有奖调研' (SMS Service Usability Survey) with a '点击进入' (Click to Enter) button. The main content area has tabs for '新手引导' (Newbie Guide), 'OpenAPI 开发者门户' (OpenAPI Developer Portal), '开发者指南' (Developer Guide), and 'AccessKey' (highlighted with a red oval). On the left, a sidebar shows '发送量数据' (Delivery Volume Data) and '用户状态/类型: 正常 / 个人用户' (User Status/Type: Normal / Individual User). The center features a '快速上手短信服务, 从这里开始!' (Get started with SMS service here!) section with a progress bar indicating 20% completion. A blue button says '快速学习短信服务' (Quickly learn about SMS service). To the right, there are sections for '用户监控信息' (User Monitoring Information), '快捷操作入口' (Quick Operation Entry), and '国内消息' (Domestic Messages). A summary table shows existing resources: 0 short message signatures, 0 short message templates, and 0 group message tasks. Buttons for '添加签名' (Add Signature), '添加模板' (Add Template), and '提交发送任务' (Submit Delivery Task) are available. At the bottom, there's a '国际/港澳台消息' (International/Hong Kong/Macau/Taiwan Messages) section.

通过创建AccessKey，我获得了我的AccessKey ID和AccessKey Secret:

The screenshot shows the Alibaba Cloud security management interface under the '安全信息管理' (Security Information Management) section. It displays a table for '用户 AccessKey' (User AccessKey). The columns are 'AccessKey ID', 'AccessKey Secret', '状态' (Status), '最后使用时间' (Last Used Time), '创建时间' (Creation Time), and '操作' (Operations). One row is shown: 'LTAI4Fy4mVoMjAzC95rt5Wh7' with '显示' (Visible) status, '启用' (Enabled) status, '2020年7月19日 20:24:58' (Last Used Time), '2020年7月11日 17:52:50' (Creation Time), and buttons for '禁用' (Disable) and '删除' (Delete). A note at the top of the page states: '① AccessKey ID和AccessKey Secret是您访问阿里云API的密钥, 具有该账户完全的权限, 请您妥善保管,' (① AccessKey ID and AccessKey Secret are your keys to access Alibaba Cloud API, they have full permissions for the account, please keep them safe).

- 签名

The screenshot shows the Alibaba Cloud signature management interface. The left sidebar includes 'Go China', 'Go Globe', 'Analytics', 'Dashboard', 'Delivery Report', 'Messaging Logs', 'Bills', 'Resource Plan Usage', 'Short URL Statistics', 'System Configurations', and 'General Settings'. The main area has a QR code with the text 'Join the group chat to try new features.' and a large blue bird icon. A note below the QR code states: 'Alibaba Cloud SMS prohibits illegal content such as illegal financial marketing, gambling, fraud, obscenity, pornography, and violence in a message. If you send a message that contains illegal content, Alibaba Cloud will suspend your service and account according to Short Message Service Terms of Service. If your message is against the law, Alibaba Cloud will transfer evidences to the police, including but not limited to the personal information authenticated in Alibaba Cloud.' The 'Signatures' tab is selected, showing a table with columns: 'Create Signature', 'Select a review status', 'Search by signature', 'Actions', 'Signature', 'Ticket ID', 'Scenario', 'Review Status', and 'Created At'. One row is shown: 'casdoor 测' (casdoor test) with 'General' scenario, 'Approved' status, and '2023-07-26 13:15:49' creation time. Buttons for 'Export Records' and 'Export' are at the top right. A note at the bottom of the table area says: 'Generally, signatures are reviewed within 2 hours. Enterprise or institution signatures are reviewed within 2 business days. Recently, a review process took about 1 hour on average. More time may be required due to system upgrades or workload spikes. Business hours: Signatures are reviewed from 9:00 to 21:00 (UTC+8) every day, excluding statutory holidays. Thanks for your cooperation.'

- 模板代码

Short Message Service

- Overview
- Quick Start & Delivery Test
- Go China**
- Go Globe
- Analytics
- Dashboard
- Delivery Report
- Messaging Logs
- Bills
- Resource Plan Usage
- Short URL Statistics
- System Configurations
- General Settings
- Domestic SMS Settings

Create Dedicated DingTalk Group Chat



Scan the QR code to create your dedicated DingTalk group chat.
You can use the group chat to submit and modify signatures and message templates, and check whether the signatures and message templates are reviewed.

Alibaba Cloud SMS prohibits illegal content such as illegal financial marketing, gambling, fraud, obscenity, pornography, and violence in a message. If you send Alibaba Cloud will suspend your service and account according to Short Message Service Terms of Service. If your message is against the law, Alibaba Cloud will not be limited to the personal information authenticated in Alibaba Cloud.

Message Templates

Signatures **Message Templates** Mass Messaging

1. Generally, signatures are reviewed within 2 hours. Recently, a review process took about **1 hour** on average. More time may be required due to system up hours: Signatures are reviewed from 9:00 to 21:00 (UTC+8) every day, excluding statutory holidays. Thanks for your cooperation.
2. Message templates provided by Alibaba Cloud SMS do not require submission for approval. However, you are still charged for message delivery.

Create Message Template	Select a template type	Select a review status	Search by message template name	Tag	Ticket ID	Template Code	Template Type	Created At
					20020389144	SMS_462155126	Verification Code Message	2023-07-26 17:54:00

配置Casdoor提供商

在**短信测试**字段中输入您的电话号码进行测试。

Name ② :	alibaba		
Display name ② :	alibaba		
Organization ② :	admin (Shared)		
Category ② :	SMS		
Type ② :	Aliyun SMS		
Client ID ② :	LTAI5tFwxoA51CnSiQFyyPU5		
Client secret ② :	***		
Sign Name ② :	casdoor		
Template code ② :	SMS_462155126		
SMS Test ② :	+86	Input your phone num...	Send Testing SMS
Provider URL ② :	🔗		

通知

概述

在您的应用程序中添加通知提供商

Telegram

使用Telegram作为Casdoor的通知提供者

自定义HTTP

使用自定义HTTP作为Casdoor的通知提供者

Slack

使用Slack作为Casdoor的通知提供者

Google Chat

使用Google Chat作为Casdoor的通知提供者

Twitter

将Twitter用作Casdoor的通知提供商

Discord

将Discord用作Casdoor的通知提供者

WeCom

Using WeCom as a notification provider for Casdoor

概述

Casdoor可以配置为使用各种通知提供商发送通知消息。

目前，Casdoor支持多个通知提供商。以下是Casdoor支持的提供商：

提供商	Logo
Telegram	
自定义HTTP	
Slack	
Google Chat	
Twitter	
Discord	
Bark	
DingTalk	

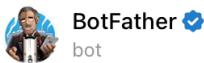
提供商	Logo
Lark	
Line	
Matrix	[matrix]
Microsoft Teams	
WeCom	
Pushbullet	
Pushover	
Reddit	
Rocket Chat	
Viber	
Webpush	

Telegram

步骤1：获取API令牌

首先，您需要在[Telegram](#)上创建一个账户。 创建账户后，您应该联系[BotFather](#)，这是一个用于创建其他机器人的机器人。

要创建您的机器人，使用命令[/newbot](#)：



Games

[/mygames](#) - edit your games
[/newgame](#) - create a new game
[/listgames](#) - get a list of your games
[/editgame](#) - edit a game
[/deletegame](#) - delete an existing game



usher
[/newbot](#)



BotFather

Alright, a new bot. How are we going to call it? Please choose a name for your bot.



usher
casdoor



BotFather

Good. Now let's choose a username for your bot. It must end in `bot`. Like this, for example: TetrisBot or tetris_bot.



usher
CasdoorBot



BotFather

Done! Congratulations on your new bot. You will find it at t.me/CasdoorBot. You can now add a description, about section and profile picture for your bot, see [/help](#) for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:

6531753859:AAEJV6-fopJLLyNa3mSn_H-dFIPO8VXwEto

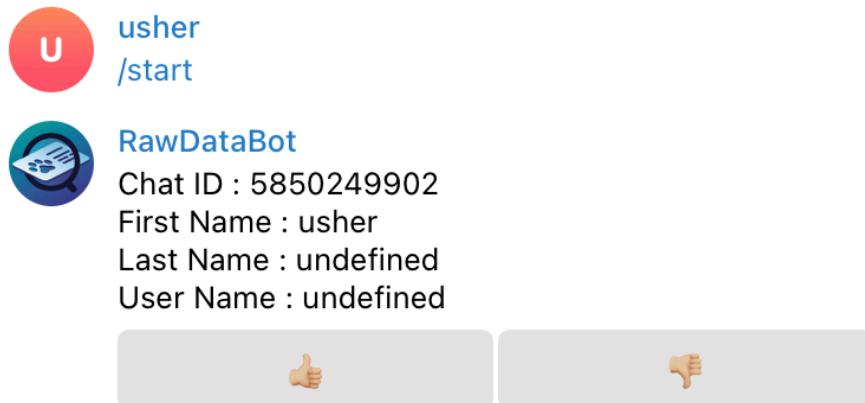
Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page: <https://core.telegram.org/bots/api>

您的机器人应该有两个属性：`name` 和 `username`。创建机器人后，您将收到一个 API 令牌。

步骤2：获取聊天ID

要找到您的聊天ID，请使用 [RawDataBot](#)。



步骤3：配置Casdoor Telegram提供者

有三个必填字段：`App Key`，`Content` 和 `Chat ID`。字段与 Telegram 之间的关系如下：

名称	在Telegram中的名称
Secret key	API Token
Chat ID	Chat ID

名称	在Telegram中的名称
Content	

Name ? : telegram

Display name ? : telegram

Organization ? : admin (Shared)

Category ? : Notification

Type ? :  Telegram

Secret key ? : ***

Content ? : test

Chat ID ? : 5850249902 Send Testing Notification

Provider URL ? : <https://github.com/organizations/xxx/settings/applications/1234567>

自定义HTTP

① 备注

Casdoor支持自定义HTTP通知提供者。您可以使用它向特定的HTTP地址发送消息。

配置Casdoor自定义HTTP提供者

有三个必填字段：**方法**，**参数名称**，**内容**和**聊天ID**。

名称	描述
方法	选择 GET 或 POST 方法。
参数名称	URL查询参数名称或主体参数，取决于 方法 。
内容	您想要发送的消息。
Endpoint	您的HTTP地址

Name ②:

Display name ②:

Organization ②:

Category ②:

Type ②: M

Method ②:

Parameter ②:

Content ②:

Endpoint ②: Send Testing Notification

Provider URL ②:

在我的示例中，当我点击发送通知消息时，我收到了这个请求：

```
Listening on :12345...
Received a request:
Method: POST
URL: /
Body: test
```

Slack

步骤1：配置Slack应用

首先，你需要在[Slack API](#)上创建一个应用。给你的机器人/应用授予以下OAuth权限范围：`chat:write`, `chat:write.public`

The screenshot shows the 'Scopes' section of the Slack API configuration. It includes a table with two rows, each with an 'OAuth Scope' and its description. The first row has 'chat:write' selected, indicated by a red border around the column. The second row has 'chat:write.public'. Both rows have a trash icon on the right. A button at the bottom left says 'Add an OAuth Scope'.

OAuth Scope	Description	
chat:write	Send messages as @casdoor	trash
chat:write.public	Send messages to channels @casdoor isn't a member of	trash

Add an OAuth Scope

步骤2：获取机器人用户OAuth访问令牌和频道ID

复制你的[Bot User OAuth Access Token](#)以供下面使用。

Features

- App Home
- Org Level Apps
- Incoming Webhooks
- Interactivity & Shortcuts
- Slash Commands
- Workflow Steps

OAuth & Permissions

- Event Subscriptions
- User ID Translation
- App Manifest NEW
- Beta Features

Submit to App Directory

- Review & Submit
- Give feedback

Slack ❤️

- Help
- Contact
- Policies
- Our Blog

Opt In

OAuth Tokens for Your Workspace

These tokens were automatically generated when you installed the app to your team. You can use these to authenticate your app. [Learn more.](#)

User OAuth Token

xoxp-5865439759200-5827199080935-5865457291440-67810c12dfcae [Copy](#)

Access Level: Workspace

Bot User OAuth Token

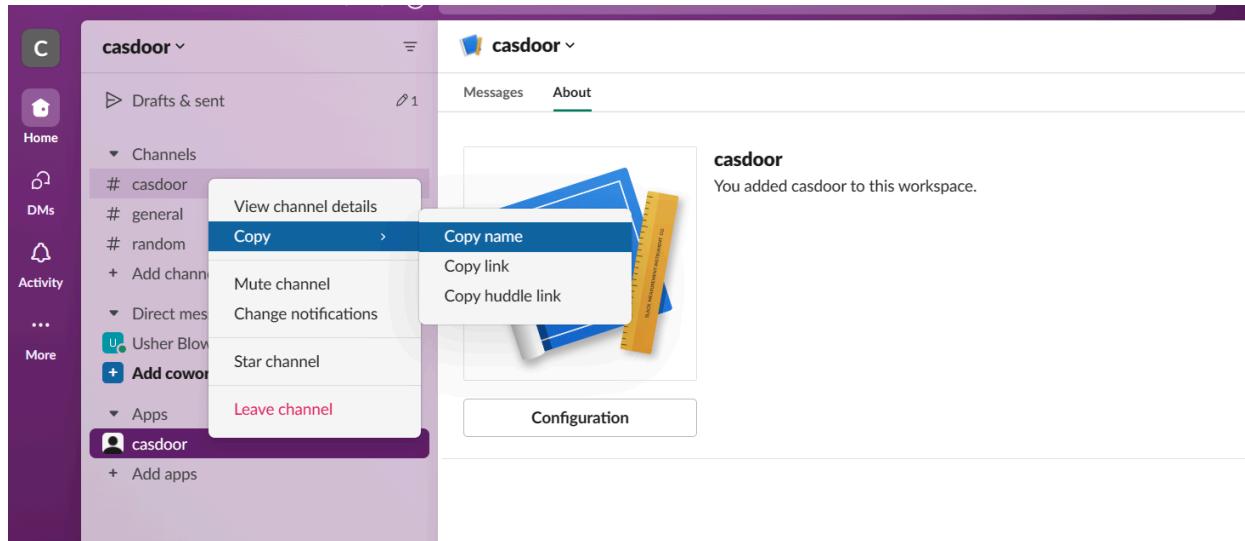
xoxb-5865439759200-5865457299776-2tbOAVTNPpG7vmLog7OFJS5t [Copy](#)

Access Level: Workspace

[Reinstall to Workspace](#)

Redirect URLs

复制你想要发布消息的频道的频道ID。 你可以通过右键点击一个频道并选择[复制名称](#)来获取频道ID



步骤3：配置Casdoor Slack提供者

有三个必填字段：`App Key`，`Content`，和`Chat ID`。字段与Slack之间的关系如下：

名称	Slack中的名称
Secret key	Access Token
Chat ID	Channel ID
Content	

The screenshot shows the Casdoor configuration interface for setting up a Slack provider. The provider is named "slack". The "Secret key" field contains "***". The "Content" field contains "dont reply". The "Chat ID" field contains "casdoor". A purple button labeled "Send Testing Notification" is visible next to the Chat ID input field. The "Provider URL" field contains a placeholder URL: <https://github.com/organizations/xxx/settings/applications/1234567>.

Name ② : slack

Display name ② : slack

Organization ② : admin (Shared)

Category ② : Notification

Type ② : Slack

Secret key ② : ***

Content ② : dont reply

Chat ID ② : casdoor Send Testing Notification

Provider URL ② : <https://github.com/organizations/xxx/settings/applications/1234567>

Google Chat

步骤1：获取应用默认凭据

为了将notify集成到Google Chat应用中，必须提供应用凭据。有关Google应用凭据JSON的更多信息，请参见：[应用默认凭据是如何工作的](#)

json将如下所示：

```
{  
  "type": "service_account",  
  "project_id": "",  
  "private_key_id": "",  
  "private_key": "",  
  "client_email": "",  
  "client_id": "",  
  "auth_uri": "",  
  "token_uri": "",  
  "auth_provider_x509_cert_url": "",  
  "client_x509_cert_url": ""  
}
```

步骤3：配置Casdoor Google Chat提供者

在元数据中填写应用凭据。

Name [?](#):

Display name [?](#):

Organization [?](#):

Category [?](#):

Type [?](#): 

Metadata [?](#):

```
{  
  "type": "service_account",  
  "project_id": "",  
  "private_key_id": ""  
}'
```

Content [?](#):

Test Notification [?](#):

Provider URL [?](#): 

Twitter

步骤1：从twitter获取配置项

首先，注册一个Twitter开发者账户，在开发者门户内创建一个Twitter应用，参考文档：[认证](#)

复制你的API Key和API Secret，Access Token和Access Token Secret

The screenshot shows the Twitter Developer Portal interface. On the left is a dark sidebar with navigation links: Dashboard, Projects & Apps (with a dropdown arrow), Products (NEW), and Account. The main content area has a light background. At the top, there are two tabs: 'Settings' and 'Keys and tokens', with 'Keys and tokens' being the active tab. Below the tabs, there are two sections: 'Consumer Keys' and 'Authentication Tokens'. The 'Consumer Keys' section contains a box for 'API Key and Secret' with a 'Reveal API Key hint' link and a 'Regenerate' button, all of which are highlighted with a red border. The 'Authentication Tokens' section contains a box for a 'Bearer Token' generated on September 3, 2023, with 'Revoke' and 'Regenerate' buttons. Below that is another box for an 'Access Token and Secret' also generated on September 3, 2023, for the user '@Allcompleteness', with 'Revoke' and 'Regenerate' buttons. This second box is also highlighted with a red border.

步骤2：获取Twitter ID

Twitter ID不能直接获取，你可以通过一些第三方工具获取。

- [TweeterID](#)
- [Twiteridfinder](#)

步骤3：配置Casdoor Twitter提供商

有五个必填字段：`Client ID`, `Client secret`, `Client ID 2`, `Client secret 2`和`Chat ID`。字段与Twitter之间的关系如下：

名称	Twitter中的名称
Client ID	API Key
Client secret	API Secret
Client ID 2	Access Token
Client secret 2	Access Token Secret
Chat ID	Twitter ID

Name ? :

Display name ? :

Organization ? :

Category ? :

Type ? : 

Client ID ? :

Client secret ? :

Client ID 2 ? :

Client secret 2 ? :

Content ? :

Chat ID ? : Send Testing Notification

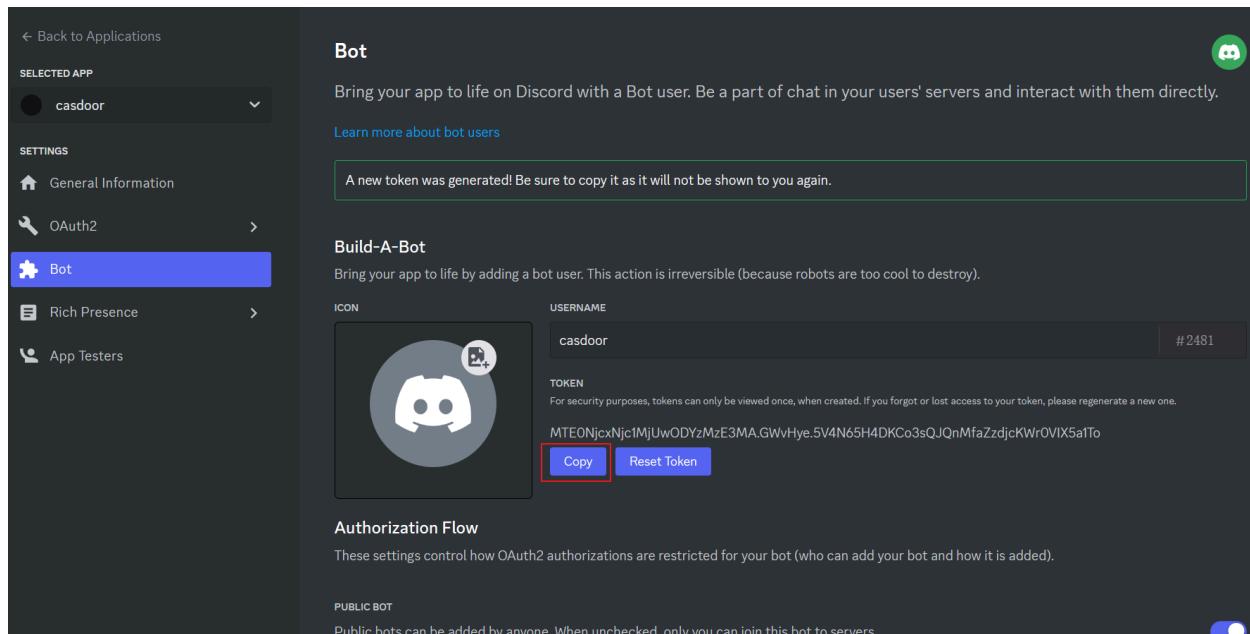
Provider URL ? :

Discord

步骤1：从Discord获取令牌

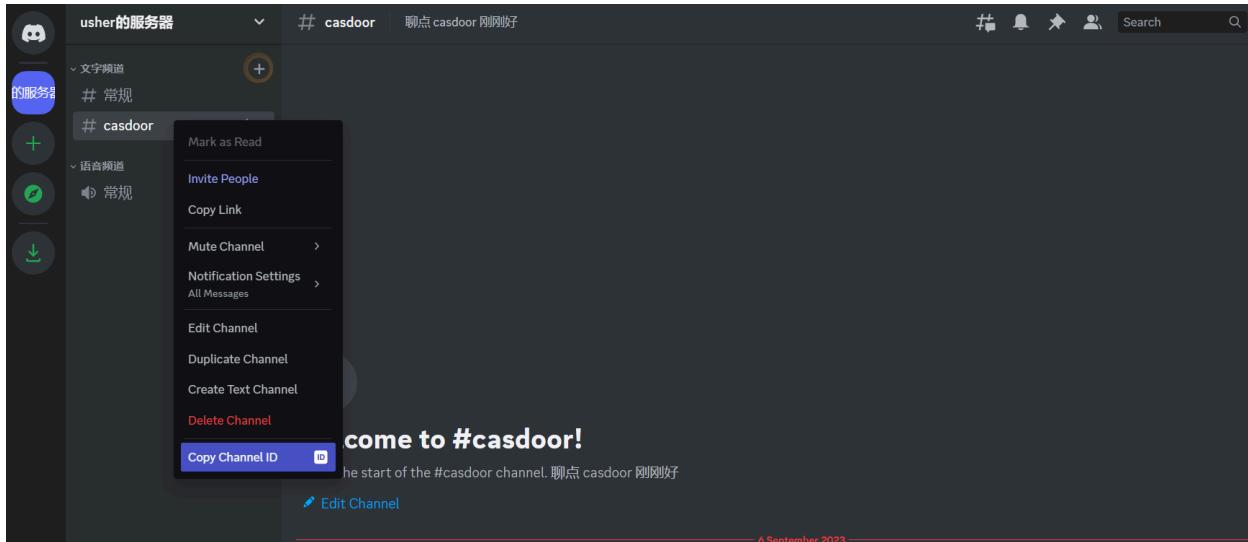
首先，注册Discord开发者门户，创建一个新的应用程序，导航到“Bot”选项卡进行配置。

复制你的Bot **token**



步骤2：获取频道ID

复制你想要发布消息的频道的频道ID。你可以通过右键点击频道并选择**复制频道ID**来获取频道ID



步骤3：配置Casdoor Discord提供者

有三个必填字段：`App Key`，`Content`，和`chat ID`。字段与Discord之间的关系如下：

名称	在Slack中的名称
密钥	令牌
聊天ID	频道ID
内容	

Name ⓘ :	discord
Display name ⓘ :	discord
Organization ⓘ :	admin (Shared)
Category ⓘ :	Notification
Type ⓘ :	 Discord
Secret key ⓘ :	***
Content ⓘ :	test
Chat ID ⓘ :	1146715329133821972
Provider URL ⓘ :	🔗 https://github.com/organizations/xxx/settings/applications/1234567
	<button>Send Testing Notification</button>

WeCom

Step 1: Create a WeCom Group Chat Bot

WeCom (WeChat Work) supports sending notifications through group chat bots. First, create a group chat in WeCom and add a bot to it.

In your WeCom group chat, go to group settings and add a bot. After adding the bot, you will receive a webhook URL.

Step 2: Get the Webhook URL

Copy the webhook URL provided by WeCom. This URL is used to send messages to your group chat.

The webhook URL format is: `https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=YOUR_KEY`

For more information, refer to the [WeCom Webhook Documentation](#).

Step 3: Configure Casdoor WeCom Provider

In Casdoor, create a new notification provider and select "WeCom" as the type.

Configure the following field:

Name	Name in WeCom
Endpoint	Webhook URL

Paste your webhook URL into the `Endpoint` field. The `Content` field can be used to define a message template for notifications sent to your WeCom group.

存储

概述

在Casdoor中设置一个存储提供者以上传文件

本地文件系统

使用本地文件系统作为Casdoor的存储提供者

Amazon S3

使用Amazon S3作为Casdoor的存储提供者

Azure Blob

使用 Azure Blob 作为Casdoor的存储提供商

Google Cloud Storage

使用Google Cloud Storage作为Casdoor的存储提供商

MinIO

使用MinIO作为Casdoor的存储提供商

阿里云OSS

使用阿里云OSS作为Casdoor的存储提供商

腾讯云COS

使用腾讯云COS作为Casdoor的存储提供商

Synology NAS

使用Synology NAS作为Casdoor的存储提供商

概述

如果你需要使用文件存储服务，如“头像上传”，你需要在Casdoor中设置一个存储提供者并将其应用到你的应用程序中。

Casdoor支持两种类型的存储：**本地**和**云**。在本章中，你将学习如何添加一个存储提供者以使用这些服务。

项目

- **客户端ID**: 由云存储提供者提供的唯一标识符。
- **客户端密钥**: 只有Casdoor和云存储服务知道的安全值。
- **端点**: 云存储服务的公共URL或域名。
- **端点（内网）**: 云存储服务的内部或私有URL或域名。
- **路径前缀**: 文件位置的路径前缀。

① 信息

默认的**路径前缀**是"/"。例如，当**路径前缀**为空时，一个默认的文件路径将是：

```
https://cdn.casbin.com/casdoor/avatar.png
```

你可以用"abcd/xxxx"填充它，然后你可以在以下位置存储你的头像：

```
https://cdn.casbin.com/abcd/xxxx/casdoor/avatar.png
```

- **存储桶**: 用于存储文件和数据的容器。
- **域名**: 你的云存储的CDN的自定义域名。
- **区域ID**: 用于指定云存储服务所在数据中心区域的标识符。

本地设置

我们支持将文件上传到本地系统。

云

我们支持AWS S3、Azure Blob Storage、MinIO、阿里云OSS、腾讯云COS，并且我们正在不断添加更多的云存储服务。

本地文件系统

① 信息

本地文件系统提供者将在Casdoor的`files`文件夹中存储您上传的文件。

例如，当您的Casdoor位于`/home/user/casdoor`目录时，上传的文件将存储在`/home/user/casdoor/files`文件夹中。

配置Casdoor提供者

Name [?](#) :

localfile

Display name [?](#) :

localfile

Organization [?](#) :

admin (Shared)

Category [?](#) :

Storage

Type [?](#) :

Local File System

Path prefix [?](#) :

Domain [?](#) :

http://localhost:8000

Provider URL [?](#) :



`Path prefix`是您文件位置路径的前缀。 您可以根据需要填写。 在以下示例中，您可

以看到带前缀和不带前缀的区别。

带前缀

Path prefix [?](#) :

images

casdoor > files > images > resource > built-in > admin > withPrefix.png

无前缀

Path prefix [?](#) :

casdoor > files > resource > built-in > admin > withoutPrefix.png

Amazon S3

 备注

这是一个Amazon S3的例子。

创建安全凭证

按照文档：[管理访问密钥](#)在Amazon控制台中创建并保存您的access key和secret access key。

配置您的存储桶

在您的存储桶权限选项中，取消勾选“阻止”选项并保存更改。

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#)

[Save changes](#)

编辑对象所有权并检查ACLs已启用。

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer

The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more ↗](#)

Cancel

Save changes

配置Casdoor

名称	在Amazon中的名称	是否必需
Client ID	Access key	必需
Client secret	Secret access key	必需
Endpoint	Endpoint	必需
Endpoint (intranet)	VPC endpoint	

名称	在Amazon中的名称	是否必需
Bucket	Bucket name	必需
Path prefix		
Domain	CloudFront domain	
Region ID	AWS region	必需

填写必要的信息，包括从上一步中 `access key` 和 `secret access key` 获取的 `Client ID` 和 `Client Secret`。您可以参考此文档以获取有关 `endpoint` 格式的信息：[网站端点](#)

Name ? :	awss3
Display name ? :	awss3
Organization ? :	admin (Shared)
Category ? :	Storage
Type ? :	AWS S3
Client ID ? :	AKIAYOMMXHVZC5CHBNR
Client secret ? :	***
Endpoint ? :	http://kininaru.s3-website.ap-northeast-1.amazonaws.com
Endpoint (Intranet) ? :	
Bucket ? :	kininaru
Path prefix ? :	
Domain ? :	
Region ID ? :	ap-northeast-1
Provider URL ? :	🔗

(可选) 使用VPC

您可以参考官方文档进行配置: [通过AWS PrivateLink访问AWS服务](#)

(可选) 使用CloudFront分发

按照文档配置CloudFront: [配置CloudFront](#)

在域名字段中，输入您的分发域名。

Endpoint [?](#) : <http://kininaru.s3-website.ap-northeast-1.amazonaws.com>

Bucket [?](#) : kininaru

Path prefix [?](#) :

Domain [?](#) : <https://d20zlk9foisfk0.cloudfront.net>

Region ID [?](#) : ap-northeast-1

Provider URL [?](#) : [🔗](#)

Azure Blob

① 备注

这是一个Azure Blob的例子。

- 您必须拥有一个 Azure storage 帐户。

步骤1：选择Azure Blob

选择 Azure Blob 作为存储类型。

Edit Provider Save Save & Exit

Name ② :	provider_ftfzes
Display name ② :	New Provider - ftfzes
Category ② :	Storage
Type ② :	Azure Blob
Client ID ② :	Local File System AWS S3
Client secret ② :	Aliyun OSS Tencent Cloud COS
Endpoint ② :	Azure Blob

步骤2：在Casdoor中填写必要的信息

需要填写四个必填字段：`Client ID`、`Client secret`、`Endpoint`和`Bucket`。与 Azure Blob账户的对应关系如下：

字段名称	Azure 名称	必需的
Client ID	AccountName	必需
Client secret	AccountKey	必需的
Endpoint	ContainerUrl	必需的
Endpoint (intranet)	PrivateEndpoint	
Bucket	ContainerName	必需的
Path prefix		
Domain	DomainName	

- 账户名称

AccountName 就是你的账户名。

- AccountKey

AccountKey 是您访问 Azure API 的密钥。

 备注

您可以从 Azure 门户的“Access Keys”部分获取您的账户密钥，该部分位于您的存储账户的左侧面板上。

The screenshot shows the 'Access keys' section of the Azure Storage account settings for a storage account named 'casbin'. The left sidebar lists 'Data storage' (Containers, File shares, Queues, Tables), 'Security + networking' (Networking, Azure CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and 'Data management'. The main area displays the 'Storage account name' as 'casbin'. It shows two sets of keys: 'key1' (Last rotated: 2023/7/22) and 'key2' (Last rotated: 2023/7/22). Each key has a 'Key' field (redacted) and a 'Show' button. Below each key is a 'Connection string' field (redacted) and a 'Show' button. A note at the top right says: 'Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.' A link 'Learn more about managing storage account access keys' is also present.

- ContainerUrl

您可以从容器属性中获取ContainerUrl。

 default | Properties

Container

Search Refresh Give feedback

Overview Diagnose and solve problems Access Control (IAM)

Shared access tokens Access policy Properties Metadata

NAME
default

URL
`https://casbin.blob.core.windows.net/default`

LAST MODIFIED
7/22/2023, 5:18:03 PM

ETAG
0x8DB8A948D644055

- (可选) PrivateEndpoint

Azure Private Endpoint是一个功能，允许将Azure服务连接到Azure虚拟网络（VNet）的私有子网。您可以参考官方Azure文档进行配置：[私有端点配置](#)

- ContainerName

在这个例子中，创建了一个名为'default'的默认容器。

Home > casbin

casbin | Containers

Storage account

Search (Ctrl+ /) Container Change access level Restore containers Refresh Delete

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser (preview)

Data storage

- Containers** (highlighted with a red circle)
- File shares
- Queues
- Tables

Name

Name	Created
\$logs	2022-04-23
default	2022-04-26

- (可选) 域名

在您的Azure CDN中的自定义域名。

Home > fd-profile

fd-profile

Front Door and CDN profiles

Search (Ctrl+ /) Purge cache Origin response timeout Delete Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings**
- Front Door manager
- Domains
- Origin groups
- Rule set
- Security policies
- Optimizations
- Secrets
- Properties
- Locks
- Analytics
- Reports
- Monitoring

Essentials

Resource group (move)	: default
Status	: Active
Location	: Global
Subscription (move)	: Visual Studio Enterprise
Subscription ID	[REDACTED]
Tags (edit)	: Click here to add tags

Properties

Endpoints	Endpoint hostname	endpoint-hth4eebgcdzc2ex.z01.azurefd.net
	Provision succeeded	Enabled

Custom domains

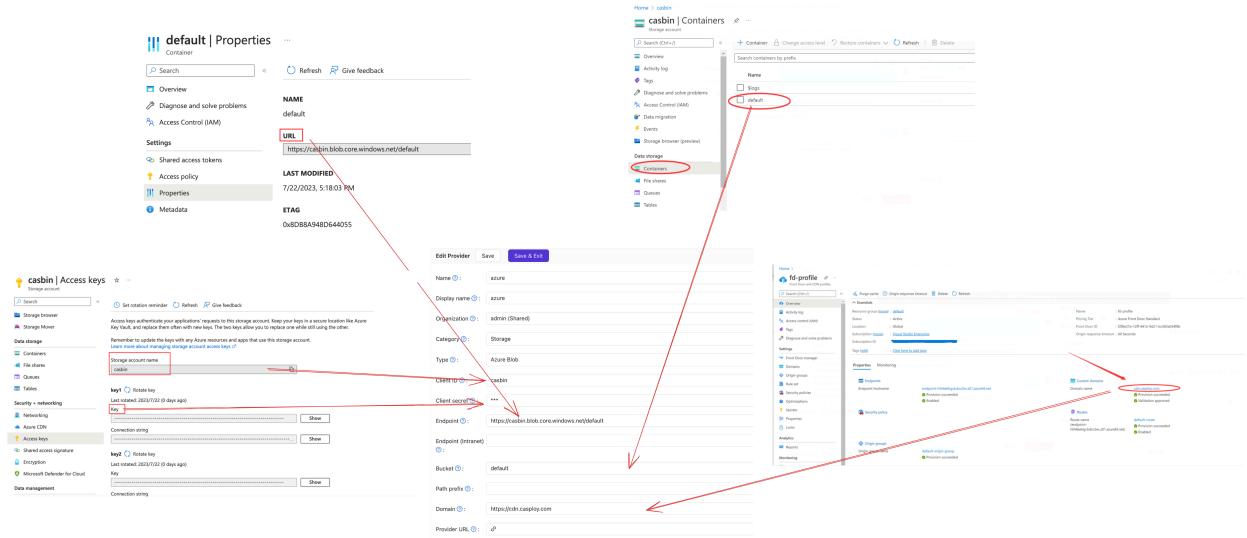
Domain name	cdn.casploy.com
	Provision succeeded
	Validation approved

Routes

Route name	default-route
(endpoint-hth4eebgcdzc2ex.z01.azurefd.net)	Provision succeeded
	Enabled

步骤3：保存您的配置

最终结果如下：



现在您可以在您的应用程序中使用Azure Blob存储服务。

Google Cloud Storage

① 备注

这是一个Google Cloud Storage的例子。

创建安全凭证

按照文档: [Cloud Storage Authentication](#) 在GCP控制台中创建一个具有正确的 IAM 权限 来访问bucket的 服务账户。

配置Casdoor

名称	Google中的名称	是否必需
Service Account JSON	Service Account Key	必需
Endpoint	Endpoint	
Bucket	Bucket name	必需

Name ⓘ :

Display name ⓘ :

Organization ⓘ : ▾

Category ⓘ : ▾

Type ⓘ : ▾

Service account JSON ⓘ :

Endpoint ⓘ :

Bucket ⓘ :

Path prefix ⓘ :

Provider URL ⓘ :

MinIO

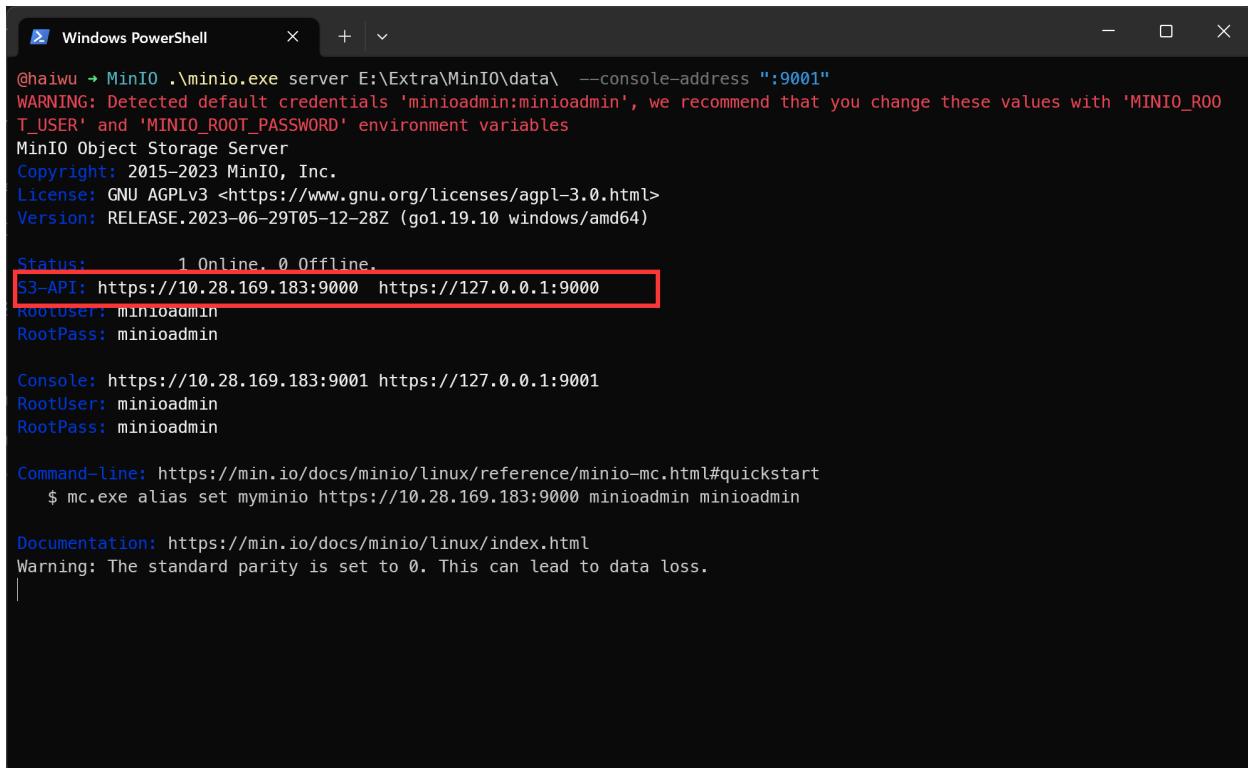
① 备注

这是一个如何配置MinIO提供商的示例。

MinIO是一个与Amazon S3云存储服务API兼容的高性能对象存储服务。

步骤1：部署MinIO服务

首先，部署启用TLS的MinIO服务。您可以从控制台获取API地址。



```
@haiwu ~ MinIO .\minio.exe server E:\Extra\MinIO\data\ --console-address ":9001"
WARNING: Detected default credentials 'minioadmin:minioadmin', we recommend that you change these values with 'MINIO_ROOT_USER' and 'MINIO_ROOT_PASSWORD' environment variables
MinIO Object Storage Server
Copyright: 2015-2023 MinIO, Inc.
License: GNU AGPLv3 <https://www.gnu.org/licenses/agpl-3.0.html>
Version: RELEASE.2023-06-29T05-12-28Z (go1.19.10 windows/amd64)

Status: 1 Online, 0 Offline.
S3-API: https://10.28.169.183:9000 https://127.0.0.1:9000
RootUser: minioadmin
RootPass: minioadmin

Console: https://10.28.169.183:9001 https://127.0.0.1:9001
RootUser: minioadmin
RootPass: minioadmin

Command-line: https://min.io/docs/minio/linux/reference/minio-mc.html#quickstart
$ mc.exe alias set myminio https://10.28.169.183:9000 minioadmin minioadmin

Documentation: https://min.io/docs/minio/linux/index.html
Warning: The standard parity is set to 0. This can lead to data loss.
```

其次，创建Access Key和Secret key。

The screenshot shows the MinIO Object Store interface. On the left sidebar, under the 'Administrator' section, the 'Buckets' option is highlighted with a red box. The main content area is titled 'Create Access Key'. It has two input fields: 'Access Key' containing 'ulqg2f67Or9mmTnphPA' and 'Secret Key' with a masked value. Below these is a 'Restrict beyond user policy' section with a note about specifying an optional JSON-formatted IAM policy. At the bottom are 'Clear' and 'Create' buttons. To the right, there's a sidebar with sections for 'Learn more about Access Keys', 'Create Access Keys', and 'Assign Custom Credentials'. The 'Assign Access Policies' section is also visible.

第三，创建 Bucket。

The screenshot shows the MinIO Object Store interface. On the left sidebar, under the 'Administrator' section, the 'Buckets' option is highlighted with a blue box. The main content area is titled 'Create Bucket'. It has a 'Bucket Name*' field containing 'casdoor'. Below it are sections for 'Features': 'Versioning' (OFF), 'Object Locking' (OFF), and 'Quota' (OFF). At the bottom are 'Clear' and 'Create Bucket' buttons. To the right, there's a sidebar with sections for 'Buckets', 'Versioning' (allows keeping multiple versions of the same object), 'Object Locking' (prevents objects from being deleted), 'Quota' (limits the amount of data in the bucket), and 'Retention' (imposes rules to prevent object deletion).

步骤2：在Casdoor中创建一个MinIO提供商

现在在Casdoor中创建一个MinIO提供商。 填写必要的信息。

名称	在MinIO中的名称
Category	选择 Storage
Type	选择 MinIO
Client ID	从步骤1获取的 Access Key
Client secret	从步骤1获取的 Secret Key
Endpoint	从步骤1获取的 API地址
Bucket	从步骤1获取的 Bucket

步骤3：在您的应用程序中使用MinIO存储服务

现在您可以在您的应用程序中使用MinIO存储服务。

阿里云OSS

① 备注

这是一个阿里云OSS的例子。

AccessKey是您用于以完全账户权限访问阿里云API的密钥。

要创建AccessKey，请按照[阿里云工作台](#)中的说明操作。

接下来，创建OSS服务：

创建 Bucket

② 创建存储空间 X

注意：Bucket 创建成功后，您所选择的 **存储类型、区域、存储冗余类型** 不支持变更。

Bucket 名称	mycasdoor	9/63 ✓
地域	华北2 (北京)	▼
相同区域内的产品内网可以互通；订购后不支持更换区域，请谨慎选择。		
Endpoint	oss-cn-beijing.aliyuncs.com	

在Casdoor中填写必要的信息并保存：

Name <small>?</small> :	provider_storage_aliyun_oss
Display name <small>?</small> :	Storage Aliyun OSS
Category <small>?</small> :	Storage
Type <small>?</small> :	Aliyun OSS
Client ID <small>?</small>	LTAIxFoNpNAnPoiT
Client secret <small>?</small>	***
Endpoint <small>?</small> :	oss-cn-beijing.aliyuncs.com
Endpoint (Intranet) <small>?</small> :	oss-cn-beijing-internal.aliyuncs.com
Bucket <small>?</small> :	casbin
Domain <small>?</small> :	https://cdn.casbin.com/casdoor/
Provider URL <small>?</small> :	https://oss.console.aliyun.com/bucket/oss-cn-beijing/casbin/object

您现在可以在您的应用程序中使用阿里云云存储服务。

腾讯云COS

① 备注

这是一个腾讯云COS的例子。

在Casdoor中填写必要的信息

有五个必填字段：`客户端ID`，`客户端密钥`，`端点`，`存储桶`，和`区域ID`。与腾讯云COS账户的对应关系如下：

名称	在腾讯的名称	必需的
Client ID	SecretId	是
Client secret	SecretKey	是
Endpoint	Endpoint	是
Bucket	BucketName	是
Path prefix		
Domain	CDNDomain	
Region ID	Region	是

腾讯云COS信息

- SecretId和SecretKey

The screenshot shows the Tencent Cloud API密钥管理 (API Key Management) page. On the left sidebar, under 访问管理 (Access Management), the API密钥管理 (API Key Management) option is selected. The main content area displays a table of keys. A single row is highlighted, showing:

APPID	密钥	创建时间	最近访问时间	状态
1319606438	SecretId: AKIDdAlMuNrJn8GHI6mLi6NSWbheNr7MViec SecretKey: ***** 显示	2023-07-22 19:01:...	2023-07-22 22:09	已启用

- 端点, BucketName和区域

The screenshot shows the Tencent Cloud 存储桶概览 (Bucket Overview) page for the bucket 'casdoor-1319606438'. The left sidebar lists various management options like 概览 (Overview), 文件列表 (File List), 基础配置 (Basic Configuration), and 安全管理 (Security Management). The main content area includes sections for 用量概览 (Usage Overview), 基本信息 (Basic Information), and 域名信息 (Domain Information). In the 基本信息 section, the storage bucket name is listed as 'casdoor-1319606438' and the location is '广州 (中国) (ap-guangzhou)'. In the 域名信息 section, the domain name is listed as 'https://casdoor-1319606438.cos.ap-guangzhou.myqcloud.com'.

- (可选) CDNDomain

您可以参考官方文档进行配置：配置CDN

配置Casdoor提供商

The screenshot shows the Tencent Cloud API Management interface. A new secret key is being created with the following details:

APPID	密钥	创建时间	最近访问时间	状态
1319606438	SecretAKDdAMuJn8GHbmLjNSWbheN7Mveic SecretKey	2023-07-22 19:01:...	2023-07-22 22:29	已启用

Red arrows from the Casdoor provider configuration fields point to the following fields in the screenshot:

- Name: tencentcos
- Display name: tencentcos
- Organization: admin (Shared)
- Category: Storage
- Type: Tencent Cloud COS
- Client ID: AKID4MhAuNjN8GH6mL6NSWbheN7Mveic
- Client secret: ***
- Endpoint: casdoor-1319606438.cos.ap-guangzhou.myqcloud.com
- Bucket: casdoor-1319606438
- Path prefix:
- Domain:
- Region ID: ap-guangzhou
- Provider URL: dP

Below the screenshot, the Casdoor provider configuration fields are shown again, with red boxes highlighting the Client ID, Client secret, Endpoint, Bucket, and Region ID fields.

The screenshot shows the Tencent Cloud Object Storage (COS) interface. A bucket's basic information is displayed:

基本信息	域名信息
桶名: casdoor-1319606438 (存储桶不支持修改) 所属地域: AP 中国 广州 (ap-guangzhou) 创建时间: 2023-07-22 18:57:50 访问权限: 私有可见	自定义CDN连接域名: 自定义源站域名: 带宽: 流量计费: 自动加速: 主节点: 注: COS 的域名必须部署于阿里云 DNS 解析, 如果您在腾讯云内部部署了自有解析服务, 则腾讯云不支持为您提供。如果您选择腾讯云外网地址, 涉及内外网互通的的相关设置, 请详细参见 相关技术文档 。

Red arrows from the Casdoor provider configuration fields point to the Bucket and Region ID fields in the screenshot.

Synology NAS

① 备注

这是一个Synology NAS的例子。

在Casdoor中填写必要的信息

有五个必填字段: Client ID、Client secret和Endpoint。与Synology NAS账户的对应关系如下:

名称	在腾讯中的名称	必需
Client ID	SecretId	是
Client secret	SecretKey	是
Endpoint	Endpoint	是
Bucket		
Path prefix		
Domain		
Region ID		

配置Casdoor提供商

The screenshot displays three windows related to provider configuration:

- Casdoor Provider Configuration:** Shows the "Edit Provider" form for "provider_synology". Key fields include:
 - Name: provider_synology
 - Display name: New Provider - synology
 - Organization: built-in
 - Category: Storage
 - Type: Synology
 - Client ID: password_ls_xiaokonglong
 - Client secret: ***
 - Endpoint: http://169.254.0.2:5000
- Synology Assistant:** Shows a list of Synology devices. One device is highlighted:

服务器名称	IP 地址	IP 状态	状态	网络物理地址	版本	型号	序列号	IWOL
synologyNAS	169.254.0.2	Manual	已就绪	00:11:32:2C:A6:03	6.1.7-15284	DS3617xs	A8ODD02468	-

Endpoint: http://169.254.0.2:5000 (default http/https port of Synology is 5000/5001)
- Personal Account Settings:** Shows the "Personal" tab of a user account settings dialog. Fields include:
 - Name: password_ls_xiaokonglong
 - New Password: ****
 - Confirm password: ****
 - Email: (empty)
 - Default language: System default

Red arrows point from the "Client ID", "Client secret", and "Endpoint" fields in the provider configuration to their respective counterparts in the Synology Assistant window. A red arrow also points from the "Name" field in the account settings to the "Name" field in the provider configuration.

您可以参考官方文档进行配置: [链接](#)

SAML

概述

使用来自支持SAML 2.0 的外部身份提供商的身份

自定义

配置您的SAML自定义提供商

Keycloak

使用 Keycloak 验证用户

阿里巴巴云IDaaS

使用阿里巴巴云IDaaS进行用户身份验证

概述

Casdoor可以配置为支持用户使用支持SAML 2.0的外部身份提供商的身份登录到UI。在此配置中，Casdoor从不存储任何用户的凭证。

现在，Casdoor支持多个SAML应用程序提供商。在添加到Casdoor后，提供商的图标将在登录页面上显示。以下是Casdoor支持的提供商：

阿里巴巴云IDaaS	Keycloak	自定义
		
		

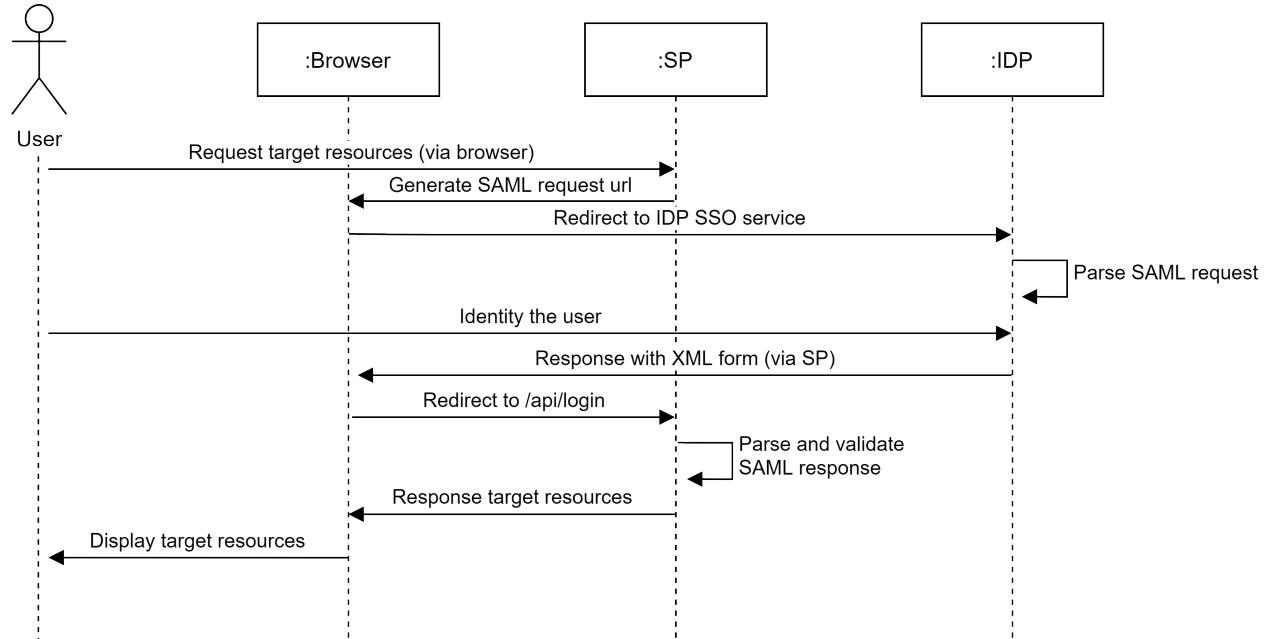
条款

- 身份提供商 (IDP) —— 储存身份数据库并向Casdoor提供身份和认证服务的服务。
- 服务提供商 (SP) - 向终端用户提供资源的服务，在这种情况下，是Casdoor部署。
- 申述消费者服务——身份提供者提出的SAML断言的消费者。

SAML 集成工作方式

当使用SAML SSO时，用户通过身份提供商登录Casdoor，而无需将凭证传递给

Casdoor。进展情况见下图表。



自定义

Casdoor支持配置SAML自定义提供商，您可以使用Casdoor作为服务提供商（SP）连接任何支持SAML 2.0协议的身份提供商（IDP）。

步骤1. 获取IDP的元数据

首先，您需要获取IDP的元数据，这是一个用于描述IDP提供的服务的配置信息的XML文档。它需要包括EntityID、SSO Endpoint等信息。

一些IDP，如Keycloak，需要SP信息来提供元数据。您可以参考文档[Keycloak](#)。

您可以使用oktadev来测试SAML自定义提供商，这是[元数据](#)。

步骤2. 配置SAML自定义提供商

获取IDP的元数据后，创建一个SAML自定义提供商并填写必要的信息。

字段	描述
Category	选择SAML
Type	选择自定义
Favicon.URL	IDP logo的URL

字段	描述
Metadata	IDP的元数据

然后点击 **解析** 按钮, **Endpoint**、**IdP**、**Issuer URL**、**SP ACS URL** 和 **SP Entity ID** 将被自动解析。

Name [?](#): saml_custom_provider_oktadev

Display name [?](#): saml_custom_provider_oktadev

Organization [?](#): admin (Shared)

Category [?](#): SAML

Type [?](#): Custom

User mapping [?](#):

- ID [?](#):
- Username [?](#):

 - FirstName

- Display name [?](#):

 - LastName

- Email [?](#):

 - Email

- Avatar [?](#):

Favicon [?](#):

URL [?](#): https://cdn.casbin.org/img/social_okta.png

Preview:



Client ID [?](#):

Client secret [?](#):

Sign request [?](#):

Metadata [?](#):

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="urn:example:idp">
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
```

Parse

Endpoint [?](#): <http://idp.oktadev.com>

IdP [?](#): MIIDPDCCAiQCCQDyJgOlsqbzANBgkqhkiG9w0BAQUFADBgMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pYTEWMBQGA1UEBxMNU2FuiEZyYW5jaXNjbzEQMA4GA1UEChMHShr

Issuer URL [?](#): urn:example:idp

SP ACS URL [?](#): /api/acs

SP Entity ID [?](#): /api/acs

Provider URL [?](#): [?](#)

最后，将SAML自定义提供商添加到应用程序的 Providers。

Providers	Action							
Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action
provider_storage_minio_s3	Storage	HMAC	<input checked="" type="checkbox"/>	 				
provider_oauth_lark	OAuth		<input checked="" type="checkbox"/>	 				
provider_email_eq	Email		<input checked="" type="checkbox"/>	 				
provider_web3_metamask	Web3		<input checked="" type="checkbox"/>	 				
provider_google_oauth	OAuth		<input checked="" type="checkbox"/>	 				
provider_web3_onboard	Web3		<input checked="" type="checkbox"/>	 				
saml_custom_provider_oktadev	SAML		<input checked="" type="checkbox"/>	 				
saml_custom_provider_keycloak	SAML		<input checked="" type="checkbox"/>	 				

Keycloak

JBoss [Keycloak](#) 系统是一个广泛使用的开源身份管理系统，支持通过SAML和OpenID Connect与应用程序集成。它还可以作为其他提供商（如LDAP或其他SAML提供商）和支持SAML或OpenID Connect的应用程序之间的身份代理运行。

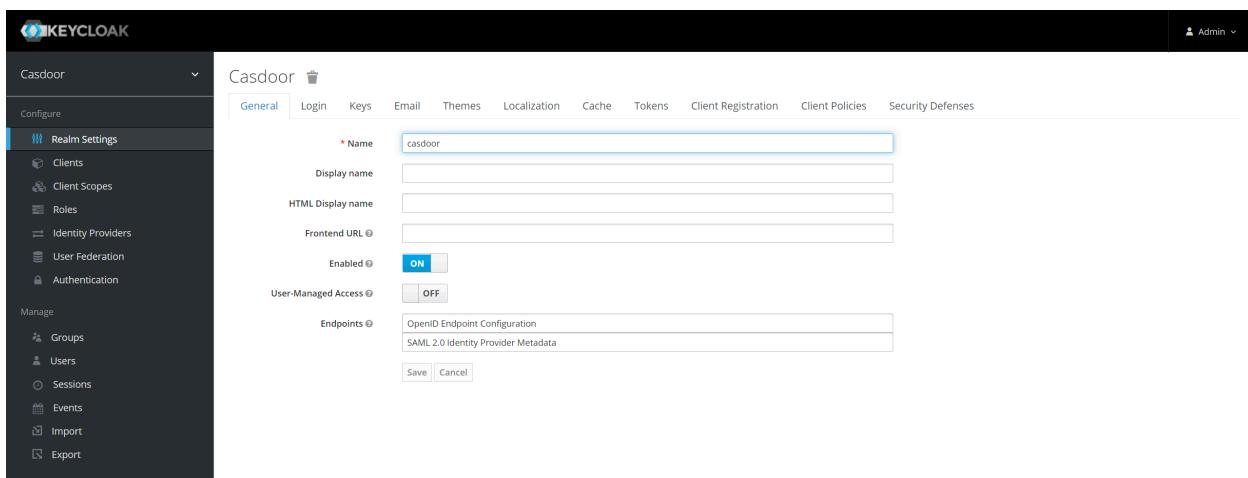
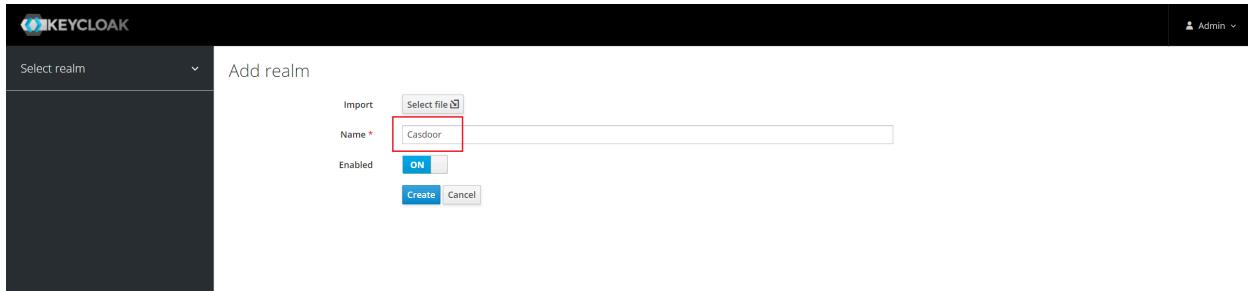
这是一个示例，说明如何在Keycloak中配置新的客户端条目，并配置Casdoor使用它，以允许通过Keycloak配置授予访问权限的Keycloak用户进行UI登录。

Configure Keycloak

对于这个例子，让我们做出以下配置选择和假设：

- 假设你正在本地以开发模式运行Casdoor。Casdoor UI可在<http://localhost:7001>处获取，服务器可在<http://localhost:8000>处获取。根据需要替换为适当的URL。
- 假设你正在本地运行Keycloak。Keycloak UI可在<http://localhost:8080/auth>处获得。
- 在此基础上，用于此部署的SPACS URL将是：<http://localhost:8000/api/acs>。
- 我们的SP实体ID将使用相同的URL：<http://localhost:8000/api/acs>。

您可以使用默认的领域，或者创建一个新的领域。



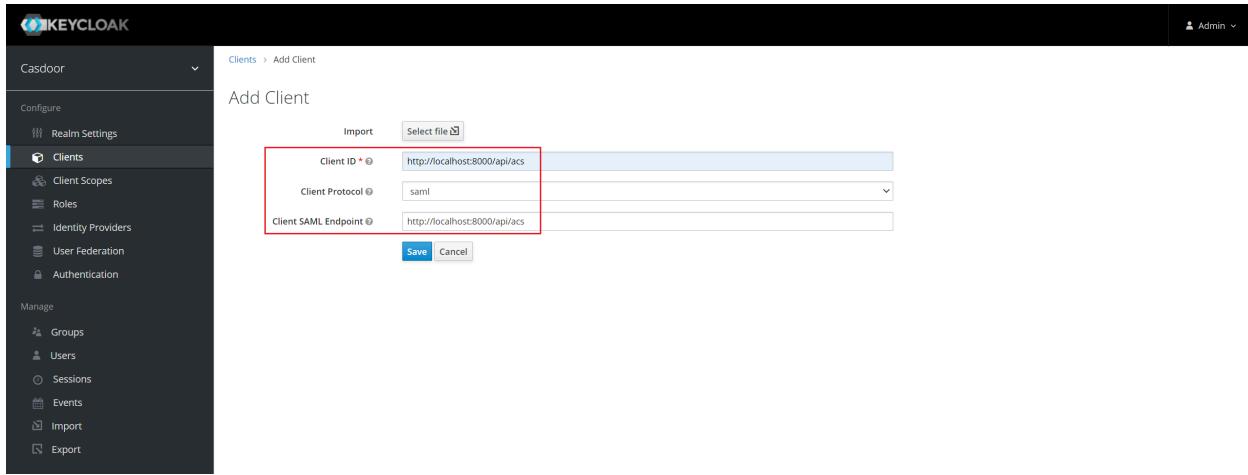
在 Keycloak 中添加客户端条目

① 信息

有关Keycloak Clients的更多详细信息，请参阅[Keycloak文档](#)。

在菜单中点击 **客户端** 然后点击 **创建** 去到 **添加客户端** 页面。按照以下方式填写字段：

- **客户端 ID:** `http://localhost:8000/api/acs` - 这将是以后在 Casdoor 配置中使用的 SP 实体ID。
- **Client Protocol:** `saml`.
- **客户端SAML端点:** `http://localhost:8000/api/acs` - 这个URL是你希望 Keycloak服务器发送SAML请求和响应的地方。通常，应用程序有一个用于处理 SAML请求的URL。客户端的设置选项卡中可以设置多个URL。



单击 **Save** (保存)。此动作创建客户端并将您带到 **设置** 选项卡。

以下是设置的一部分：

1. **名称** - **Casdoor**. 这只用于在Keycloak用户界面中向Keycloak用户显示友好的名称。您可以使用任何您喜欢的名字。
2. **已启用** - 选择 **on**。
3. **包含 Authn 语句** - 选择 **on**。
4. **签署文件** - 选择 **on**。
5. **签名断言** - 选择 **off**。
6. **加密断言** - 选择 **off**。
7. **需要客户签名** - 请选择 **off**。
8. **强制名称ID格式** - 选择 **on**。
9. **名称 ID 格式** - 选择 **username**。
10. **有效重定向 URI** - 添加 **http://localhost:8000/api/acs**。
11. **Master SAML 处理 URL** - **http://localhost:8000/api/acs**。
12. 精良的谷物SAML端点配置
 - i. **声明消费者服务公开绑定URL** - **http://localhost:8000/api/acs**。
 - ii. **声明消费者服务重定向绑定URL** - **http://localhost:8000/api/acs**。

保存该配置。

The screenshot shows the Keycloak administration interface with the following details:

- Left Sidebar:** Shows the navigation menu with "Casdoor" selected under "Clients". Other options include "Configure", "Realm Settings", "Client Scopes", "Roles", "Identity Providers", "User Federation", and "Authentication".
- Header:** Shows the URL "Clients > http://localhost:8000/api/acs" and a user "Admin".
- Main Content:** The "Settings" tab is active, showing the following configuration for the client "Casdoor":
 - Client ID:** http://localhost:8000/api/acs
 - Name:** Casdoor
 - Description:** (empty)
 - Enabled:** ON
 - Always Display in Console:** OFF
 - Consent Required:** OFF
 - Login Theme:** (dropdown menu)
 - Client Protocol:** saml
 - Include AuthnStatement:** ON
 - Include OneTimeUse Condition:** OFF
 - Force Artifact Binding:** OFF
 - Sign Documents:** ON
 - Optimize REDIRECT signing key lookup:** OFF
 - Sign Assertions:** OFF
 - Signature Algorithm:** RSA_SHA256
 - SAML Signature Key Name:** KEY_ID
 - Canonicalization Method:** EXCLUSIVE
 - Encrypt Assertions:** OFF
 - Client Signature Required:** OFF
 - Force POST Binding:** OFF
 - Front Channel Logout:** ON
 - Force Name ID Format:** ON
 - Name ID Format:** username
 - Root URL:** (empty)
 - Valid Redirect URLs:** http://localhost:8000/api/acs (with a minus sign and plus sign for modification)
 - Base URL:** (empty)
 - Master SAML Processing URL:** http://localhost:8000/api/acs
 - IDP Initiated SSO URL Name:** (empty)
 - IDP Initiated SSO Relay State:** (empty)
- Advanced Options:** "Fine Grain SAML Endpoint Configuration" and "Advanced Settings" sections are collapsed.
- Bottom:** "Save" and "Cancel" buttons.

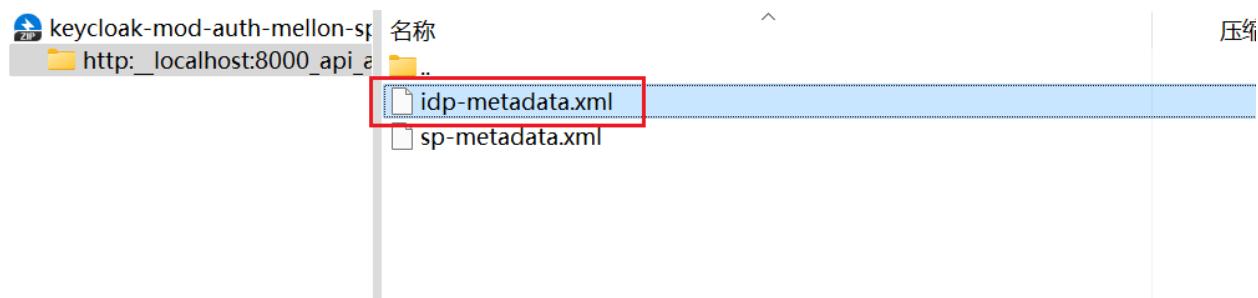
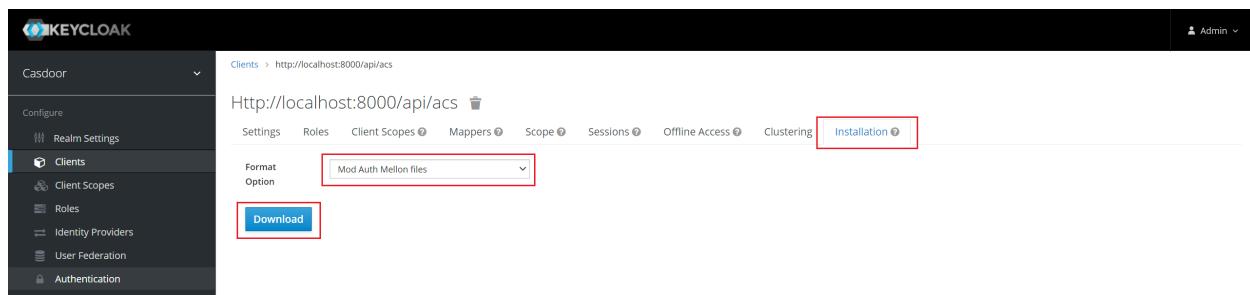
💡 提示

如果您想要签署authn请求，您需要启用**客户端签名要求**选项，并上传自己生成的证书。在Casdoor中使用的私钥和证书，`token_jwt_key.key` 和 `token_jwt_key.pem`，位于**object**目录中。在Keycloak中，您需要点击**密钥**选项卡，点击**导入**按钮，选择**档案格式为证书PEM**，并上传证书。

点击**安装**标签页。

对于 Keycloak <= 5.0.0，选择格式选项 - **SAML Metadata IDPSSODescriptor** 并复制元数据。

对于Keycloak 6.0.0+，选择格式选项 - **Mod Mellon 文件** 并点击**下载**。解压下载的.zip文件，找到 `idp-metadata.xml`，并复制元数据。



在Casdoor配置

在 Casdoor 中创建一个新的提供商。

选择分类为 SAML, 输入 Keycloak. 将metadata的内容复制并粘贴到元数据字段中。 点击解析按钮后, 端点、IdP和发行者URL的值将自动生成。 最后, 点击保存按钮。

💡 提示

如果您在 Keycloak 中启用 **客户端签名需要** 选项并上传证书, 请在 Casdoor 中启用 **签名请求** 选项。

Name ⓘ: keycloak-casdoor

Display name ⓘ: keycloak-casdoor

Category ⓘ: SAML

Type ⓘ: Keycloak

Client ID ⓘ:

Client secret ⓘ:

Sign request ⓘ:

Metadata ⓘ: <md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realm/casdoor"><md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo><ds:KeyName>qpm-3k76jG-na5Zc3uPI7bp-4wYtMbWMp2wqUHAY</ds:KeyName><ds:X509Data><ds:X509Certificate>MIICnTCAYUCBgF9pAmxSDANBqkjhkiG9w0BAQsFADASMR AwDgYDVQQDDAdjYXNkb29yMB4XDThMTIxMDExMDg1OFoXDTMxMTIxMDExMTAzOFowEjEQMA4GA1UEAwWWY2FzZG9vcjCCASlwDQYKoZlhvNA

Parse

Endpoint ⓘ: http://localhost:8080/auth/realm/casdoor/protocol/saml

IdP ⓘ: MIICnTCAYUCBgF9pAmxSDANBqkjhkiG9w0BAQsFADASMR AwDgYDVQQDDAdjYXNkb29yMB4XDThMTIxMDExMDg1OFoXDTMxMTIxMDExMTAzOFowEjEQMA4GA1UEAwWWY2FzZG9vcjCCASlwDQYKoZlhvNAQEBBQADggEPADCCAQ

Issuer URL ⓘ: http://localhost:8080/auth/realm/casdoor

SP ACS URL ⓘ: http://localhost:8000/api/acs **Copy**

SP Entity ID ⓘ: http://localhost:8000/api/acs **Copy**

Provider URL ⓘ: https://github.com/organizations/xxx/settings/applications/1234567

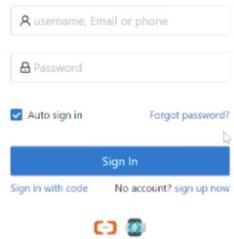
编辑您想要在 Cassdoor 中配置的应用程序。 选择你刚刚添加的提供商, 然后点击保存按钮。

Providers ⓘ:	Add	Name	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
		casdoor-idaas	SAML						
		keycloak-casdoor	SAML						

验证效果

转到您刚刚配置的应用程序, 您会在登录页面上找到一个Keycloak图标。

点击图标，您将被重定向到Keycloak登录页面。成功认证后，您将登录到Casdoor。



阿里巴巴云IDaaS

在阿里巴巴云IDaaS中创建SAML应用

登录到[阿里巴巴云管理控制台](#)，搜索并进入应用程序身份服务（身份即服务，IDaaS）。

The screenshot shows the Alibaba Cloud Management Console interface. The top navigation bar includes links for Home, Workstation, and various services like SAML, ICP, and App. The main content area is titled "概览页" (Overview Page) under "应用身份管理" (Application Identity Management). A central section is titled "IDaaS (Identity-as-a-Service) 是为企业客户提供的身份访问管理服务, IDaaS支持 EIAM 和 CIAM" (IDaaS provides identity access management services for enterprise customers, supporting EIAM and CIAM). It compares EIAM (Employee Identity & Access Management) and CIAM (Customer Identity & Access Management System). Below this is a table comparing EIAM Standard Edition and Enterprise Edition across various features like single sign-on, user quota, and integration with external systems. To the right, there's a QR code for customer support and a "Help Documents" sidebar with links to various EIAM and CIAM documentation.

点击 EIAM 实例列表 并打开免费版本。

The screenshot shows the "EIAM 实例列表" (EIAM Instance List) page. The left sidebar has a red box around the "EIAM 实例列表" link under "应用身份管理". The main content area shows a table with columns for "实例ID/名称" (Instance ID/Name), "标准版实例ID" (Standard Edition Instance ID), "状态 (全部)" (Status (All)), "规格授权" (Specification Authorization), "最大用户数" (Max User Count), "到期时间" (Expiration Time), "产品版本" (Product Version), "用户登录页地址" (User Login Page Address), and "实例开放接口域名" (Instance Open Interface Domain Name). A large blue button labeled "开通免费版" (Launch Free Edition) is visible in the top right corner. The bottom of the page shows pagination controls.

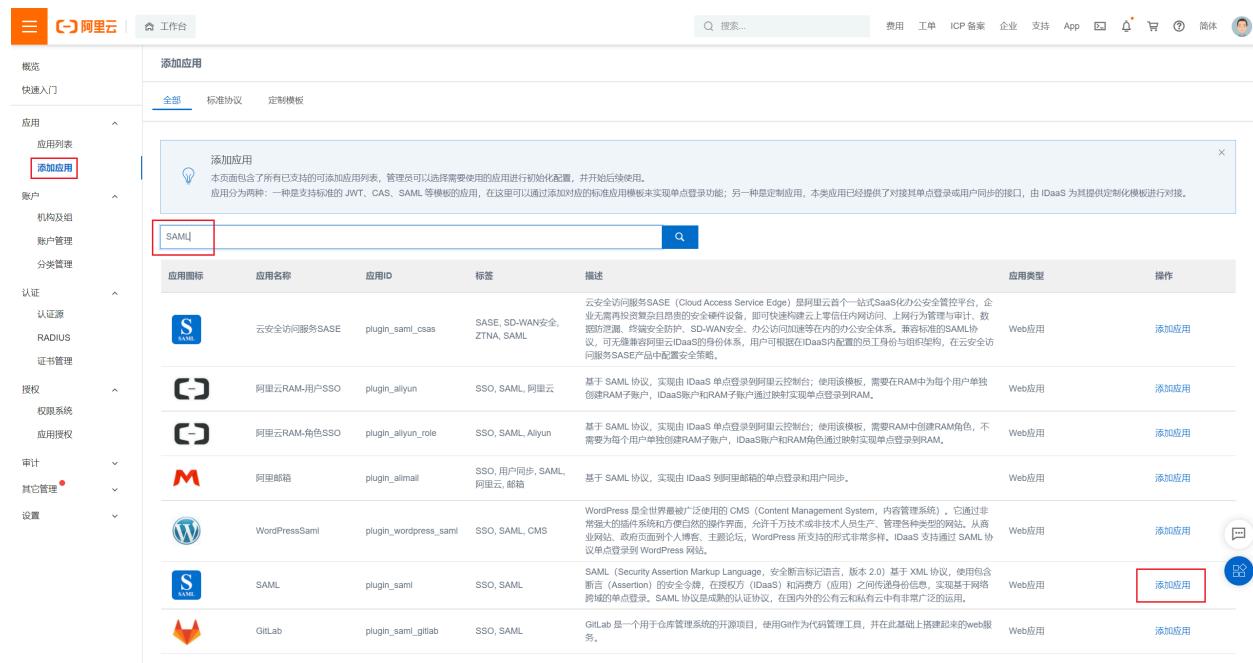
打开后将自动创建并运行一个实例。点击实例名称或 管理 按钮来输入 IDaaS 管理控制台。



EIAM 实例列表

实例ID/名称	标准版实例ID	状态 (全部) ▾	规格授权	最大用户数	到期时间	产品版本	用户登录页地址	实例开放接口域名	操作
idaas-cn-shanghai		运行中	免费版	100	-	V1.9.6-GA			管理

输入了 IDaaS 管理控制台后，点击 添加应用程序，搜索 SAML，然后点击 添加应用程序



添加应用

应用图标	应用名称	应用ID	标签	描述	应用类型	操作
S	云安全访问服务SASE	plugin_saml_cas	SASE, SD-WAN安全, ZTNA, SAML	云安全访问服务SASE (Cloud Access Service Edge) 是阿里云首个一站式SaaS办公云安全管控平台，企业无需再投资复杂的堡垒机设备，即可快速构建云上零信任内网访问、上网行为稽查与审计、数据防泄漏、终端全盘加密、SD-WAN安全、办公访问限速等在内的办公云安全体系。兼容标准的SAML协议，可无缝兼容阿里云IDaaS的身份体系，用户可根据在IDaaS中配置的员工身份与组织架构，在云安全访问服务SASE产品中设置安全策略。	Web应用	添加应用
C	阿里云RAM-用户SSO	plugin_aliyun	SSO, SAML, 阿里云	基于 SAML 协议，实现由 IDaaS 单点登录到阿里云控制台；使用该模板，需要在 RAM 中为每个用户单独创建 RAM 子账户，IDaaS 账户和 RAM 子账户通过映射实现单点登录到 RAM。	Web应用	添加应用
C	阿里云RAM-角色SSO	plugin_aliyun_role	SSO, SAML, Aliyun	基于 SAML 协议，实现由 IDaaS 单点登录到阿里云控制台；使用该模板，需要 RAM 中创建 RAM 角色，不需要为每个用户单独创建 RAM 子账户，IDaaS 账户和 RAM 角色通过映射实现单点登录到 RAM。	Web应用	添加应用
M	阿里邮箱	plugin_aimail	SSO, 用户同步, SAML, 阿里云, 邮箱	基于 SAML 协议，实现由 IDaaS 到阿里邮箱的单点登录和用户同步。	Web应用	添加应用
W	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress 是全世界最流行的泛应用的 CMS (Content Management System, 内容管理系统)，它通过非常强大的插件系统和开放的自然的操作界面，允许千万技术爱好者生产、管理各种类型的网站。从商业网站、政府网站到个人博客、主题论坛，WordPress 所支持的形式非常多样。IDaaS 支持通过 SAML 协议单点登录到 WordPress 网站。	Web应用	添加应用
S	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全断言标记语言，版本 2.0) 基于 XML 协议，使用包含断言 (Assertion) 的安全令牌，在授权 (IDaaS) 和消费者 (应用) 之间传递身份信息，实现基于网络安全的单点登录。SAML 协议是成熟的身份协议，在国内外的公司和机构有非常多的应用。	Web应用	添加应用
G	GitLab	plugin_saml_gitlab	SSO, SAML	GitLab 是一个用于仓库管理系统的开源项目，使用 Git 作为代码管理工具，并在此基础上搭建起来的 web 服务器。	Web应用	添加应用

点击 添加签名密钥。

添加应用 (SAML)

×

导入SigningKey	添加SigningKey	别名	序列号	有效期	秘钥算法	算法长度	操作
暂无数据							

填写所有必需的信息并提交。

添加SigningKey

×

* 名称	CASDOOR-TEST
部门名称	请输入部门名称
公司名称	请输入公司名称
* 国家	CN
* 省份	Beijing
城市	请输入城市
* 证书长度	1024
* 有效期	3 年
提交	取消

选择添加的签名密钥。

添加应用 (SAML)

×

操作					
别名	序列号	有效期	秘钥算法	算法长度	
CN=CASDOOR-TEST, ST=Beijing, C=CN	3322747020095790430	1095	RSA	1024	<button>选择</button> <button>导出</button>

填写下面所需的所有信息并保存。

- IDP 身份ID：保持与签发者地址在 Casdoor 中相同。
- SP 实体 ID & SP ACS URL (SSO 定位)：现在填写您想要的任何东西。完成 Casdoor 配置后，您需要修改。
- 描述属性：直接填充为用户名。
- 账户关联模式：账户协会

添加应用 (SAML)

X

图片大小不超过1MB

应用ID

idaas-cn-shanghai-pvl0hq0ojppugin_saml

* 应用名称

CASDOOR-SAML

* IDP IdentityId

CASDOOR

IDP IdentityId is required

* SP Entity ID

http://localhost

SP Entity ID is required

* SP ACS URL(SSO Location)

http://localhost

* NameIdFormat

urn:oasis:names:tc:SAML:2.0:nameid-format:transient

v

* Binding

POST

v

SP 登出地址

请输入 SP 登出地址

Assertion Attribute

username

应用子账户

v

-

+

断言属性。设值后，会将值放入 SAML 断言中。名称为自定义名称，值为账户的属性值。

Sign Assertion



IDaaS发起登录地址

IDaaS发起登录地址

以 http://、https:// 开头，填写后使用 IDaaS 发起登录将会跳转到该地址，而不会使用 SAML 的 IdP 发起登录流程

* 账户关联方式

账户关联 (系统按主子账户对应关系进行手动关联，用户添加后需要管理员审批)

账户映射 (系统自动将主账户名称或指定的字段映射为应用的子账户)

提交

取消

帐户授权 & 关联

在 SAML 应用成功添加后，授权提示会高亮。现在不要授权它，添加一个帐户，然后授权它。

转到组织和组，然后点击新帐户。

The screenshot shows the Alibaba Cloud Organization Structure Management interface. On the left sidebar, under the '账户' (Account) category, the '机构及组' (Organizational Units and Groups) option is selected and highlighted with a red box. In the main content area, there is a large callout box titled '机构及组' (Organizational Units and Groups) with the following text:
管理员在当前页面对组织架构、部门及其包含的组、账户进行管理，也可以使用AD、LDAP或Excel文件的方式配置导入或同步。
在左侧的组织架构树中，可以右键点击某个部门对其进行操作，也可以左键选择某个部门，并在右侧为其进行创建账户、创建组、创建部门等操作。

The main panel is titled '组织架构' (Organizational Structure) and contains a search bar with '新账账户' (Create New Account) highlighted by a red box. Below the search bar is a table with one row of data:

编号	账户名称	显示名称	类型	目录	操作
1	idaas_manager	默认管理员	自建账户	/	修改 账户同步 同步记录

At the bottom right of the table, there is a pagination bar showing '共1条' (1 item), page number '1', and a '10条/页' (10 items per page) dropdown.

填写所有必需的信息并提交。

新建账户

X

账户属性

扩展属性

父级组

父级

阿里云IDaaS

* 账户名称

casdoor

账户名称不能以特殊字符开始，可包含大写字母、小写字母、数字、中划线(-)、下划线(_)、点(.)，长度至少 4 位

* 显示名称

casdoor

* 密码

密码中必须包含大小写字母+数字+特殊字符的组合;长度至少 10 位，密码不能包含"<"和">"。

邮箱

请输入有效的邮箱地址

手机号或邮箱至少填写一个。

手机号

+86 ▾ 151 123456789

手机号或邮箱至少填写一个。

外部ID

外部ID

IDaaS 平台中的唯一身份标识, 若不填将由系统自动生成。

过期时间

过期时间

不填将使用系统默认过期时间 2116-12-31

备注

备注

用户备注信息

提交

取消

转到 **应用程序授权**, 选择您想要授权的帐户, 然后点击 **保存**。

The screenshot shows the 'Application Authorization' section of the Alibaba Cloud IAM console. On the left sidebar, under the '授权' (Authorization) category, '应用授权' (Application Authorization) is selected and highlighted with a red box. The main panel displays a table of accounts associated with the application 'CASDOOR-SAML'. One account, 'casdoor', is selected and highlighted with a red box. A large blue '保存' (Save) button is visible at the bottom of the table area.

前往 应用程序列表, 点击 查看应用子账户, 然后点击 添加帐户关联。

The screenshot shows the 'Application List' section of the Alibaba Cloud IAM console. On the left sidebar, '应用列表' (Application List) is selected and highlighted with a red box. The main panel displays a table of applications. One application, 'CASDOOR-SAML', is selected and highlighted with a red box. In the '操作' (Operations) column for this application, there is a blue '授权' (Authorization) button and a red '详情' (Details) button. The '查看详情' (View Details) link in the '应用信息' (Application Information) section of the details panel is also highlighted with a red box.

The screenshot shows the Alibaba Cloud IDaaS application management interface. On the left, there is a sidebar with various navigation options like '概览', '快速入门', '应用' (with '应用列表' highlighted), '账户', '认证', '授权', etc. The main content area has a breadcrumb navigation '应用列表 / 子账户'. A modal window titled '子账户' (Sub-account) is open, containing a detailed explanation of what a sub-account is and how it relates to the main account. Below the modal, there is a table titled 'CASDOOR-SAML' with columns: 账户名称 (Account Name), 显示名称 (Display Name), 子账户 (Sub-account), 子账户密码 (Sub-account Password), 是否关联 (Is Associated), 审批状态 (Review Status), 关联时间 (Association Time), and 操作 (Operations). The table shows '暂无数据' (No data available). At the top right of the main content area, there are three buttons: '添加账户关联' (Add Account Association) with a red border, '批量导入' (Batch Import), and '批量导出' (Batch Export).

填写需要关联的主账户和子账户，然后点击 **保存**。

主账户存在于IDaaS中，子账户是Cassdoor用户的ID。

The screenshot shows the 'Add Account Association' dialog box. It has two input fields: one for the '主账户' (Main Account) labeled 'casdoor' and another for the '子账户' (Sub-account) labeled '52908237-fa4c-4681-b636-a6afce22fb2e'. At the bottom, there are two buttons: a blue '保存' (Save) button and a white '返回' (Back) button.

导出 IDaaS 元数据

转到 **应用程序列表**, 点击 **查看应用程序详细信息** 然后点击 **导出 IDaaS SAML Metadada**

The screenshot shows the Alibaba Cloud IAM application management interface. On the left, there's a sidebar with various navigation items like '概览', '快速入门', '应用' (selected), '账户', '认证', '审计', '其它管理', and '设置'. The main area has tabs for '应用列表' and '添加应用'. Under '应用列表', it says '管理员可以在当前页面管理已经添加的所有应用，应用可以实现单点登录和数据同步能力。当添加成功后，应该确认应用处于启用状态，并已经完成了授权。在应用详情中，可以看到应用的详细信息。' Below this, there's a table with columns '应用图标', '应用名称', and '应用ID'. One row shows 'CASDOOR-SAML', 'idaas-cn-shanghai...', and 'saml'. To the right, a detailed view for '应用详情 (CASDOOR-SAML)' is shown. It includes sections for '图标' (SAML logo), '应用ID' (idaas-cn-shanghai..._jin_saml), '应用名称' (CASDOOR-SAML), '应用Uuid' (d9bd59093c5c031b7abbb0efa849f7bRxS506SQ3y7), '应用信息' (显示了应用的详细信息、查看详情、修改应用、删除应用), '认证信息' (显示了应用的单点登录地址、IDaaS发起地址), '授权信息' (显示了应用与人员组织的授权关系), and '审计信息' (显示了查看应用系统详细的操作日志、查看日志、查看同步记录). The 'IDP IdentityId' field contains 'CASDOOR' with a red box around it, and a link '导出 IDaaS SAML 元配置文件 | 立即轮转密钥 | 导入'.

在 Casdoor 配置

在 Casdoor 中创建一个新的提供商。

选择类别为**SAML**, 类型为**阿里云IdaaS**。 复制元数据内容并粘贴到 **元数据** 输入。 **端点**, **的值**, **IdP** 和 **发行商URL** 将在点击 **分析** 按钮后自动生成。

Name ⓘ :	casdoor-idaas	
Display name ⓘ :	casdoor-idaas	
Category ⓘ :	SAML	
Type ⓘ :	Aliyun IDaaS	
Client ID ⓘ :		
Client secret ⓘ :		
Metadata ⓘ :	<pre><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aliyunidaas.com/charon/api/applications/plugin_idaas/charon"> <md:SPSSOServiceBinding Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aliyunidaas.com/charon/api/applications/plugin_idaas/charon"/> </md:SingleSignOnService> </md:IDPSSODescriptor> </md:EntityDescriptor></pre>	
<input style="margin-right: 10px;" type="button" value="Parse"/> Success		
Endpoint ⓘ :	https://dvmoykbkx.login.aliyunidaas.com/enduser/api/application/plugin_saml/idaas-cn-shanghai	
IdP ⓘ :	MIIByzCAVcGAwIBAgIILhzEz2NMHV4wDQYJKoZIhvNAQEFBQAwNjELMAkGA1UEBhMCQ04xE DAOBgNVBAgT B0JlaWppbmcxFTATBgNVBAMTDENBU0RPTIItVEVTVDaeFw0yMTEyMDkwNzEyMTFaFw0yNDEyMDgwNzEyMTFaMDYxCzAJE	
Issuer URL ⓘ :	CASDOOR	
SP ACS URL ⓘ :	http://localhost:8000/api/acs	<input type="button" value="Copy"/>
SP Entity ID ⓘ :	http://localhost:8000/api/acs	<input type="button" value="Copy"/>
Provider URL ⓘ :	https://github.com/organizations/xxx/settings/applications/1234567	

复制 SP ACS URL 和 SP 实体 ID 并点击 保存 按钮

编辑您想要在 Cassdoor 中配置的应用程序。选择刚刚添加的提供者，然后点击按钮 **保存**。

Providers	②
Providers	Add
Name	Category
casdoor-idaas	SAML
Preview	②
Test signup page.	Test signin page.

在阿里云IDaaS中修改SAML应用

禁用应用程序，然后点击 **修改应用程序**。

The screenshot shows the Alibaba Cloud Application Management interface. On the left, there's a sidebar with categories like Application, Account, Authentication, Authorization, Audit, and Settings. The main area is titled '应用列表' (Application List) and shows a table with columns: 应用图标 (Application Icon), 应用名称 (Application Name), 应用ID (Application ID), 设备类型 (Device Type), 应用状态 (Application Status), 二次认证状态 (Two-factor authentication status), and 操作 (Operations). A row for 'CASDOOR-SAML' is selected, with its icon highlighted. The '操作' column for this row has a red box around it. Below the table, there are tabs for '应用信息' (Application Information), '认证信息' (Authentication Information), '账户信息 - 同步' (Account Information - Sync), and '账户信息 - 子账户' (Account Information - Sub-account). The '应用信息' tab is active. It shows fields like '应用的详细信息' (Detailed information about the application), '应用的单点登录地址' (Single sign-on address), 'IDaaS发起地址' (IDaaS initiation address), '同步机构' (Sync institution), and 'SCIM配置' (SCIM configuration). There are also buttons for '查看详情' (View details), '修改应用' (Edit application), and '删除应用' (Delete application). The '认证信息' tab shows '查看应用系统详细的操作日志' (View detailed operation logs for the application system). The '账户信息 - 同步' tab shows '是否对应用开放系统API' (Whether to open system API for the application), 'API Key', 'API Secret', and 'IP 白名单配置' (IP white list configuration). The '账户信息 - 子账户' tab shows '管理应用内权限' (Manage permissions within the application). At the bottom, there are pagination controls: '共 1 条' (1 page), a page number input field with '1', and a '10条/页' (10 items per page) dropdown.

填写 SP 实体 ID and SP ACS URL (SSO location) 将内容复制到Casdoor。 提交并启用应用程序。

修改应用 (CASDOOR-SAML)

×

图标



上传文件

图片大小不超过1MB

应用ID

idaas-cn-shanghai-...\\login_saml

* 应用名称

CASDOOR-SAML

* IDP IdentityId

CASDOOR

IDP IdentityId is required

* SP Entity ID

http://localhost:8000/api/acs

SP Entity ID is required

* SP ACS URL(SSO Location)

http://localhost:8000/api/acs

* NameIdFormat

urn:oasis:names:tc:SAML:2.0:nameid-format:transient

* Binding

POST

SP 登出地址

请输入SP 登出地址

Assertion Attribute

username

应用子账户



断言属性。设值后，会将值放入SAML断言中。名称为自定义名称，值为账户的属性值。

Sign Assertion



IDaaS发起登录地址

IDaaS发起登录地址

以 http://、https://开头，填写后使用 IDaaS 发起登录将会跳转到该地址，而不会使用 SAML 的idp发起登录流程

验证效果

转到您刚刚配置的应用程序，您可以在登录页面找到一个图标。

点击图标，跳转到阿里云IDaaS登录页面，然后在认证后成功登录到Casdoor。



username, Email or phone

Password

Auto sign in [Forgot password?](#)

[Sign In](#)

[Sign in with code](#) No account? [sign up now](#)

A row of social media icons for GitHub, LinkedIn, and others.

支付

概述

将支付提供商添加到您的应用程序

PayPal

将PayPal添加为应用的支付提供商

Stripe

将Stripe支付提供商添加到您的应用程序

支付宝

将支付宝支付提供商添加到您的应用程序

 微信支付

将微信支付提供商添加到您的应用程序

 AirWallex

Add AirWallex payment provider to your application

概述

如果您想在Casdoor中使用支付服务，您需要创建一个支付提供商并将其添加到您的产品中。

The screenshot shows the Casdoor web interface with the 'Providers' tab selected. A new provider is being created with the following details:

- Name: provider_payment_paypal
- Display name: PayPal Payment Provider
- Organization: admin (Shared)
- Category: Payment (highlighted with a red box)
- Type: PayPal (selected from a dropdown menu)
- Client ID: Alipay, Dummy, GC, PayPal (available options)
- Client secret: WeChat Pay (available option)
- Provider URL: (empty field)

At the bottom, there are 'Save' and 'Save & Exit' buttons.

要了解如何配置产品，请参考[产品](#)。配置产品后，您可以为产品添加支付提供商，以便用户可以通过支付提供商购买产品。

PayPal

① 备注

这是一个如何配置PayPal支付提供商的示例。

步骤1：创建一个PayPal应用

首先，你需要在PayPal中创建一个应用。要访问PayPal开发者网站，你应该有一个PayPal商业账户。如果你还没有账户，[先创建一个](#)。

创建PayPal商业账户后，使用你的账户登录到[开发者控制台](#)，然后点击[Apps & Credentials](#)下的[Create App](#)。

The screenshot shows the PayPal Developer Dashboard. At the top, there's a navigation bar with links for Docs, APIs & SDKs, Tools, Help, Business Dashboard, and a user profile icon. Below the navigation is a secondary navigation bar with Home, Apps & Credentials (which is highlighted with a red box), Testing Tools, and Event Logs. To the right of this bar are buttons for Sandbox (which is turned on) and Live. A red arrow points from the text "Sandbox mode" in the middle of the page down to the Sandbox button. The main content area is titled "API Credentials" and contains a yellow banner stating "Viewing sandbox API credentials. [View live credentials](#)". Below the banner is a table titled "REST API apps". The table has columns for "App name", "Client ID", "Secret", and a settings icon. Two rows are listed: "casdoor" with Client ID "AVEu0A_sbq6tnKyOxbeBAcEw0Jcsgbv..." and Secret "....."; and "Default Application" with Client ID "AR6LK9lz8ZkHdt6HIn_N9Jaq3IXY5rVK..." and Secret ".....".

App name	Client ID	Secret	⋮
casdoor	AVEu0A_sbq6tnKyOxbeBAcEw0Jcsgbv...	⋮
Default Application	AR6LK9lz8ZkHdt6HIn_N9Jaq3IXY5rVK...	⋮

您可以在应用的基本信息中找到[Client ID](#)和[Secret key](#)。

[← Back](#)

casdoor

● Viewing sandbox API credentials. [View live credentials.](#)

API credentials

App name casdoor 

Client ID AVEu0A_sbq6ttKyOxbeBAcEw0Jcsgbv2JZvQAtK  

Secret key 1   

[+ Add Second Key](#)

Sandbox account info

[View details](#)

Sandbox URL <https://sandbox.paypal.com> 

Sandbox Region C2

Email sb-qqaiv26894991@business.example.com 

Password *****  

Features

步骤2：创建一个PayPal支付提供商

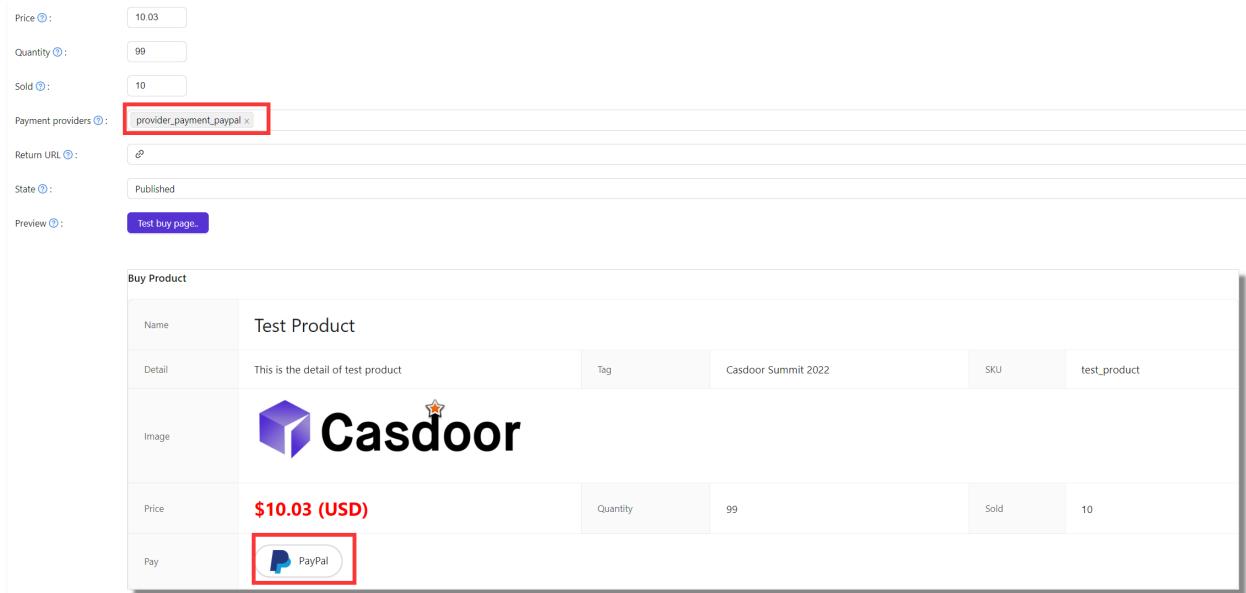
接下来，在Casdoor中创建一个PayPal支付提供商。 填写必要的信息：

名称	PayPal中的名称
Category	选择 <input type="button" value="Payment"/>
Type	选择 <input type="button" value="PayPal"/>

名称	PayPal中的名称
Client ID	使用从步骤1获得的 client ID
Client secret	使用从步骤1获得的 Secret key

步骤3：为你的产品添加PayPal支付提供商

最后，为你的产品添加PayPal支付提供商，这样用户就可以使用PayPal购买产品。



The screenshot shows the Casdoor product configuration page. In the 'Payment providers' field, 'provider_payment_paypal' is selected and highlighted with a red box. Below the form, a preview window displays the product details: Name: Test Product, Detail: This is the detail of test product, Image: Casdoor logo, Price: \$10.03 (USD), and a 'Pay' button with a PayPal icon.

① 备注

以上操作都是在PayPal的 Sandbox 模式下进行的。如果你想在实际生产环境中使用它，你需要在PayPal的 Live 模式下创建一个应用，并在Casdoor的配置文件 conf/app.conf 中设置 runmode=prod。

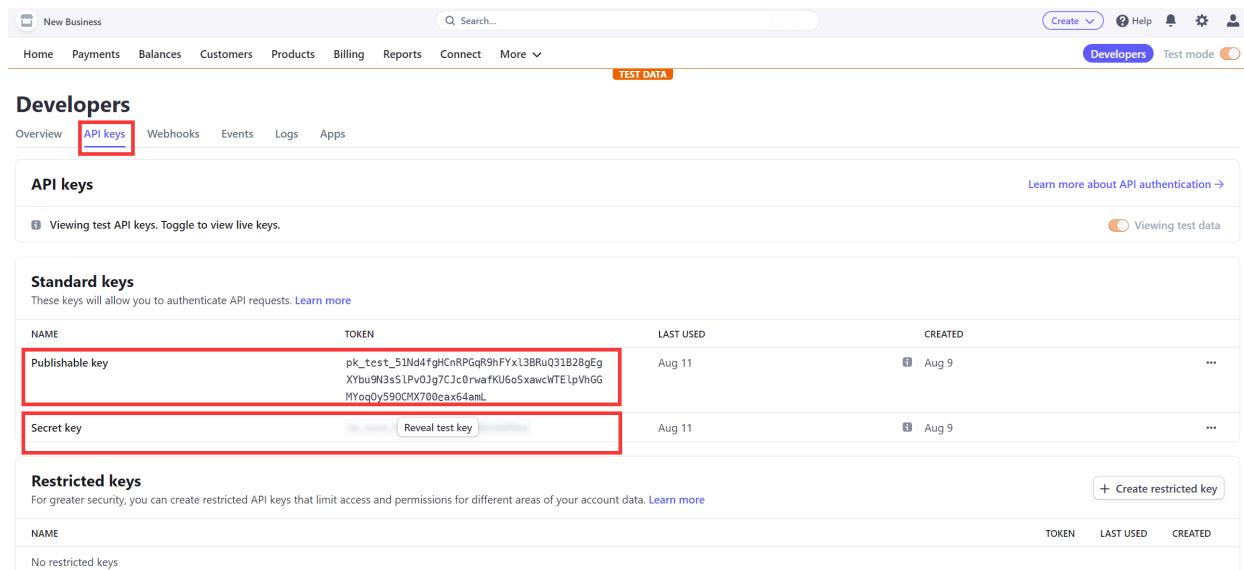
Stripe

① 备注

这是一个如何配置Stripe支付提供商的示例。

步骤1。 获取可发布的密钥和秘密密钥

首先，你需要在Stripe有一个账户。 创建Stripe账户后，使用您的账户凭据登录到开发者仪表板。 您可以在API密钥选项卡下找到可发布的密钥和秘密密钥。



The screenshot shows the Stripe Developers API keys page. The 'API keys' tab is selected. It displays two types of keys: 'Standard keys' and 'Restricted keys'. The 'Standard keys' section contains two rows:

NAME	TOKEN	LAST USED	CREATED	...
Publishable key	pk_test_51Nd4fghCnRPGqR9hFYxL3BRuQ31B28gEgXYbu9N3sLPvOJg7CjcoRwafKU6oSxawcITELphGGMYogqy590CHX700eax64aml	Aug 11	Aug 9	[More]
Secret key	[Reveal test key]	Aug 11	Aug 9	[More]

The 'Restricted keys' section is currently empty.

步骤2。 创建一个Stripe支付提供商

接下来，在Casdoor中创建一个Stripe支付提供商，填写必要的信息。

名称	Stripe中的名称
Category	选择 支付
Type	选择 Stripe
Client ID	从步骤1获取的 可发布的密钥
Client secret	从步骤1获取的 秘密密钥

Edit Provider Save Save & Exit

Name ② :	provider_payment_stripe
Display name ② :	Stripe Payment Provider
Organization ② :	admin (Shared)
Category ② :	Payment
Type ② :	S Stripe
Client ID ② :	pk_test_51Nd4fgHCnRPGqR9hFYxl3BRuQ31B28gEgXYbu9N3sSIPvOjg7CJc0rwafKU6oSxawcWTElpVhGGMYoqOy59OCMX700eax64amL
Client secret ② :	***
Provider URL ② :	🔗

Save Save & Exit

步骤3。 为您的产品添加Stripe支付提供商

最后，为您的产品添加Stripe支付提供商，以便用户可以使用Stripe购买产品。

Currency [?](#) :

Price [?](#) :

Quantity [?](#) :

Sold [?](#) :

Payment providers [?](#) : provider_payment_stripe

Return URL [?](#) :

State [?](#) : Published

Preview [?](#) : [Test buy page.](#)

Buy Product

Name	Test Product	Detail	This is the detail of test product	Tag	Casdoor Summit 2022	SKU	test_product
Image	 Casdoor						
Price	\$10.04 (USD)			Quantity	99	Sold	10
Pay	 PayPal  Stripe						

支付宝

步骤1。准备

首先，您需要在支付宝开放平台拥有一个商家账户。

在访问支付宝之前，需要做一些准备工作。

您可以参考文档 [接入前的准备](#) 以获取更多信息。

1.1 获取APPID

登录支付宝开放平台控制台并[创建一个应用](#)。

如何获取 APPID：[支付宝APPID查询指南](#)

1.2 配置证书

根据[文档](#)生成一个RSA2证书，然后你可以获取 `appPrivateKey.txt` 和 `appPublicKey.txt`。

将证书上传到应用程序，然后您可以下载三个文件：`alipayRootCert.crt`, `appCertPublicKey.crt`, `alipayCertPublicKey.crt`。

在Casoor创建一个名为 `App Cert` 的证书：

名称	支付宝中的姓名
Type	选择 Payment
Certificate	appCertPublicKey.crt 的内容
Private key	appPrivateKey.txt 的内容

The screenshot shows the 'appCertPublicKey' configuration page in Casoor. It includes fields for Organization, Name (set to 'cert_alipay_app'), Display name (set to 'Cert Alipay'), Scope (set to 'JWT'), Type (set to 'Payment'), Crypto algorithm (set to 'RS256'), Bit size (set to 4096), and Expire in years (set to 20). A 'Certificate' field contains the base64-encoded certificate content. Below it, a 'Copy certificate' button and a 'Download certificate' button are visible. To the right, there are 'Copy private key' and 'Download private key' buttons. The certificate content starts with:

```
-----BEGIN CERTIFICATE-----
MIIEyCAQBgAwIBAgICIDC8BgDQGQxCu0bjpUDeuDGjANBgkqhkiGvwoBAAQsFADCBgELMAKgA1UE
BhMCQ04aJAUbgVBAmoDUFu0dBGw5WhmNpWwvD4e8NVNaM0NlcR2pZmlyXrbzb2qDxV0
aG9yaXR5MTxwYXVvdVYDQQDDBbbBnQgrmWVUpSjWfWfENrEq2mNyXrbzb4qXVQa9yxR5lE1Ns
YXzNzIEdjgjwRhchMjWmAD2MT1EOOTM1WhnMcwM1A1MTEDOTM1WhnMcwM1BjM0QwCQYIVQzGgeWjDfjq
MCg4IAUECpwuSYXLsp5jY2h5ocd5e+56ef5oqj5p5j6Zm7Q5Yw5Y+4M0QwDQyDVQQLDA2BbDg
YXxkxjwbgNVBAMhMTtivoDgNDE2NTY3NdyM1TEMjAyM1TauMExneryMTM2DCCAsDQVYk2I
-----END CERTIFICATE-----
```

The certificate content continues with a large base64 string.

在Casoor创建一个名为 Root Cert 的证书:

名称	支付宝中的名称
Type	选择 Payment
Certificate	alipayCertPublicKey.crt 的内容
Private key	alipayRootCert.crt 的内容

步骤2。 创建一个支付宝支付提供商

接下来，在Casdoor中创建一个支付宝支付提供商，填写必要的信息。

名称	支付宝中的姓名
Category	选择 Payment
Type	选择 Alipay
Client ID	从步骤1.1获取的 APPID
Cert	App Cert 在步骤1.2中配置
Root Cert	Root Cert 在步骤1.2中配置

Edit Provider

[Save](#) [Save & Exit](#)

Name <small>②</small> :	provider_payment_alipay
Display name <small>②</small> :	Alipay Payment Provider
Organization <small>②</small> :	admin (Shared)
Category <small>②</small> :	Payment
Type <small>②</small> :	 Alipay
Client ID <small>②</small> :	2021003117621368
Client secret <small>②</small> :	
Cert <small>②</small> :	cert_alipay_app
Root Cert <small>②</small> :	cert_alipay_root
Provider URL <small>②</small> :	

[Save](#) [Save & Exit](#)

步骤3。为您的产品添加支付宝支付提供商

最后，为您的产品添加支付宝支付提供商，以便用户可以使用支付宝购买产品。

Quantity <small>②</small> :	99
Sold <small>②</small> :	10
Payment providers <small>②</small> :	provider_payment_paypal  provider_payment_stripe  provider_payment_wechat  provider_payment_alipay 
Return URL <small>②</small> :	
State <small>②</small> :	Published
Preview <small>②</small> :	Test buy page

Buy Product

Name	Test Product				
Detail	This is the detail of test product				
Image					
Price	¥ 0.01 (CNY)	Quantity	99	Sold	10
Pay	 PayPal	 Stripe	 WeChat Pay	 Alipay	

[Save](#) [Save & Exit](#)

微信支付

步骤1. 准备工作

首先，你需要在[微信商户平台](#)拥有一个商户账户。

在接入微信支付之前，需要做一些准备工作。

你可以参考文档[接入前的准备](#)以获取更多信息。

1.1 获取API密钥v3

登录微信商户平台，选择[账户设置 > API安全 > 设置APIv3密钥](#)，然后点击[设置APIv3密钥](#)获取[API密钥v3](#)。

The screenshot shows the left sidebar of the WeChat Merchant Platform with the 'API Security' tab selected. The main content area has two sections:

- API certificate**: This section displays a success message: "You have successfully applied for the certificate at 2020-03-13 17:17". It includes a 'View' and 'Change' button.
- Set APIv3 Secret**: This section contains a note: "This key is used to encrypt messages in APIv3's 'download platform certificate' and 'payment callback notification'". Below is a text input field labeled "Set APIv3 Secret" and a green "Set APIv3 Secret" button. The entire "Set APIv3 Secret" section is highlighted with a red border.

如何获取 API密钥v3：APIv3密钥设置

1.2 获取商户证书

你可以登录微信商户平台，并选择账户设置 > API安全 > API证书 下载证书。

The screenshot shows the WeChat Pay API Security settings page. On the left, there is a sidebar with the following menu items:

- Operating Certificate
- API Security** (highlighted in green)
- Staff Management
- Settlement Info
- Agreement
- Merchant Information

The main content area has a header "API certificate". Below it, there is a sub-section titled "API certificate (CA issued)". It contains the text: "API certificate are used to identify and define your ID; Some of the APIs with higher security lever will require the certificate to identify you to avoid the loss caused by possible ID theft." There is also a note: "To better protect the security of merchant accounts, WeChat pays to provide merchants with an API certificate issued by an authoritative CA from June 2018." A green "Apply" button is located on the right side of this section. Below this, there is another section titled "API security" with a note: "In the API call to the specified rules used to sign your request parameters, the server will receive your request for signature verification, both to define your identity can also prevent other people maliciously tamper with the request data. Some APIs are securely hardened using API key signing alone. Some APIs that require more security will require both AP key signature and API certificate to be securely consolidated."

下载证书后，根据如何查看证书序列号获取证书序列号，并根据如何获取证书的私钥获取私钥。

然后，在Casdoor创建一个证书并填写必要的信息。

The screenshot shows the 'Edit Cert' page in Casdoor. On the left, there are fields for Organization (admin (Shared)), Name (cert_wechatpay), Display name (Cert Wechatpay), Scope (JWT), Type (Payment, highlighted with a red box), Crypto algorithm (RS256), Bit size (4096), and Expiry in years (20). Below these are buttons for 'Copy certificate' and 'Download certificate'. A red box highlights the certificate serial number: 31:aaaaaaaaaaaaaaaaaaaa032FCFD864829CC51AA6E1986. On the right, there is a 'Private key' section with a 'Copy private key' button and a large text area containing a long string of characters representing the private key, also highlighted with a red box.

1.3 获取商户ID和应用ID

如何获取 商户ID：[微信支付商户ID查询指南](#)

如何获取 应用ID：[微信支付APPID查询指南](#)

步骤2. 创建一个微信支付提供商

接下来，在Casdoor中填写必要的信息创建一个微信支付提供商。

名称	微信支付中的名称
Category	选择 支付
Type	选择 微信支付
Client ID	从步骤1.3获取的 商户ID

名称	微信支付中的名称
Client secret	从步骤1.1获取的 API密钥v3
App ID	从步骤1.3获取的应用ID
Cert	在步骤1.2配置的证书

Edit Provider
Save
Save & Exit

Name ②:

provider_payment_wechat

Display name ②:

Wechat Payment Provider

Organization ③:

admin (Shared)

Category ②:

Payment

Type ②:

WeChat Pay

Client ID ②:

1619999244

Client secret ②:

App ID ②:

wxe933a9cd81c396d1

Cert ②:

cert_wechatpay

Provider URL ②:

Save
Save & Exit

步骤3. 为您的产品添加微信支付提供商

最后，为您的产品添加微信支付提供商，以便用户可以使用微信支付购买产品。

Currency : CNY

Price : 0.01

Quantity : 99

Sold : 10

Payment providers : provider_payment_paypal x provider_payment_stripe x provider_payment_wechat x

Return URL : /p

State : Published

Preview : [Test buy page.](#)

Buy Product

Name	Test Product
Detail	This is the detail of test product
Image	
Price	¥ 0.01 (CNY)
Quantity	99
Sold	10

Pay   

支持JSAPI支付

目前， Casdoor支持微信支付中的[JSAPI支付](#)和[原生支付](#)。

要支持JSAPI支付，你应该配置一个支持[微信媒体平台](#)的[微信OAuth提供商](#)。微信OAuth提供商的[客户端ID](#) 和微信支付提供商的[应用ID](#)需要相同。

[Edit Provider](#) [Save](#) [Save & Exit](#)

Name ②:	provider_casdoor_wechat
Display name ②:	Casdoor WeChat
Organization ②:	admin (Shared)
Category ②:	OAuth
Type ②:	WeChat
Client ID ②:	wx049c70e6c2027b0b
Client secret ②:	***
Client ID 2 ②:	wxe933a9cd81c396d1
Client secret 2 ②:	***
Enable QR code ②:	<input checked="" type="checkbox"/>
Provider URL ②:	https://open.weixin.qq.com/

[Save](#) [Save & Exit](#)

[Edit Provider](#) [Save](#) [Save & Exit](#)

Name ②:	provider_payment_wechatpay
Display name ②:	Payment - WeChatPay
Organization ②:	admin (Shared)
Category ②:	Payment
Type ②:	WeChat Pay
Client ID ②:	1619999244
Client secret ②:	***
App ID ②:	wxe933a9cd81c396d1
Cert ②:	cert_wechatpay
Provider URL ②:	https://pay.weixin.qq.com/index.php/core/cert/api_cert/#/

[Save](#) [Save & Exit](#)

用户通过微信登录后（在移动场景中，例如微信移动应用内的微信内置浏览器），可以基于JSAPI支付使用微信支付购买产品。

AirWallex

 备注

This is an example of how to configure a AirWallex payment provider.

Step 1. Get Client ID and API Key

First, you need to have an account at [AirWallex](#). After creating an AirWallex account, log in to the [Developer Dashboard](#) using your account credentials. You can find the `CLIENT ID` and `API KEY` under the `API Keys` tab, or add a new custom permission key.

YOUR CORP
YOUR CORP

Guides API Keys Webhooks

whisper@example.com

Manage your API keys

Create restricted API key

NAME	CLIENT ID	API KEY	CREATION DATE
casdoor_test	test_BLXd98nQWkj8K\$Tx1Bi5	3296c48013cb1a80ffecfb285515854768272214040a585...	2025-02-07 ...

Dashboard Wallet Transfers Cards Expenses Bills Payments Reports Rewards Account

User Management Connections Approvals **Developer** Statements Settings

≡ Airwallex

Step 2. Create an AirWallex Payment provider

Next, create an AirWallex Payment provider in Casdoor by filling in the necessary information.

Name	Name in AirWallex
Category	choose Payment
Type	choose AirWallex

Name	Name in AirWallex
Client ID	CLIENT_ID obtained from Step 1
Client secret	API_KEY obtained from Step 1

The screenshot shows the Casdoor interface for managing identity providers. The top navigation bar includes Home, User Management, Identity (which is selected and highlighted in blue), Authorization, Logging & Auditing, Business & Payments, and Admin.

The main form is titled "Edit Provider" and contains the following fields:

- Name: airwallex_test
- Display name: AirWallex Sandbox
- Organization: admin (Shared)
- Category: Payment
- Type: AirWallex
- Client ID: test_BLXd98nQWkj8K\$Tx1Bi5
- Client secret: ***
- Provider URL: (empty field)

Below the form are two buttons: "Save" and "Save & Exit". A dropdown menu is open over the "Save & Exit" button, showing options: Applications, Providers (which is selected and highlighted in grey), Resources, and Certs.

Step 3. Add the AirWallex Payment provider for your product

Finally, add the AirWallex Payment provider for your product so that users can purchase the product using AirWallex.

Currency [?](#):

Is recharge [?](#):

Price [?](#):

Quantity [?](#):

Sold [?](#):

Payment providers [?](#): [X](#)

Return URL [?](#):

State [?](#):

Preview [?](#): [Test buy page...](#)

Buy Product

Name	New Product - drxsq				
Detail	Tag	Casdoor Summit 2022	SKU	product_drxsq	
Image					
Price	\$80.59 (USD)	Quantity	99	Sold	10
Pay					

验证码

概述

添加验证码到您的应用程序

默认

在您的应用程序中使用Casdoor的默认验证码

Cloudflare Turnstile

将Cloudflare Turnstile添加到您的应用程序

reCAPTCHA

添加reCAPTCHA 到您的应用程序

 **hCaptcha**

将 hCaptcha 添加到您的应用程序

 **阿里云 Captcha**

将阿里云 Captcha 添加到您的应用程序

 **Geetest**

将Geetest验证码添加到您的应用程序

概述

Casdoor可以配置为支持不同的验证码，以验证操作是否由人类执行。通过添加验证码提供商并在应用程序中应用它，当用户登录、注册或忘记密码并需要发送代码时，将出现一个验证码检查对话框，以验证操作是否由人类执行。

目前，Casdoor支持多个验证码提供商。以下是Casdoor支持的提供商：

默认	Cloudflare 旋转门	reCAPTCHA	hCaptcha	阿里巴巴云验证码	Geetest
					
					

我们将向您展示如何应用验证码并将其添加到Casdoor。

添加验证码提供商

1. 导航至您的Casdoor首页。
2. 点击顶部栏中的 Providers。
3. 点击 Add，然后你会在顶部列表中看到一个新的提供商。
4. 点击新的提供商以修改它。
5. 在 Category 中选择 Captcha。
6. 在 Type 中选择你需要的验证码提供商。

7. 填写最重要的信息。不同的验证码提供商可能需要填写不同的信息。

在应用程序中应用

1. 点击顶部栏中的 Application，然后选择一个应用进行编辑。
2. 点击提供商添加按钮，并选择你刚刚添加的提供商。
3. 完成！

默认

默认的验证码实现会生成并验证一个图像。在默认的验证码图片中，使用了一串长度为5的0-9数字序列。

在Casdoor中进行配置

要在Casdoor中配置默认的验证码，请按照以下步骤操作：

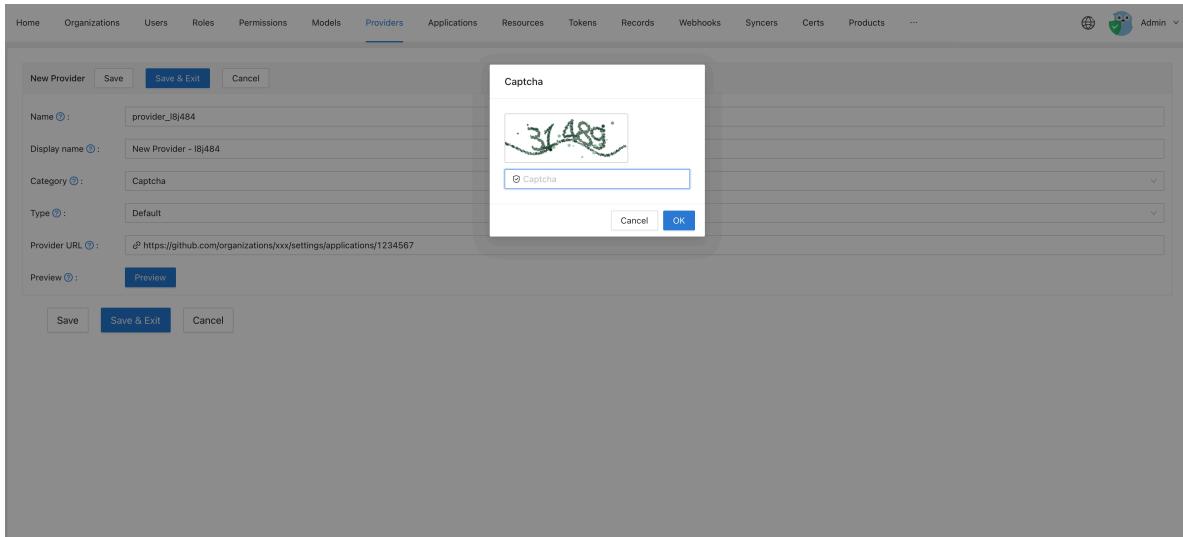
1. 在 Casdoor 中创建一个新的提供商。
2. 选择类别为**Captcha**，类型为**Default**。

The screenshot shows the Casdoor web interface with the 'Providers' tab selected. A modal dialog is open for creating a new provider. The form fields are as follows:

- Name: provider_18484
- Display name: New Provider - 18484
- Category: Captcha
- Type: Default
- Provider URL: https://github.com/organizations/xxx/settings/applications/1234567
- Preview button (highlighted in blue)

At the bottom of the modal are three buttons: Save, Save & Exit (highlighted in blue), and Cancel.

3. 点击预览按钮以预览此验证码的样式。



在您的应用程序中应用

要在您的应用程序中应用默认的验证码，请执行以下操作：

1. 编辑您想要在 Cassdoor 中配置的应用程序。
2. 选择你刚刚添加的提供商。有三种类型的规则可供选择：
 - **Always**：登录时始终需要进行人机验证。
 - **None**：永不需要人机验证。如果账户在15分钟内尝试使用错误的密码登录5次，该账户将被封锁。该阻塞将在15分钟后解除。
 - **Dynamic**：在5次登录尝试失败后，将需要进行人机验证，但账户不会被封锁。

Providers		Add	Name	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Rule	Action
provider_4olfdm			provider_4olfdm	Captcha		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Always	
provider_casdoor_github			provider_casdoor_github	OAuth		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
provider_casdoor_google			provider_casdoor_google	OAuth		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

我们还提供了一个演示视频来展示规则的不同，希望对您有所帮助。

Cloudflare Turnstile

Cloudflare Turnstile是Cloudflare提供的一个CAPTCHA服务，它是对CAPTCHA的一种用户友好、保护隐私的替代方案。您可以在[Turnstile文档](#)中找到更多详细信息。

创建一个API密钥对

要开始使用Cloudflare Turnstile，您需要[创建一个Cloudflare账户](#)，导航到导航栏上的[Turnstile](#)标签，并获取站点密钥和秘密密钥。

首先，为小部件添加一个名称，以便将来识别它，并输入您的网站的主机名。然后选择小部件类型。建议选择[Managed](#)。最后，点击[创建](#)。

The screenshot shows the Cloudflare dashboard with the sidebar collapsed. The main area is titled 'Add Site' under the 'Turnstile' section. It includes fields for 'Site name' (set to 'Casdoor') and 'Domain' (set to 'door.casdoor.org'). The 'Widget Type' section has three options: 'Managed' (selected), 'Non-interactive', and 'Invisible'. At the bottom right are 'Cancel' and 'Create' buttons.

然后，您将能够获得一个站点密钥和一个秘密密钥。

The screenshot shows the Cloudflare dashboard with the sidebar expanded. The 'Turnstile' option under the 'Security Center' section is selected and highlighted with a blue background. The main content area is titled 'Add Site' and contains fields for 'Site Key' and 'Secret Key'. The 'Site Key' field contains the value '0x4AAA/' and includes a 'Copy' button. Below it is a code block for 'Client side integration code':

```
<script src="https://challenges.cloudflare.com/turnstile/v0/api.js" async defer></script>
```

The 'Secret Key' field contains the value '0xAAAAAAAB' and also includes a 'Copy' button. Below it is a code block for 'Server side integration code':

```
Click to copy
```

At the bottom right of the main form is a 'Done' button.

在Casdoor中配置

在Casdoor中创建一个新的提供者。

将类别选择为Captcha，类型选择为Cloudflare Turnstile。填写您在上一步中获得的站点密钥和秘密密钥。

Casdoor Home Organizations Users Roles Permissions Models Adapters Applications Providers Resources ... Admin

Edit Provider Save Save & Exit

Name : Cloudflare Turnstile

Display name : Cloudflare Turnstile

Organization : admin (share)

Category : Captcha

Type : Cloudflare Turnstile

Site key : 0x4AAAAAAABXhq3vOlgpUTmk

Secret key : ***

Provider URL :

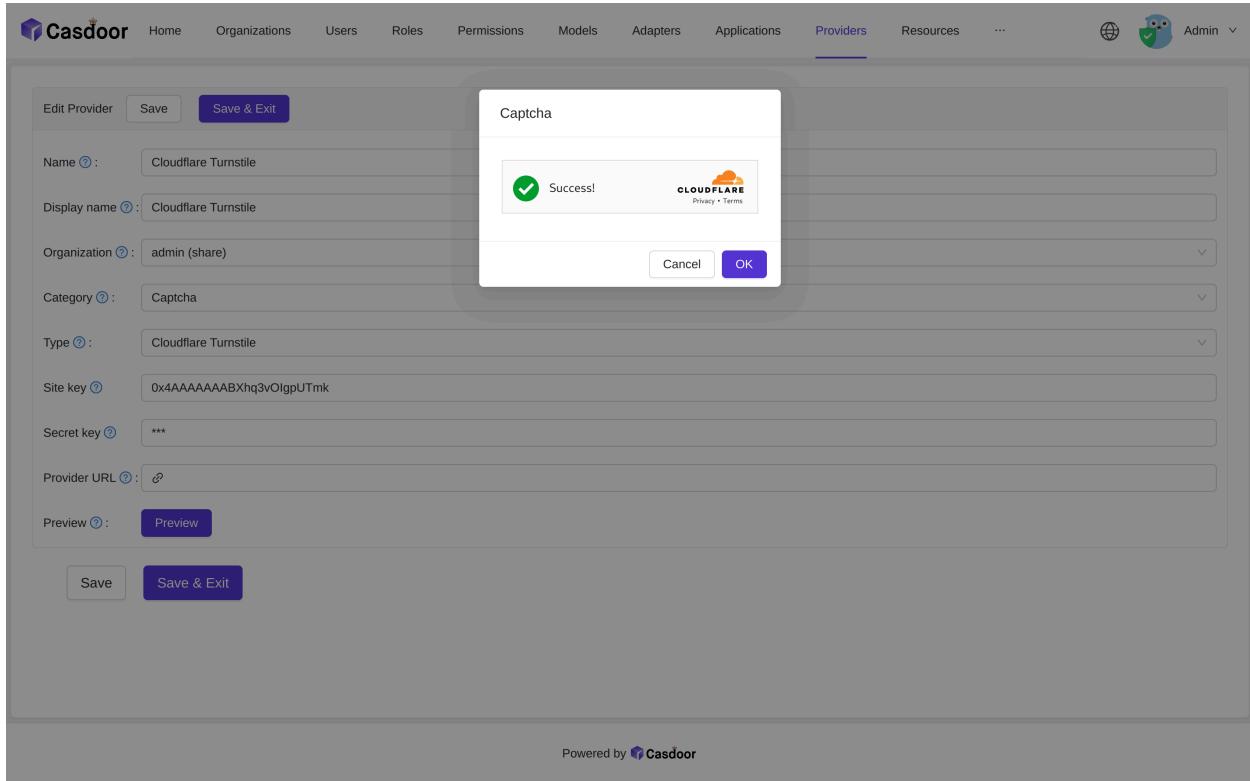
Preview : Preview

Save Save & Exit

The screenshot shows the 'Providers' section of the Casdoor web interface. A new provider is being configured for 'Cloudflare Turnstile'. The form fields include: Name (Cloudflare Turnstile), Display name (Cloudflare Turnstile), Organization (admin (share)), Category (Captcha), Type (Cloudflare Turnstile), Site key (0x4AAAAAAABXhq3vOlgpUTmk), Secret key (***), and Provider URL (empty). There are two buttons at the bottom: 'Save' and 'Save & Exit'.

Powered by Casdoor

您可以点击预览按钮，查看此CAPTCHA的样式预览。



应用集成

编辑您想在Casdoor中配置的应用程序。选择您刚刚添加的提供者，然后点击**保存**按钮。

Providers								
Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action
Cloudflare Turnstile	Captcha							

reCAPTCHA

reCAPTCHA由Google提供，我们使用的是reCAPTCHA v2复选框。 您可以在此[链接](#)中找到更多相关详情。

创建一个 API 密钥对

要开始使用 reCAPTCHA，您需要[注册您的站点的 API 密钥对](#)。 配对的密钥由一个站点密钥组成。 站点密钥用于在您的网站或移动应用上调用reCAPTCHA服务。 密钥授权您的应用程序后端和 reCAPTCHA 服务器之间的通信来[验证用户的回应](#)。

首先，选择[reCAPTCHA的类型](#)，然后填写授权域名或[包名](#)。 在您接受服务条款后，[点击注册](#)以获取新的API密钥对。

The screenshot shows the 'Register a new site' page for Google reCAPTCHA. At the top, there's a blue header bar with the text 'Google reCAPTCHA'. Below it is a light gray navigation bar with a back arrow and the text 'Register a new site'. A yellow banner below the navigation bar says 'Get unlimited assessments using reCAPTCHA Enterprise'. The main form area has a white background. It starts with a 'Label' field containing 'reCaptcha'. Under 'reCAPTCHA type', 'reCAPTCHA v2' is selected, which is described as 'Verify requests with a challenge'. There are three options under this: 'I'm not a robot' Checkbox (selected), Invisible reCAPTCHA badge, and reCAPTCHA Android. Below this is a 'Domains' section with '+ casdoor.org' listed. In the 'Owners' section, 'resultlee@gmail.com (You)' is listed, followed by a placeholder 'Enter email addresses'. At the bottom, there's a checked checkbox for 'Accept the reCAPTCHA Terms of Service'. A small note at the very bottom states: 'By accessing or using the reCAPTCHA APIs, you agree to the Google APIs [Terms of Use](#), Google [Terms of Use](#), and to the Additional Terms below. Please read and understand all applicable terms and policies before accessing the APIs.'

然后，您将收到一个站点密钥和一个秘密密钥。

The screenshot shows the Google reCAPTCHA configuration interface. At the top, it says 'Google reCAPTCHA' and 'Adding reCAPTCHA to your site'. Below that, a message says "'reCaptcha' has been registered.''. It provides 'Site key' and 'Secret key' for integration. Buttons at the bottom include 'GO TO SETTINGS' and 'GO TO ANALYTICS'.

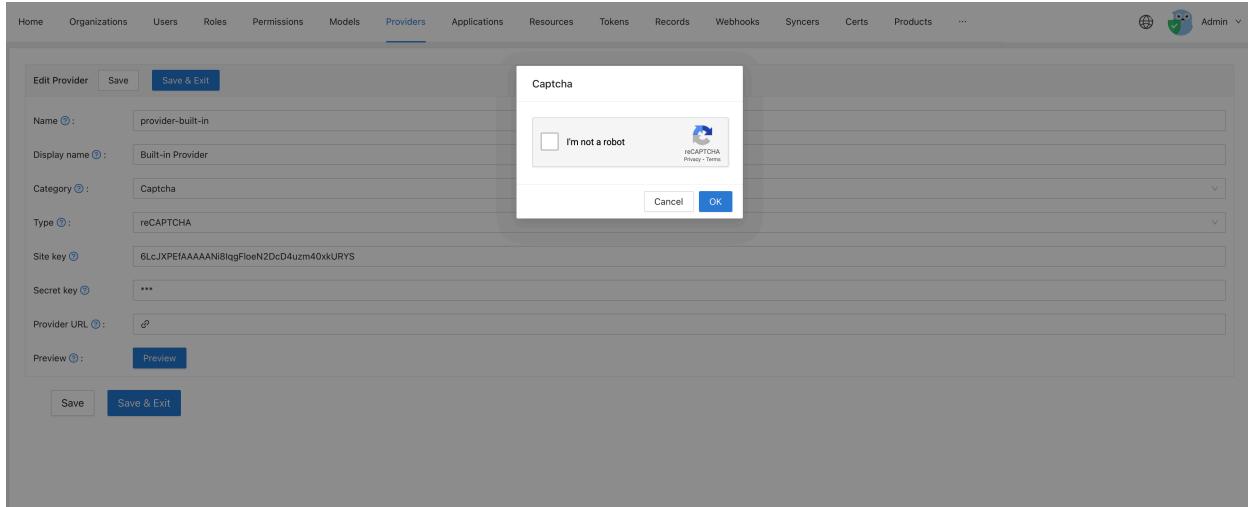
在 Casdoor 配置

在 Casdoor 中创建一个新的提供商。

选择类别为**Captcha**, 类型为**reCAPTCHA**。您需要提供在上一步中创建的网站密钥和秘密密钥。

The screenshot shows the Casdoor provider configuration interface under the 'Providers' tab. A new provider named 'reCaptcha' is being created. The 'Type' is set to 'reCAPTCHA'. The 'Site key' and 'Secret key' fields are populated with values from the previous screenshot. The 'Provider URL' field contains a placeholder URL. A 'Preview' button is available to see the reCAPTCHA style. Buttons at the bottom include 'Save', 'Save & Exit', and 'Cancel'.

您可以点击预览按钮来查看这个验证码的样式。



在应用程序中应用

编辑您想要在 Cassdoor 中配置的应用程序。选择你刚刚添加的提供商，然后点击保存按钮。

Providers	Add	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
reCaptcha	Captcha							

hCaptcha

hCaptcha是一个验证码服务提供商，类似于reCAPTCHA。 您可以在此处找到有关hCaptcha的更多详细信息[这里](#)。

创建一个 API 密钥对

要开始使用hCaptcha，您需要为您的网站注册一个API密钥对。 您可以在您的[个人资料页面](#)上获取您的站点密钥。

一旦您已经注册，您将会收到一个站点密钥和一个秘密密钥。

在 Casdoor 配置

要在Casdoor中配置hCaptcha，请创建一个新的提供商。

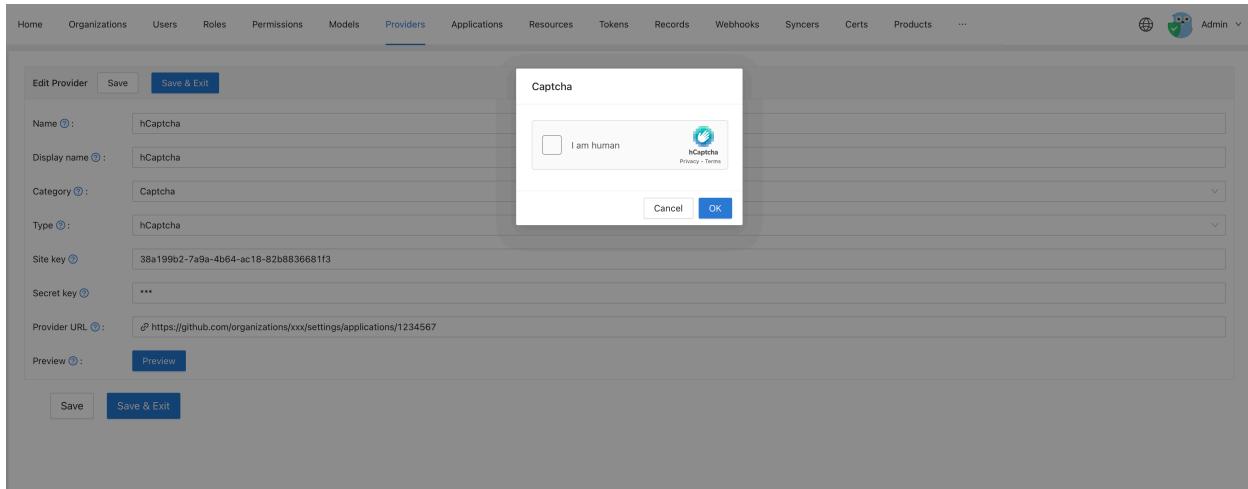
选择类别为Captcha，类型为hCaptcha。 填写在上一步中获得的站点密钥和秘密密钥。

The screenshot shows the Casdoor web interface with the 'Providers' tab selected. A new provider named 'hCaptcha' is being configured. The form fields are as follows:

- Name: hCaptcha
- Display name: hCaptcha
- Category: Captcha
- Type: hCaptcha
- Site key: 38a199b2-7a9a-4b64-ac18-82b8836681f3
- Secret key: 38a199b2-7a9a-4b64-ac18-82b8836681f3
- Provider URL: <https://github.com/organizations/xxx/settings/applications/1234567>
- Preview: Preview button

At the bottom of the form are three buttons: Save, Save & Exit, and Cancel.

您可以点击预览按钮，查看验证码样式的效果。



在您的应用程序中应用

转到您想在Casdoor中配置的应用程序。选择你刚刚添加的提供商，然后点击**保存**按钮。

Providers	Add	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
hCaptcha	✓	Captcha						

阿里云 Captcha

阿里云 Captcha 是由 阿里云 提供的验证码服务。 它提供两种验证方式："滑动验证" 和 "智能验证"。 您可以从此 [链接](#) 中查询更多详细信息。

在阿里云中添加验证码配置

要添加验证码配置，请登录[阿里云管理控制台](#)，搜索并进入验证码服务。 然后，点击确认开启以启用验证码服务。



一旦您进入了验证码管理控制台，点击[添加配置](#)。

The screenshot shows the Alibaba Cloud Scene Management interface. On the left, there is a sidebar with the following navigation links:

- 验证码2.0
- 概览
- 场景管理** (highlighted with a blue background)
- 安全管理
- 自定义策略
- 白名单策略 (NEW)
- 账单管理
- 版本管理
- 告警通知
- 其他
- 实人认证

The main content area displays a table titled "场景管理" (Scene Management) with the following columns:

场景名称/ID	接入方式	验证码形态	策略状态	策略类型	数据统计	操作
test 1kyi	Web/H5	一点即过	● 正式	默认		接入引导 编辑 自定义策略 删除

Below the table, there are pagination controls: "每页显示 10" (10 items per page), "共 1 条数据" (1 total data), and navigation buttons: "< 上一页" (Previous page), "1" (current page), "下一页 >" (Next page).

On the right side of the main content area, there is a vertical column of circular icons with the following labels:

- 编辑 (Edit)
- 购买 (Purchase)
- AP (Application Programming Interface)
- 设置 (Settings)
- 刷新 (Refresh)
- 日历 (Calendar)
- 帮助 (Help)

填写所有必需的信息并提交表格。

为提供更好的安全能力，验证码产品计划2025年8月28日下线空间推理验证形态，下线后存量空间推理配置将自动

验证码2.0

场景管理

安全管理

自定义策略

白名单策略 **NEW**

账单管理

版本管理

告警通知

其他

实人认证

验证码2.0 / 场景管理

场景管理

新建场景 验证码形态 接入方式

场景名称/ID	接入方式	验证码形态
test	Web/H5	一点即过

新建场景

* 场景名称
请输入场景名称

* 接入方式 ②

Web/H5
 Webview+H5 (支持APP/微信小程序接入)
 微信小程序原生插件

* 验证码形态

无痕验证 ②
 一点即过 **new**
 滑块验证
 拼图验证
 图像复原 **new**

* 无痕验证二次挑战形态

一点即过 **new**
 滑块验证
 拼图验证
 图像复原 **new**

请按住滑块，拖动到最右边

验证通过! **✓**

* 策略状态 ②
(从测试切到正式状态预计5分钟左右生效)

正式 测试

确定 取消

现在，您可以在控制台中查看 **Scene** 和 **App key**。

验证码2.0 / 场景管理

场景管理

场景名称/ID	接入方式	验证码形态	策略状态	策略类型	数据统计	操作
test 1key	Web/H5	一点即过	● 正式	默认		接入引导 编辑 自定义策略 删除

每页显示 10 共 1 条数据 < 上一页 1 下一页 >

帮助文档

scene

验证码2.0 / 概览

概览

今日汇总指标 (全量)

初始化量	验证量	验证拦截量	验证通过量
0	0	0	0

时间周期: 00:00 - 18:00

累计开通时间: 96 天

身份标: gc

[开通包年包月](#) | [购买资源包](#)

AppKey

查看详情

验证趋势

查看详情

验证趋势

另外, `Access key` 和 `Secret access key` 可以在您的个人资料中找到。

在 Casdoor 配置

在 Casdoor 中创建一个新的提供商。

选择类别为**Captcha**, 类型为**hCaptcha**。然后, 选择子类型: “滑动验证”或“智能验证”。确保填写在上一步中创建的 `Access key`、`Secret access key`、`Scene` 和 `App key`。

New Provider Save Save & Exit Cancel

Name : Aliyun_Captcha

Display name : Aliyun_Captcha

Category : Captcha

Type : Aliyun Captcha

Sub type : Sliding Validation

Access key :

Secret access key :

Scene : nc_other

App key :

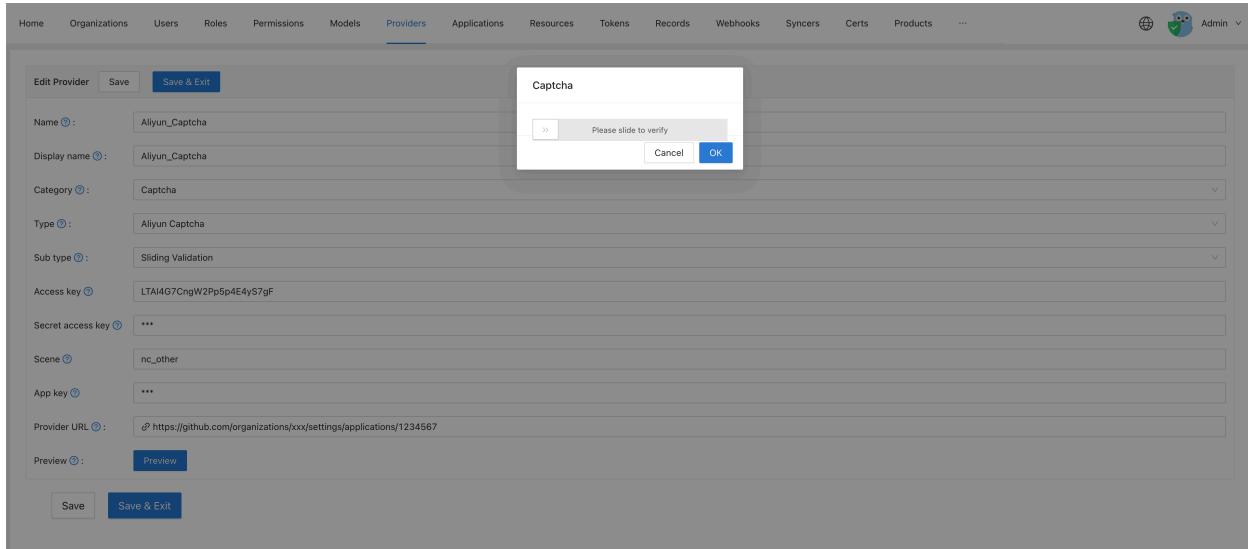
Provider URL : <https://github.com/organizations/xxx/settings/applications/1234567>

Preview : Preview

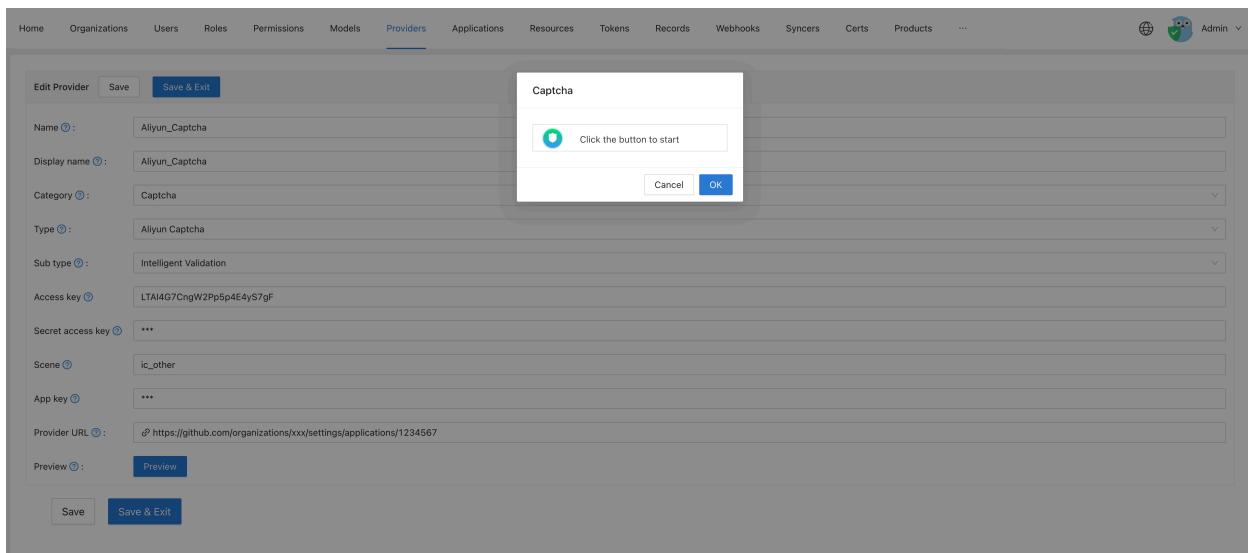
Save Save & Exit Cancel

您可以点击**预览**按钮来查看这个验证码的样式。

以下图片显示了“滑动验证”的预览:



而这张图片展示了“智能验证”的预览：



应用集成

编辑您想要配置Casdoor的应用程序。选择新添加的提供商，然后点击**保存**按钮。

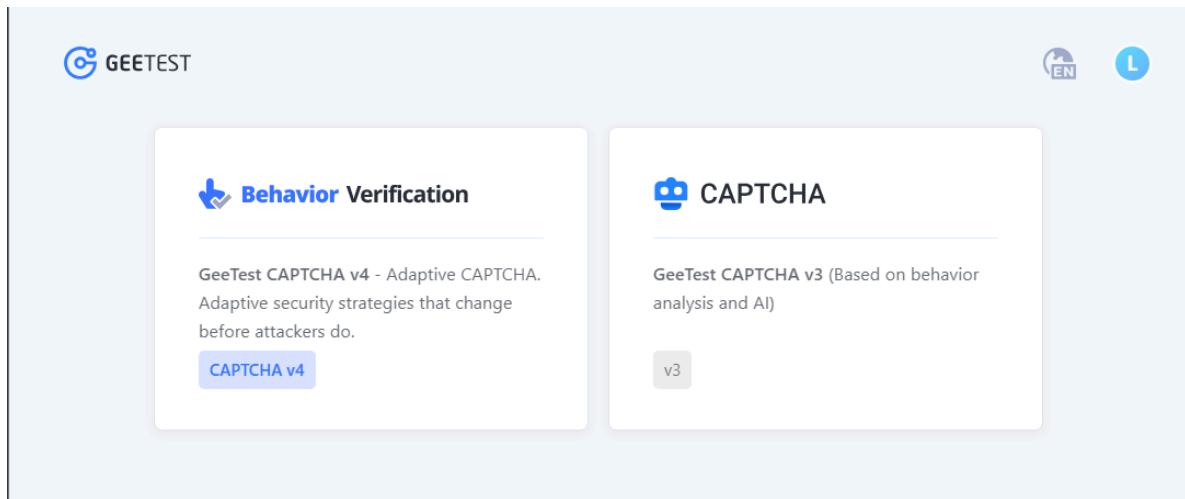
Providers	Add	Category	Type	canSignUp	canSignIn	canUnlink	prompted	Action
Aliyun_Captcha	Captcha							

Geetest

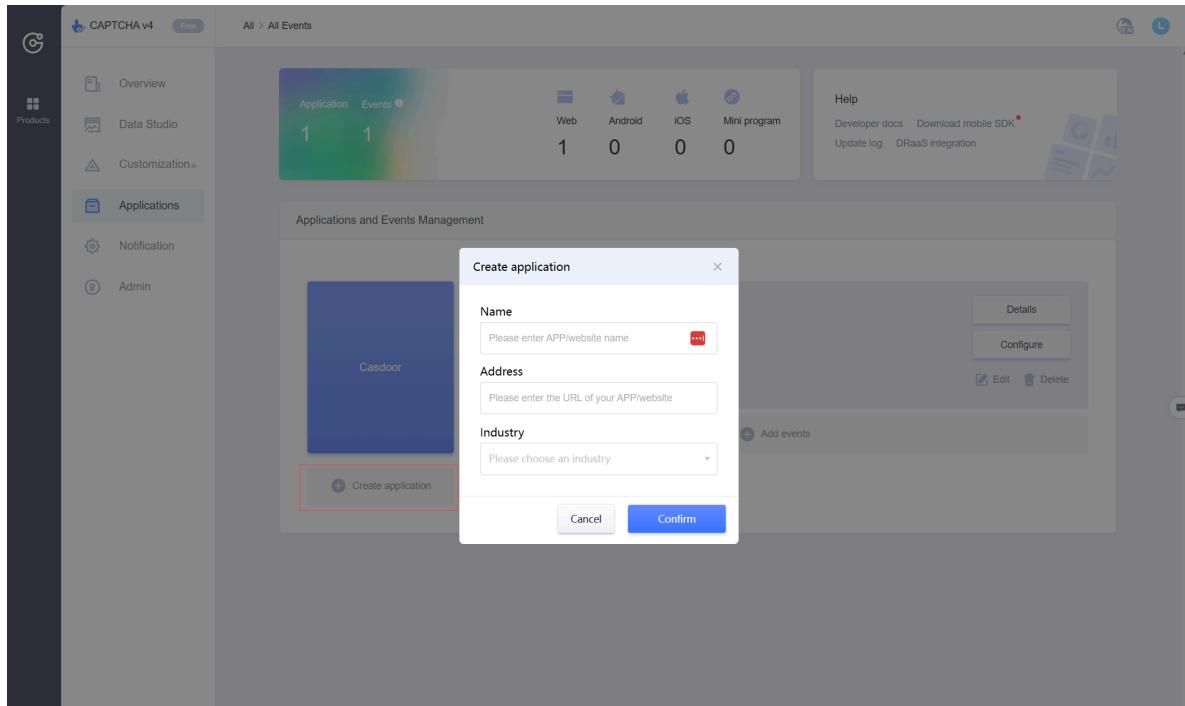
配置Geetest

按照以下步骤配置Geetest并获取公钥和密钥：

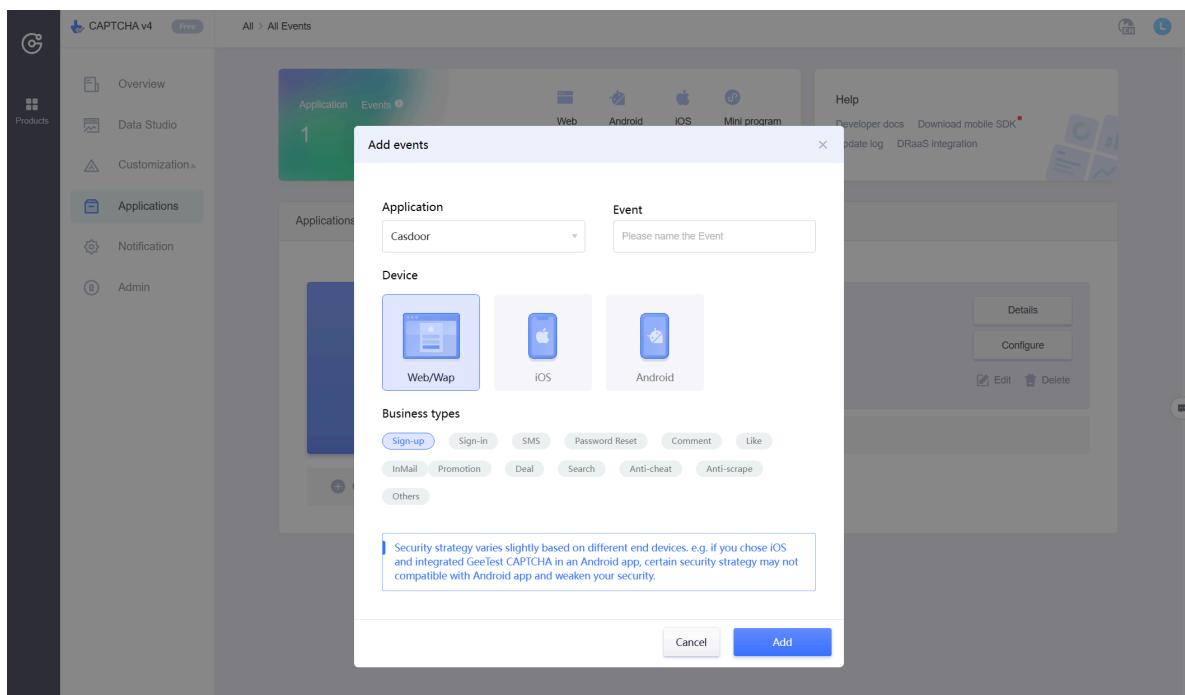
1. 转到Geetest产品页面上的Geetest CAPTCHA V4部分。



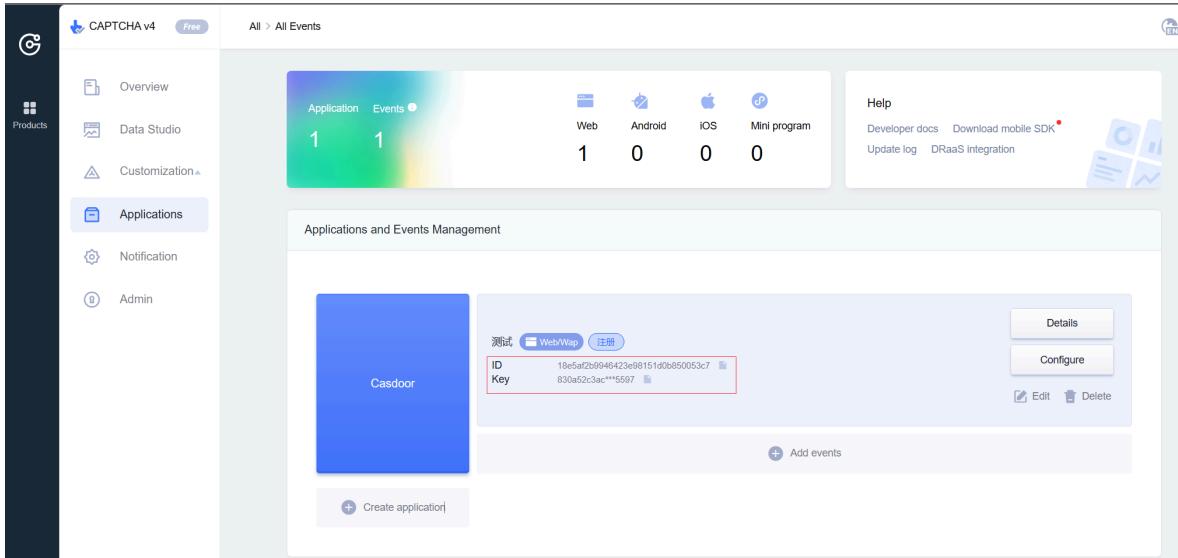
2. 通过输入您的应用程序的名称和地址来创建一个应用程序。



3. 添加事件并为设备选择"web"。



4. 检索 ID 和 Key。



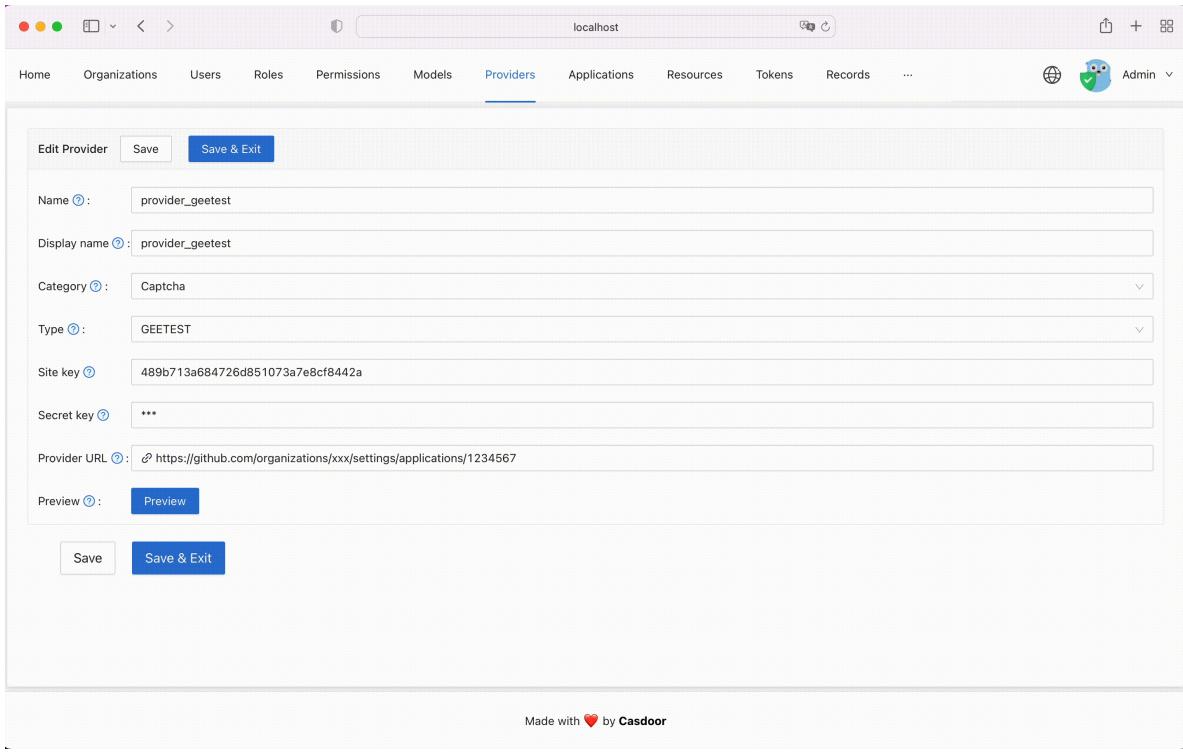
配置Casdoor

按照以下步骤配置Casdoor：

1. 在Casdoor中创建一个新的提供商。

将类别设置为**Captcha**, 类型设置为**Geetest**。用从Geetest获取的**ID**和**Key**填写**Site key**和**Secret key**。

2. 点击预览按钮以预览此验证码的样式。



在您的应用程序中应用

在您的应用程序中应用Geetest配置：

编辑您希望在Casdoor中配置的应用程序。选择您刚刚添加的提供商，然后点击保存按钮。

Providers	Add	Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action
geetest			Captcha							▼ ^ < > ✖



> 提供商 >

Web3

Web3



MetaMask

将MetaMask Web3提供者添加到您的应用程序



Web3-Onboard

将Web3-Onboard Web3提供者添加到你的应用程序

MetaMask

① 备注

这是一个如何配置MetaMask作为Web3提供者的示例。

MetaMask是一个浏览器扩展和应用程序，既可以作为加密货币钱包，也可以作为区块链应用的入口。Casdoor允许您使用MetaMask作为身份提供者，并启用MetaMask的Web3登录。

步骤1：创建一个MetaMask Web3提供者

首先，您需要在Casdoor中创建一个MetaMask Web3提供者。

名称	描述
Category	选择 Web3
Type	选择 MetaMask

Name ? :	metamask_provider
Display name ? :	MetaMask Provider
Organization ? :	admin (Shared)
Category ? :	Web3
Type ? :	MetaMask
Provider URL ? :	🔗

步骤2：将提供者添加到您的应用程序

接下来，将MetaMask Web3提供者添加到您的应用程序。

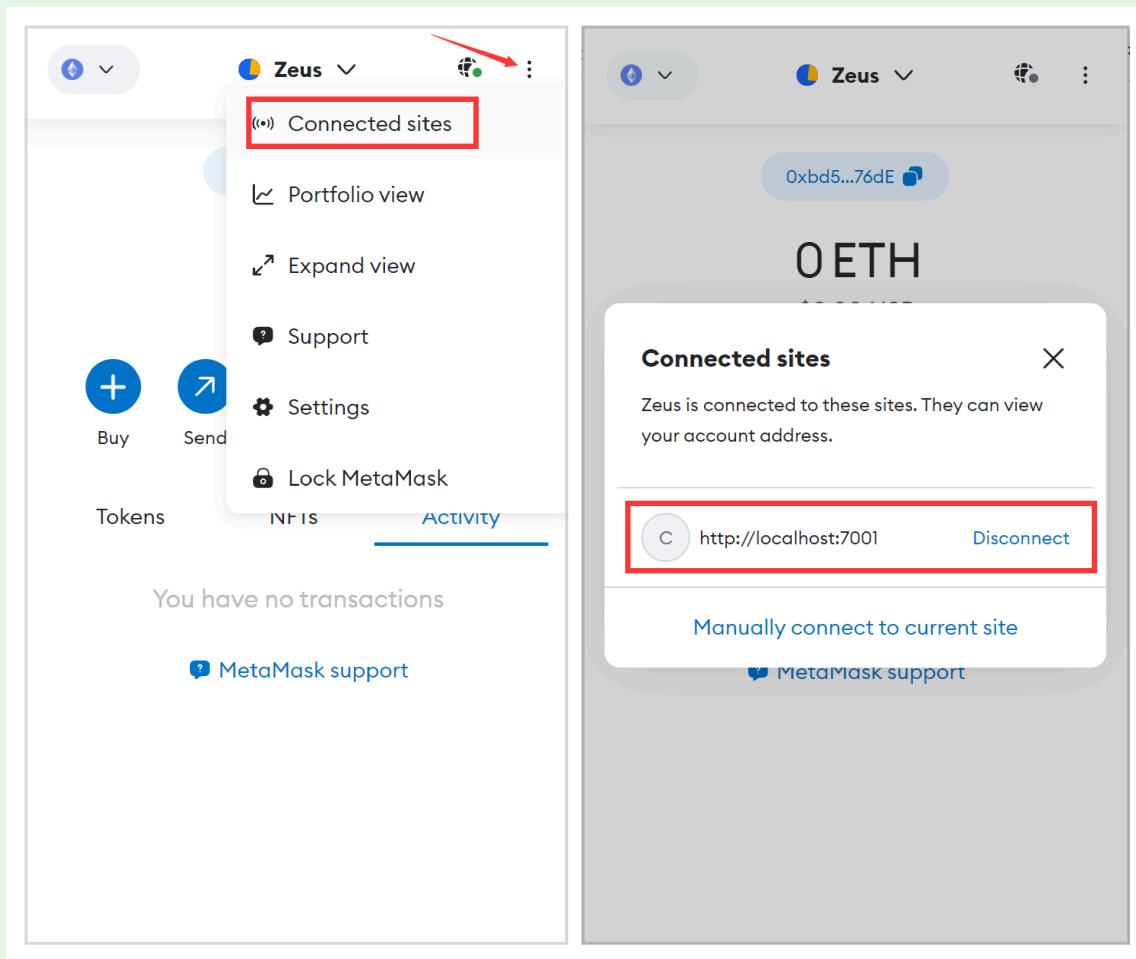
The screenshot shows a list of providers in a management interface. The provider 'metamask_provider' is highlighted with a red box. The interface includes buttons for 'Copy SAML metadata URL' and 'Copy sign-in page URL'. A preview section at the bottom shows a blurred view of a web application.

步骤3：使用MetaMask登录

您现在可以使用MetaMask登录了。这里有一个演示视频。

提示

1. 使用MetaMask登录时，请只授权一个以太坊地址。Casdoor每个用户只绑定一个以太坊地址。
2. 如果您想切换到另一个以太坊地址进行登录，请先断开当前以太坊地址与Casdoor的连接。

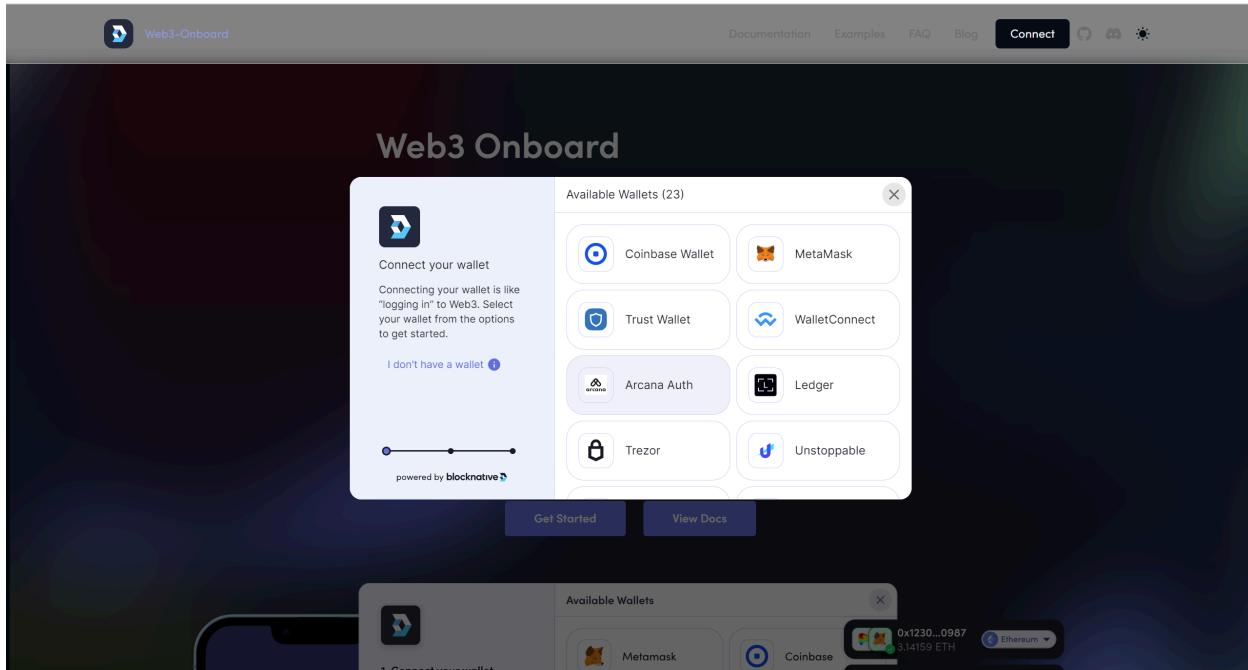


Web3-Onboard

ⓘ 备注

这是一个如何配置Web3-Onboard作为Web3提供者的示例。

Web3-Onboard可以帮助用户使用不同的钱包进行Web3登录。 Casdoor允许使用Web3-Onboard作为身份提供者，并启用Web3-Onboard的Web3登录。



步骤1：创建一个Web3-Onboard Web3提供者

首先，你需要在Casdoor中创建一个Web3-Onboard Web3提供者。

名称	描述
类别	选择 Web3
类型	选择 Web3-Onboard
钱包	选择允许登录的钱包

Edit Provider
Save
Save & Exit

Name ⓘ : provider_web3_onboard

Display name ⓘ : Web3-Onboard Web3 Provider

Organization ⓘ : admin (Shared)

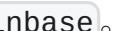
Category ⓘ : Web3

Type ⓘ :  Web3-Onboard

Wallets ⓘ : Injected Coinbase Trust Gnosis Sequence Taho Frontier Infinity Wallet

Provider URL ⓘ :  <https://github.com/organizations/xxx/settings/applications/1234567>

Save
Save & Exit

目前，Casdoor只支持上图中显示的钱包。 Injected 钱包代表浏览器注入的钱包，如 MetaMask 或 Coinbase。

步骤2：将提供者添加到你的应用程序

其次，将Web3-Onboard Web3提供者添加到你的应用程序。

Providers (0) :

Add

Name	Category	Type	Can signup	Can signin	Can unlink	Prompted	Rule	Action
provider_storage_minio_s3	Storage	MINIO						
provider_oauth_lark	OAuth	LARK	On	On	On	Off		
provider_email_qq	Email	QQ	On	On	On	Off		
provider_web3_metamask	Web3	METAMASK	On	On	On	Off		
provider_google_oauth	OAuth	GOOGLE	On	On	On	Off	One Tap	
provider_web3_onboard	Web3	ONBOARD	On	On	On	Off		

步骤3：通过Web3-Onboard登录

现在你可以通过Web3-Onboard登录。 这里有一个演示视频。

Face ID

Overview

Using Face ID for authentication

Alibaba Cloud FaceBody

Add libaba Cloud FaceBody as a third-party faceid service to complete authentication

Overview

Casdoor allows for the use of Face ID as a sign-in method.

We only recommend enabling Face ID if you can ensure that the hardware and requests cannot be tampered with.

Adding an Face ID provider

1. Go to your Casdoor index page.
2. Click on `Providers` in the top bar.
3. Click on `Add`, and you will see a new provider added to the list at the top.
4. Click on the new provider to make changes to it.
5. In the `Category` section, select `Face ID`.
6. Choose the specific Face ID provider that you require from the `Type` dropdown.
7. Fill in the necessary information, such as `Client ID` and `Client Secret`.

Alibaba Cloud FaceBody

Introduction

Based on face detection, analysis/comparison technology in images or videos, and human body detection technology, it provides independent modules for face/human body detection and localization, face attribute recognition and face comparison. It can provide developers and enterprises with high-performance online API services for various scenarios such as face AR, biometric identification and authentication, large-scale face retrieval, and photo management.

How to use?

The steps to use alibaba cloud facebody are shown below.

Step 1: Register alibaba cloud facebody

First, visit [Alibaba Cloud Facebody website](#) and open a facebody account.

The screenshot shows the Alibaba Cloud Visual Intelligence Open Platform homepage. At the top, there is a navigation bar with links for '能力广场 New' (Ability Square), '场景广场' (Scenario Square), '文档中心' (Document Center), '开发者社区' (Developer Community), and '控制台' (Control Panel). The main heading '人脸人体' (Face and Body) is displayed prominently. Below it, a brief description explains the service's purpose: '基于图像或视频中的人脸检测、分析/比对技术，以及人体检测技术，提供人脸/人体的检测定位、人脸属性识别和人脸比对等独立模块。可以为开发者和企业提供高性能的在线API服务，应用于人脸AR、生物识别和认证、大规模人脸检索、照片管理等各种场景。' A large image of two women's faces with bounding boxes and crop marks is shown. A blue button labeled '立即开通' (Activate Now) is visible. In the middle section, there is a summary 'AI能力体验' (AI Experience) with the text '技术能力150+，开发者接近1000万' (150+ technical capabilities, nearly 10 million developers) and a link '查看全部能力' (View All Abilities). The bottom section features a grid of service cards under the heading '人脸编辑' (Facial Editing). The cards include: '智能美肤' (Smart Skin Care), '智能瘦脸' (Smart Face Slimming), '图像人脸融合' (Image Facial Fusion), '人像素描风格化' (Portrait Sketch Style); '人物动漫化' (Character Animation), '人脸修复增强' (Facial Repair Enhancement), '人脸美颜' (Facial Beauty), '人脸美型' (Facial Modeling); '人脸信息脱敏' (Facial Information Desensitization); and '金融级人脸检测' (Financial-grade Facial Detection). A small icon of a gift box is located at the bottom right of the card grid.

Step 2: Buy CompareFace resource pack

Visit [Face body page](#) and buy CompareFace resource pack

Step 3: Create a client secret

Go to console and create AccessKey and AccessSecret

已开通能力
1 个
能力总使用量
最近一天 2023-03-21 - 2023-03-21 搜索

热门API
口算人比对1:1 体验测试
人脸属性识别 体验测试
红外人脸识别检测 体验测试
人像比对1:1 体验测试
更多能力体验 >

最新动态
○ 视频生产能力上新——视频人像卡通化 2023-03-13 能力上新
○ 视频理解能力上新——视频画面评估 2023-03-13 能力上新
○ 人脸识别产品上新——人脸识别1:1 2023-02-07 产品上新

AccessKey ID	状态	最后使用	已创建时间	操作
LTAI5H7yjst7LqfjhNjghz2Y	已启用	VisualInt... 2025年3月	6 天	编辑 AccessKey 禁用 查看操作记录

我确认认知云账号 AccessKey 安全风险
继续使用云账号 AccessKey | 使用 RAM 用户 AccessKey

Step 4: Find Endpoint

You can find your endpoint ID in [Aliyun doc](#)

for example, if your region id is cn-shanghai, then the endpoint is facebody.cn-shanghai.aliyuncs.com

Step 5: Create Alibaba Cloud Facebody provider in Casdoor

The last step is to add an Alibaba Cloud Facebody Face ID provider and fill in the `Client ID`, `Client Secret` and `Endpoint` in your Casdoor.



> 提供商

> MFA

MFA



Push Notification

Configure push notification provider for MFA



RADIUS

Configure RADIUS provider for MFA

Push Notification

Push notification MFA enables users to receive verification codes through mobile push services during authentication. This method leverages Casdoor's existing notification provider infrastructure, supporting services like Duo, Pushover, Telegram, and 20+ other providers.

Configure Notification Provider

Push notification MFA uses notification providers to send verification codes. To add a notification provider:

1. Navigate to the **Providers** page and click **Add**.
2. Set the **Category** to **Notification** and choose your preferred **Type** (e.g., Telegram, Pushover, Custom HTTP).
3. Configure the provider-specific settings based on your chosen notification service.
4. Click **Save** to create the provider.

Use in Application

After creating the notification provider, add it to your application:

1. Go to your application's edit page.

2. Add the notification provider to the Providers list.
3. Users can now select push notification as their MFA method when configuring multi-factor authentication.

User Setup Flow

During MFA setup, users will:

1. Select "Use Push Notification" as their MFA method.
2. Enter their push notification receiver (device token or user ID).
3. Select the notification provider from the configured options.
4. Receive a verification code via push notification.
5. Enter the verification code to complete setup and receive recovery codes.

Authentication Flow

When push notification MFA is enabled, users will receive a verification code via push notification during login. They must enter this code to complete authentication.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) providers allow Casdoor to authenticate users against external RADIUS servers during multi-factor authentication.

Configure RADIUS Provider

To add a RADIUS provider for MFA:

1. Navigate to the Providers page and click Add.
2. Set the Category to MFA and Type to RADIUS.
3. Configure the following fields:
 - Host: The IP address or hostname of your RADIUS server (e.g.,
`10.10.10.10`)
 - Port: The RADIUS server port (default is `1812`)
 - Client Secret: The shared secret configured on your RADIUS server for authenticating requests
4. Click Save to create the provider.

Use in Application

After creating the RADIUS provider, add it to your application:

1. Go to your application's edit page.
2. Add the RADIUS provider to the **Providers** list.
3. Users can now select RADIUS as their MFA method when configuring multi-factor authentication.

During MFA setup and authentication, users will be prompted to enter their RADIUS username and password, which will be verified against the configured RADIUS server.



>

资源

资源

概述

上传资源到Casdoor

概述

您可以在Casdoor中上传资源。在上传资源之前，您需要配置存储提供商。请参阅[存储提供商](#)部分以获取更多信息。

一旦您配置了至少一个存储提供商并将其添加到您的应用程序中，您就可以继续进行了。

Providers [?](#) :

Name	Category	Type
Provider_azure	Storage	A
Github_1	OAuth	G
provider_Alipay	Payment	支

太棒了！现在让我们来看一个如何上传和删除资源的例子。

上传资源

用户可以上传各种类型的资源，如文件和图片，到您配置的[云存储](#)中。

Home Organizations Users Roles Permissions Providers Applications Resources Tc

Resources [Upload a file...](#)

Provider	Created time	Tag
provider_storage_aliyun_oss	2022-05-18 17:25:21	custom
provider_storage_aliyun_oss	2022-05-18 12:28:01	custom
provider_storage_aliyun_oss	2022-05-17 16:25:39	custom

删除资源

如果您不再需要某个特定资源，您可以选择点击“删除”按钮来删除它。

Created time	Tag	Type	Format	File size	Preview	URL	Action
2022-05-19 23:16:55	custom	image	.jpg	70.3 KB		<button>Copy Link</button>	<button>Delete</button>



> SaaS Management

SaaS Management



概述

Casdoor定价概述



Product

添加您想要销售的产品



支付

查看支付中产品的交易信息



计划

Casdoor计划概述

 Pricing

Casdoor定价概览

 订阅

Casdoor订阅概览

 Transaction

Casdoor Transaction Overview

概述

Casdoor can be used as a subscription management system through its [Product](#), [Payment](#), [Plan](#), [Pricing](#), [Subscription](#), and [Transaction](#) features.

您可以选择将哪些计划包含在您的价格列表中，如下图所示：

Casdoor Pricing

Casdoor hosting services provided by Casbin Inc.

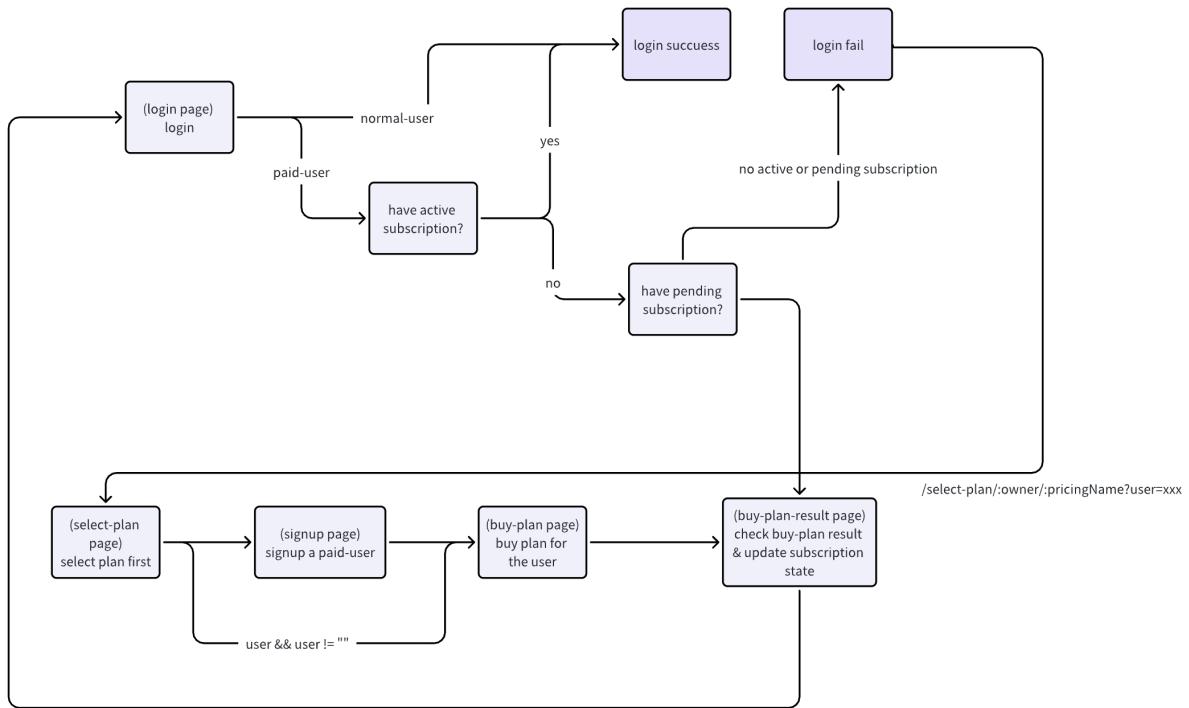
Basic Plan	Premium Plan	Enterprise Plan
\$ 10.01 per month For small teams, with limited technical support	\$ 20.02 per month For fast growing start-ups, with full technical support	\$ 30.03 per month For large & medium-sized enterprise, with full technical support
Getting started	Getting started	Getting started

Free 7-days trial available!

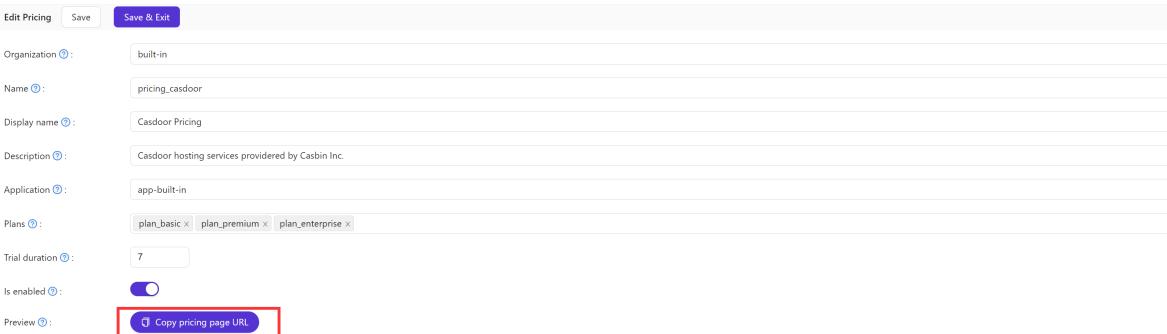
每个 [Pricing](#) 都属于一个特定的 [Application](#)。用户可以选择一个计划，并通过 [Pricing](#) 的相应 [pricing page URL](#) 注册为 [paid-user](#)。

一般流程

一般流程看起来像这样：



1. 用户通过访问管理员共享的 `pricing page URL` 进入 Pricing 的选择计划页面。



Casdoor Pricing

Casdoor hosting services providered by Casbin Inc.

Basic Plan	Premium Plan	Enterprise Plan
\$ 10.01 per month	\$ 20.02 per month	\$ 30.03 per month
For small teams, with limited technical support	For fast growing start-ups, with full technical support	For large & medium-sized enterprise, with full technical support
Getting started	Getting started	Getting started

2. 用户选择一个 `Plan` 进行订阅并完成注册过程，成为一个 `paid-user`。

Casdoor Pricing

Casdoor hosting services providered by Casbin Inc.

Basic Plan	Premium Plan	Enterprise Plan
\$ 10.01 per month	\$ 20.02 per month	\$ 30.03 per month
For small teams, with limitedtechnical support	For fast growing start-ups, withfull technical support	For large & medium-sizedenterprise, with full technicalsupport
Getting started	Getting started	Getting started

Free 7-days trial available!



Username:

Display name:

* Password:

[Sign Up](#) Have account? [sign in now](#)



3. 注册后，用户将被重定向到所选 Plan 的购买计划页面，以继续付款。

Buy Product

Name	Auto Created Product for Plan built-in/plan_premium(Premium Plan)
Detail	This Product was auto created for Plan built-in/plan_premium(Premium Plan)
Image	
Price	\$20.02 (USD)
Pay	 Stripe  PayPal

- 一旦付款成功完成，用户对 Plan 的 Subscription 就被激活。现在，用户可以作为 paid-user 登录到 Casdoor。



You have successfully completed the payment: Auto Created Product for Plan built-in/plan_premium(Premium Plan)

Please click the below button to return to the original website

[Return to Website](#)

这里有一个演示视频：

Product

您可以添加您想要销售的产品(或服务)。以下将指导您如何添加产品的过程。

配置产品属性

首先，你需要理解产品的基本属性：

- 标签
- 详情
- 货币
- 价格
- 数量
- 已售出

Tag ? :	Casdoor Summit 2022
Detail ? :	This is a description
Currency ? :	USD
Price ? :	19
Quantity ? :	100
Sold ? :	10

支付服务提供商

除了设置这些属性外，您还需要为产品添加支付提供商。可以向产品添加多个支付提供商。

要了解如何配置支付提供商，请参考[支付提供商](#)

Payment providers x

(?) :

provider_Alipay

Return URL (?) :

最后，填写**返回URL**。这是付款完成后，付款提供商页面将重定向的URL。

Success URL (Optional)

If you need the provider to redirect users directly to a custom URL instead of the Casdoor callback page, you can fill in the **Success URL** field. When configured, Casdoor will append the payment owner and transaction name as query parameters to your provided URL.

For example, if you set the Success URL to `http://example.com/payment/success`, users will be redirected to:

```
http://example.com/payment/  
success?transactionOwner={paymentOwner}&transactionName={paymentName}
```

You can include additional query parameters in your Success URL, such as:

```
http://example.com/payment/  
success?customParam=value&transactionOwner={paymentOwner}&transactionName={paymentName}
```

⚠ 注意事项

Important: If you configure the Success URL field, you must manually call the `NotifyPayment` API to complete the transaction, otherwise the payment will fail.

Call the API endpoint: `api/notify-payment/{paymentOwner}/{paymentName}` using the parameters provided in the Success URL query string.

预览产品

你已经完成了！ 查看详细信息并保存：

Preview [?](#) :

[Test buy page..](#)

Buy Product

Name	Product				
Detail	This is a subscription.	Tag	Casdoor Summit 2022	SKU	product
Image					
Price	\$300 (USD)	Quantity	99	Sold	10
Pay	 Alipay				

支付

付款成功处理后，您将能够在支付部分查看产品的交易信息。此信息将包括诸如组织、用户、购买时间和产品名称等详细信息。

发票

要开具发票，请导航至编辑屏幕：

Type	Product	Price	Curren	Action
	A notebook computer	300	USD	Result Edit Delete
.

在编辑屏幕上，您需要填写相关的发票信息。有两种可用的发票类型：`individual` 和 `organization`。

要完成此过程，只需点击“发票”按钮。

如果您有任何其他问题或疑虑，请告诉我们。

计划

Plan 描述了一个应用的一系列功能，每个功能都有自己的名称和价格。

Plan 的功能取决于 Casdoor 的 **Role**，它附带一组 **Permissions**。

这允许独立描述 **Plan** 的功能，无论命名和定价如何。

例如，**Plan** 的价格可能会根据国家或日期的不同而有所不同。

下图说明了 **Plan** 和 **Role** 之间的关系。

Plan

- Display Name
 - Price per month
- ...

Role

permission 1
permission 2
...
permission N

计划属性

每个 Plan 都有以下属性：

- 组织
- 名称
- 创建时间
- 显示名称
- 角色
- 每月价格
- 货币
- Payment Providers：用户可以通过支付提供商购买 Plan。有关如何配置支付提供商的信息，请参见[支付提供商](#)。
- 是否启用

The screenshot shows the 'Edit Plan' form interface. At the top, there are three buttons: 'Edit Plan' (disabled), 'Save' (disabled), and 'Save & Exit' (highlighted in purple). The form contains the following fields:

Organization ② :	built-in
Name ② :	plan_enterprise
Display name ② :	Enterprise Plan
Role ② :	(empty)
Description ② :	For large & medium-sized enterprise, with full technical support
Price per month ② :	30.03
Price per year ② :	100
Currency ② :	USD
Payment providers ② :	provider_payment_stripe × provider_payment_paypal ×
Is enabled ② :	<input checked="" type="checkbox"/>

At the bottom, there are two buttons: 'Save' (disabled) and 'Save & Exit' (highlighted in purple).

当通过Casdoor创建 Plan 时，会自动创建一个相关的 Product。

为 Plan 配置的信息将自动同步到 Product。

当用户购买 Plan 时，他们实际上是购买了所选 Plan 的相关 Product。

Form showing product configuration:

Name	product_4f9fak
Display name	Auto Created Product for Plan built-in/plan_enterprise(Enterprise Plan)
Organization	built-in
Image	 URL: https://cdn.casbin.org/img/casdoor-logo_1185x256.png
Preview	
Tag	auto_created_product_for_plan
Detail	This Product was auto created for Plan built-in/plan_enterprise(Enterprise Plan)
Description	
Currency	USD
Price	30.03
Quantity	999
Sold	0
Payment providers	provider_payment_stripe x provider_payment_paypal x
Return URL	dP
State	Published
Preview	Test buy page.

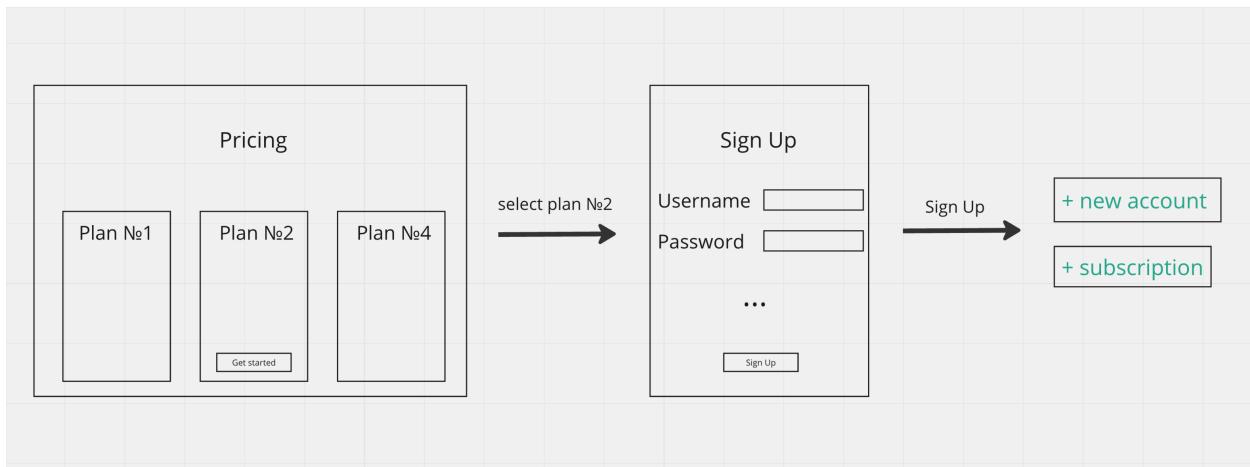
Buy Product page preview:

The page displays the product details: Name: Auto Created Product for Plan built-in/plan_enterprise(Enterprise Plan), Detail: This Product was auto created for Plan built-in/plan_enterprise(Enterprise Plan), Image: Casdoor logo, Price: \$30.03 (USD), Quantity: 999, Sold: 0. Payment providers shown are Stripe and PayPal.

Pricing

定价功能包含一个或多个计划选项，允许用户以不同的价格点注册应用。

下图描述了定价选项的一般流程：



定价属性

每个定价订阅都有以下属性：

- 组织
- 名称
- 创建时间
- 显示名称
- 描述
- 计划：计划数组。
- 是否启用

- 应用

要查看定价界面的示例，请参考下图：

Edit Pricing Save Save & Exit

Organization : built-in

Name : pricing_casdoor

Display name : Casdoor Pricing

Description : Casdoor hosting services providered by Casbin Inc.

Application : app-built-in

Plans : plan_basic ✘ | plan_premium ✘ | plan_enterprise ✘

Trial duration : 7

Is enabled :

Preview : [Copy pricing page URL](#)

Casdoor Pricing

Casdoor hosting services providered by Casbin Inc.

Basic Plan	Premium Plan	Enterprise Plan
\$ 10.01 per month	\$ 20.02 per month	\$ 30.03 per month
For small teams, with limited technical support	For fast growing start-ups, with full technical support	For large & medium-sized enterprise, with full technical support
Getting started	Getting started	Getting started

订阅

订阅功能有助于管理用户选择的计划，使得控制对应用功能的访问变得容易。

提示

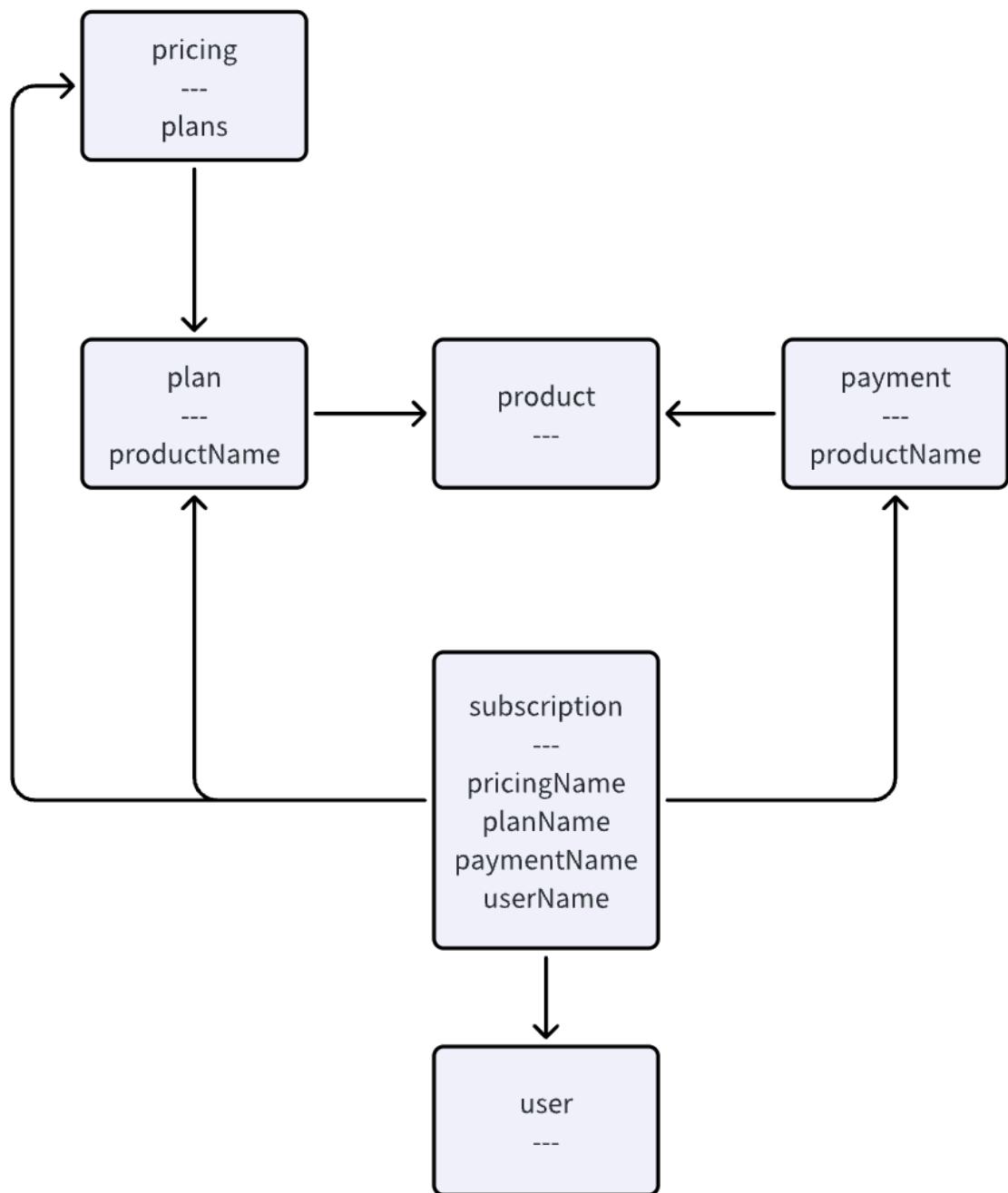
由于每个计划都基于一个角色，您可以将计划的角色分配给用户，并使用强制API进行权限检查。

订阅可以通过三种方式创建：

- 由管理员手动创建
- Via the Pricing flow when purchasing a product with pricing and plan information (available for all user types)
- 通过API

Any user can create a subscription when purchasing a product, enabling flexible conversion from free to paid tiers. Subscription enforcement (requiring an active subscription for access) only applies to users with type = "paid-user".

定价、计划、订阅、产品和支付之间的关系如下：



订阅属性

每个订阅都有以下属性：

- 所有者
- 名称
- 创建时间
- 显示名称
- 描述
- 持续时间：订阅的持续时间。
- 开始时间：订阅生效的开始时间。
- 结束时间：订阅生效的结束时间。
- 定价：相关的定价。
- 计划：相关的计划。
- 支付：相关的支付。
- 用户：持有此订阅的用户。
- 状态：目前，订阅有以下状态：待处理、错误、暂停、活动、即将到来、过期。

Edit Subscription

Organization <small>②</small> :	built-in
Name <small>②</small> :	sub.e719e2
Display name <small>②</small> :	New Subscription - e719e2
Duration <small>②</small> :	30
Start time <small>②</small> :	2023-08-25 <input type="button" value=""/>
End time <small>②</small> :	2023-09-24 <input type="button" value=""/>
User <small>②</small> :	paid-user-x
Pricing <small>②</small> :	pricing_casdoor
Plan <small>②</small> :	plan_premium
Payment <small>②</small> :	payment_20230825_160124_2d18867
Description <small>②</small> :	
State <small>②</small> :	<input checked="" type="radio"/> Active <input type="radio"/> Pending <input type="radio"/> Upcoming <input type="radio"/> Expired <input type="radio"/> Error <input type="radio"/> Suspended

Transaction

The **Transaction** feature tracks financial activities for users and organizations in Casdoor, enabling balance management and transaction history.

Transactions are automatically created when users make purchases or recharge their balance. Each transaction updates the corresponding user or organization balance in real-time.

Transaction Categories

Transactions in Casdoor fall into two categories:

User Transactions track individual user balances. When a user transaction is created, it updates both the user's balance and the organization's total user balance sum.

Organization Transactions track the organization's own operational balance, separate from user balances.

Transaction Properties

Every Transaction has these properties:

- **Owner**
- **Name**
- **CreatedTime**

- `Category`: Either "User" or "Organization"
- `Type`: The transaction type (e.g., "Recharge", "Purchase")
- `User`: Required for User category transactions
- `Amount`: Transaction amount (positive for income, negative for expenses)
- `Currency`: The currency code (e.g., "USD", "CNY")
- `State`: Transaction state (e.g., "Pending", "Paid", "Failed")
- `Payment`: Related Payment record (if applicable)

Balance Tracking

Casdoor maintains separate balance fields:

User Balance is stored on individual user records and tracks each user's available funds.

Organization Balances include two fields: `orgBalance` for the organization's own funds, and `userBalance` for the sum of all user balances within that organization.

Balances are automatically updated when transactions are created, modified, or deleted, ensuring consistency across the system.

Viewing Transactions

Transaction history is displayed in two locations:

When editing a user account, all transactions for that user appear in a dedicated table below the user details.

When editing an organization, all organization-level transactions are shown in the organization edit page.

Both views provide a chronological record with transaction details including name, creation time, category, type, amount, and state.

用户

概述

在Casdoor中管理用户

MFA / 2FA

使用MFA / 2FA保护您的账户

User Impersonation

Using master password to impersonate users in Casdoor

用户角色

分配给用户的角色

 权限

用户权限

 Forms

A tool for customizing list page displays of system entities.

概述

用户属性

作为一个认证平台，Casdoor 能够管理用户。每个用户都有以下属性：

- `Owner`: 拥有用户的组织
- `Name`: 唯一的用户名
- `CreatedTime` 创建时间
- `UpdatedTime`
- `Id`: 每个用户的唯一标识符
- `Type`
- `Password`
- `PasswordSalt`
- `PasswordOptions`: 密码复杂性选项
- `DisplayName`: 在用户界面中显示
- `FirstName`
- 姓氏
- `Avatar`: 链接到用户的头像
- 永久头像
- 电子邮件
- 电话
- 位置
- 地址
- 隶属

- 标题
- 身份证类型
- 身份证
- 主页
- 生物
- 标签
- 区域
- 语言
- 性别
- 生日
- 教育
- 得分
- 因果
- 排名
- IsDefaultAvatar
- IsOnline
- IsAdmin: 表示用户是否是其组织的管理员
- IsGlobalAdmin: 表示用户是否有权限管理Casdoor
- IsForbidden
- IsDeleted: When a user is soft-deleted (`IsDeleted = true`), they cannot sign in through any authentication method, including OAuth providers. This prevents deleted users from re-registering via third-party login.
- 注册应用程序
- 哈希
- 预哈希
- 创建的IP
- 最后登录时间

- `最后登录IP`
- `Roles`: An array of the user's roles (extended field, read-only via User API)
- `Permissions`: An array of the user's permissions (extended field, read-only via User API)

社交平台登录的唯一ID:

- `Github`
- `Google`
- `QQ`
- `微信`
- `Facebook`
- `钉钉`
- `微博`
- `Gitee`
- `LinkedIn`
- `Wecom`
- `Lark`
- `Gitlab`
- `Adfs`
- `Baidu`
- `Casdoor`
- `Infoflow`
- `Apple`
- `Azure AD`
- `Azure AD B2C`
- `Slack`
- `Steam`

- Ldap

Email Normalization

Casdoor normalizes all email addresses to lowercase to ensure uniqueness and prevent duplicate accounts. This means that `user@example.com`, `User@Example.com`, and `USER@EXAMPLE.COM` are treated as the same email address, complying with RFC 5321 standards.

This normalization happens automatically during:

- User signup and account creation
- User login and authentication
- Email duplicate checking

Understanding Roles and Permissions Fields

The `Roles` and `Permissions` fields in the User object are extended fields that are dynamically populated when retrieving user data. These fields are not stored directly in the User table but are collected from the Roles and Permissions resources through the `ExtendUserWithRolesAndPermissions()` function.

Important: You cannot update roles and permissions through the `/api/update-user` endpoint, even when using the `columns` parameter. To manage user roles and permissions, you must use the dedicated APIs for Roles and Permissions resources.

To assign roles or permissions to users:

- Roles: Use the Roles API endpoints to create and assign roles. Visit the Roles management page (e.g., <https://door.casdoor.com/roles>) or use the [roles API](#).
- Permissions: Use the Permissions API endpoints to create and assign permissions. Visit the Permissions management page (e.g., <https://door.casdoor.com/permissions>) or use the [permissions API](#).

Using the Properties Field

The `Properties` field is a flexible key-value map (`map[string]string`) that allows you to store custom attributes for users beyond the predefined fields in the User schema. This is particularly useful when you need to:

- Store organization-specific user attributes
- Add custom metadata that doesn't fit into standard fields
- Extend user profiles without modifying the core schema

从XLSX文件导入用户

您可以通过上传包含用户信息的XLSX文件来添加新用户或更新现有的Casdoor用户。

在管理员控制台中，转到用户并点击上传 (.xlsx) 按钮。

选择你的XLSX文件并点击打开。用户将被导入。

我们提供了 [模板XLSX文件](#) `user_test.xlsx` 在 `xlsx` 文件夹中。该模板包含5个测试用户和一些必需用户属性的标题。

Home	Organizations	Users	Roles	Permissions	Providers	Applications	Users uploaded successfully, refreshing the page				Syncers	Certs	Swagger	Admin
Users													Actions	
	Organization	Application	Name	Created time	Display name	Avatar	Email	Phone	Affiliation	Country/Region	Tags	Action		
built-in	app-built-in	tesla	2022-03-20 20:49:03	Nikola Tesla		9v73hn@example.com	40738134827	Example Inc.	United States of America	scientist	<button>Edit</button>	<button>Delete</button>		
built-in	app-built-in	gauss	2022-03-20 20:48:33	Carl Friedrich Gauss		vqdsan@example.com	98621482844	Example Inc.	Germany	mathematician	<button>Edit</button>	<button>Delete</button>		
built-in	app-built-in	galileo	2022-03-20 20:47:58	Galileo Galilei		8p4f38@example.com	22596937332	Example Inc.	Italy	scientist	<button>Edit</button>	<button>Delete</button>		
built-in	app-built-in	euler	2022-03-20 20:47:08	Leonhard Euler		3dzw4j@example.com	74409642681	Example Inc.	Switzerland	mathematician	<button>Edit</button>	<button>Delete</button>		
built-in	app-built-in	einstein	2022-03-20 20:46:29	Albert Einstein		z6mive@example.com	60062541396	Example Inc.	Germany	scientist	<button>Edit</button>	<button>Delete</button>		
built-in	app-built-in	admin	2022-03-20 20:07:23	Admin		admin@example.com	12345678910	Example Inc.		staff	<button>Edit</button>	<button>Delete</button>		

绕过密码加密

当从外部数据库迁移用户到Casdoor时，可能会出现您希望绕过或控制由 `organization` 默认密码类型方法提供的默认加密方法的情况。

这可以通过在用户导入过程中使用 `passwordType` 字段来实现。

① 备注

使用Bcrypt密码的用户

以下是API路由 `/api/add-user` 的POST体请求示例。

```
{  
  "owner": "组织",  
  "signupApplication": "first-app",  
  "email": "dev@dev.com",  
  "name": "dev",  
  "displayName": "开发者",  
  "password": "$2a$10$.o/  
iVyDE9Xk8iowyHDnQRu72Rvi0i6FPa1ujhusbSCZeg7V0a6MY6",  
  "passwordType": "bcrypt",  
}
```

在这里，用户的密码已经使用bcrypt算法进行了加密，所以我们将 `passwordType` 指定为"bcrypt"，以通知Casdoor不要再次加密它。

MFA / 2FA

关于多因素身份验证

MFA（多因素身份验证）是一种可以增强用户和系统安全性的安全措施。它要求用户在登录或执行敏感操作时提供两个或更多的身份验证因素。

Casdoor supports multiple second-factor authentication methods including SMS codes, email codes, TOTP authenticator apps, and RADIUS authentication.

Once you enable MFA, Casdoor requires an authentication code every time someone attempts to sign in to your account. 只有知道您的密码并能获取身份验证代码的人才能登录您的账户。

配置MFA

1. 在用户个人资料页面，您可以看到多因素身份验证的配置。如果您看不到它，请确保组织在账户项目表中添加了多因素身份验证项目。

Managed accounts ②

Managed accounts **Add**

Application	Username	Password	Action
			No data

Multi-factor authentication ②:

Multi-factor methods

Type : sms

Type : email

Setup

Setup

ID card ②:

2. 点击“设置”按钮。

Multi-factor authentication ②:

Multi-factor methods

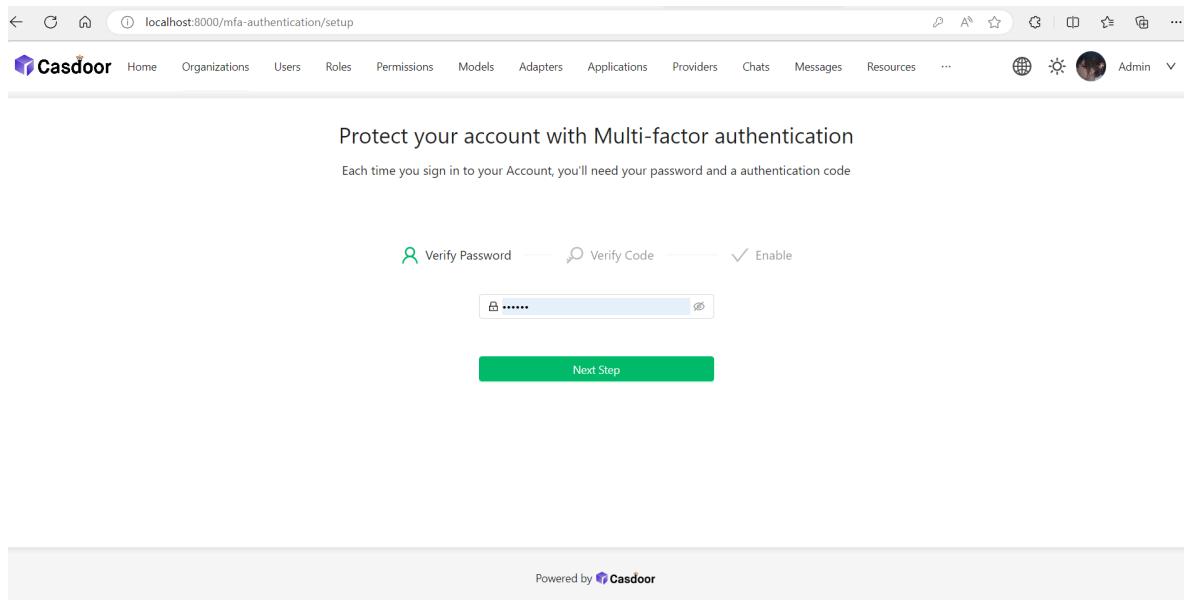
Type : sms

Type : email

Setup

Setup

3. 输入您的密码并点击“下一步”。



使用TOTP移动应用配置多因素身份验证

基于时间的一次性密码（TOTP）应用自动生成一个在一定时间后更改的身份验证代码。我们建议使用：

- [Google Authenticator](#)
- [Microsoft Authenticator.](#)

💡 提示

To configure authentication via TOTP on multiple devices, during setup, scan the QR code using each device at the same time. 如果2FA已经启用，而您想添加另一个设备，您必须从用户个人资料页面重新配置您的TOTP应用。

Protect your account with Multi-factor authentication

Each time you sign in to your Account, you'll need your password and a authentication code

 Verify Password —  Verify Code —  Enable



Scan the QR code with your authenticator app

Or copy the secret to your authenticator app

P757K7XT5MIO5RPZQYS0



 Passcode

Next Step

[Use email](#) [Use SMS](#)

1. 在“验证代码”步骤中，执行以下操作之一：

- 使用您的移动设备的应用扫描二维码。 扫描后，应用会显示一个六位数的代码，您可以在Casdoor上输入。
- 如果您无法扫描二维码，您可以手动复制并在您的TOTP应用中输入密钥。

2. TOTP移动应用将您的Casdoor账户保存并每隔几秒生成一个新的身份验证代码。 在Casdoor上，将代码输入到“验证码”字段并点击“下一步”。

3. 在“启用”按钮上方，复制您的恢复代码并将它们保存到您的设备上。 将它们保存到一个安全的位置，因为您的恢复代码可以帮助您在失去访问权限时重新获得对您账户的访问。

Protect your account with Multi-factor authentication

Each time you sign in to your Account, you'll need your password and a authentication code

 Verify Password —  Verify Code —  Enable

Please save this recovery code. Once your device cannot provide an authentication code, you can reset mfa authentication by this recovery code

ad30de29-3ce0-4e39-a97f-ceff1d503d3c

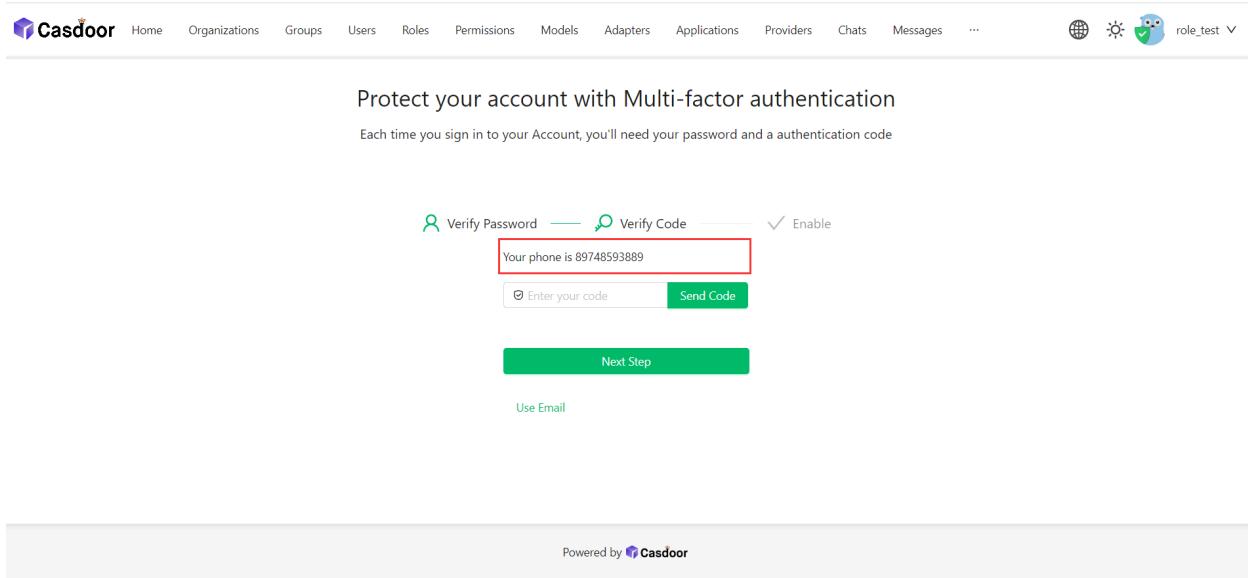
Enable

注意事项

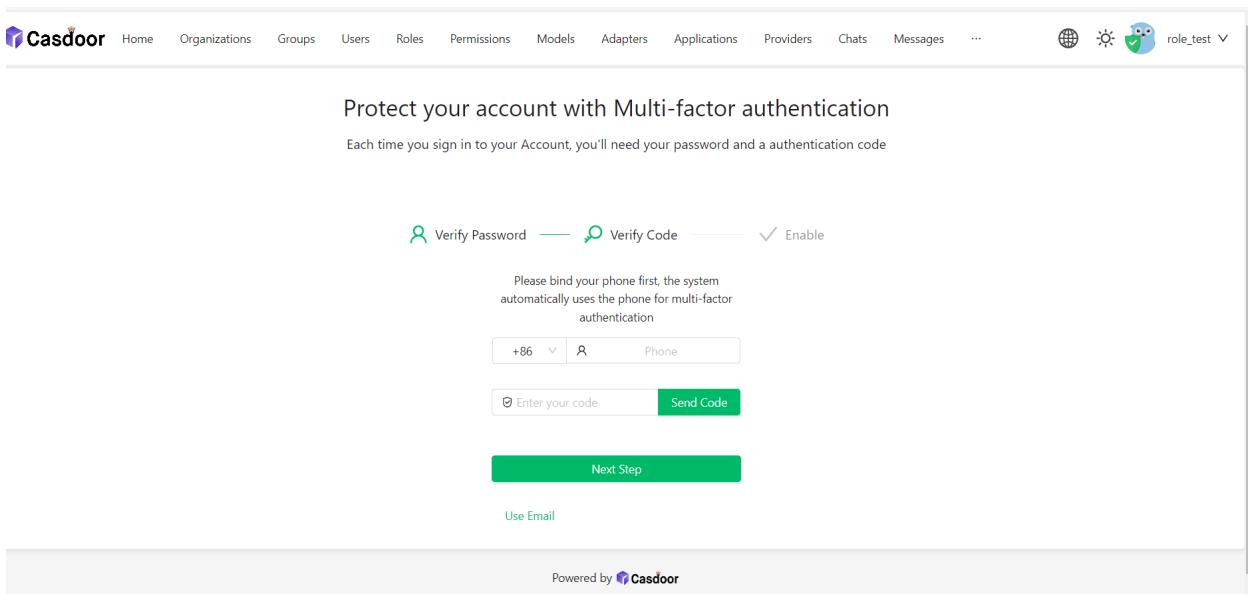
Each recovery code can only be used once. 如果您使用恢复代码登录，它将变为无效。

使用短信配置多因素身份验证

如果您已添加您的手机号码，Casdoor将使用它向您发送短信。



如果您还没有添加您的手机号码，您需要先添加它。



1. 选择您的国家代码并输入您的手机号码。
2. 检查您的信息是否正确并点击“发送代码”。
3. 您将收到一条带有安全代码的短信。然后将代码输入到“输入您的代码”字段并点击“下一步”。

4. 在“启用”按钮上方，复制您的恢复代码并将它们保存到您的设备上。将它们保存到一个安全的位置，因为您的恢复代码可以帮助您在失去访问权限时重新获得对您账户的访问。

使用电子邮件配置多因素身份验证

将电子邮件配置为您的多因素身份验证方法与使用短信类似。

1. 使用您当前的电子邮件或输入您的电子邮件地址并点击“发送代码”。
2. 然后将代码输入到“输入您的代码”字段并点击“下一步”。
3. 在“启用”按钮上方，复制您的恢复代码并将它们保存到您的设备上。将它们保存到一个安全的位置，因为您的恢复代码可以帮助您在失去访问权限时重新获得对您账户的访问。

Configuring multi-factor authentication using RADIUS

RADIUS MFA allows you to authenticate against an external RADIUS server for the second authentication factor. This is useful when integrating with existing authentication infrastructure.

Before using RADIUS MFA, your administrator must configure a RADIUS provider in the application. Once configured:

1. Enter your RADIUS username when prompted during setup.
2. Enter your RADIUS password to verify the setup. This password will be verified against the configured RADIUS server. During subsequent logins, you'll enter this same RADIUS password as your second factor.
3. Above the "Enable" button, copy your recovery codes and save them to your device. Save them to a secure location because your recovery codes can help

you regain access to your account if you lose access.

ⓘ 备注

The RADIUS authentication communicates with the external RADIUS server configured by your administrator. Make sure you have the correct username and password for your RADIUS account.

更改您首选的MFA方法

您可以添加多种MFA方法。 只有首选方法才会在您登录时使用。

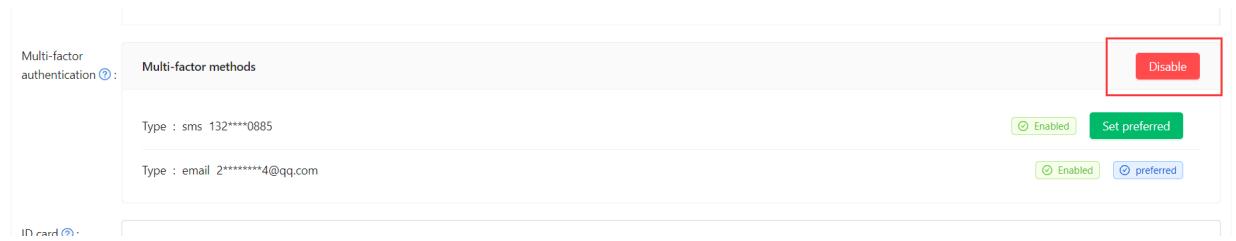
如果您想设置首选的MFA方法, 请点击“设置首选”按钮。



您首选的方法上将显示“首选”标签。

禁用多因素身份验证

如果您想禁用多因素身份验证, 请点击“禁用”按钮。 您的所有多因素身份验证设置将被删除。



User Impersonation

User impersonation allows administrators to temporarily sign in as another user within their organization. This feature is useful for troubleshooting user-specific issues, testing permissions, or providing support without requiring the user's actual password.

Overview

Casdoor supports user impersonation through the **Master Password** feature. When an organization's master password is configured, administrators can use it to sign in as any user within that organization.

How It Works

When you attempt to sign in as a user, Casdoor checks the password in the following order:

1. First, it checks if the entered password matches the organization's master password
2. If not, it checks if the password matches the user's actual password

If either check succeeds, the authentication is successful. This means that when a master password is set, administrators can use it to sign in as any user account.

Setting Up Master Password

To enable user impersonation in your organization:

1. Navigate to your **Organization** settings in the Casdoor admin console
2. Go to the **Organizations** page
3. Click on your organization to edit it
4. Find the **Master Password** field
5. Enter a strong, secure password
6. Save the changes



注意事项

Security Important

The master password is extremely sensitive. Anyone with access to the master password can sign in as any user in the organization. It should be:

- Known only to trusted administrators
- Stored securely (e.g., in a password manager)
- Changed immediately if compromised
- Sufficiently complex and unique

Using Master Password for Impersonation

To sign in as a user using the master password:

1. Go to the login page for your organization: `/login/<organization_name>`



提示

Example

For an organization named "my-company", use: `https://your-casdoor-domain.com/login/my-company`

2. Enter the username of the user you want to impersonate
3. Enter the organization's master password (not the user's password)
4. Sign in

You will be authenticated as that user and have access to their account with their permissions and settings.

Use Cases

Common scenarios where user impersonation is helpful:

- **Technical Support:** Troubleshoot user-specific issues by viewing exactly what the user sees
- **Testing:** Verify that permissions and roles are working correctly for different user types
- **Emergency Access:** Access critical information when a user is unavailable
- **Demonstration:** Show features or workflows from a specific user's perspective
- **Audit:** Investigate suspicious activity or verify user actions

Disabling User Impersonation

To disable user impersonation:

1. Navigate to your Organization settings
2. Find the Master Password field
3. Clear the master password field
4. Save the changes

Once removed, administrators will no longer be able to use a master password to sign in as other users.

Related Features

- **Default Password:** Organizations can also set a default password that is assigned to new users when they are created
- **Password Complexity:** Configure password requirements to ensure all passwords (including master password) meet security standards
- **Multi-Factor Authentication (MFA):** Even when using master password, MFA requirements will still apply if enabled for the user

用户角色

每个用户可以拥有多个角色。 您可以在用户的个人资料上查看分配给他们的角色。

Bio [?](#) :

Tag [?](#) : staff

Signup application [?](#) : app-built-in

Roles [?](#) : [role_test](#) [role_test2](#)

Permissions [?](#) : [permission_test](#)

3rd-party logins [?](#) :

Is admin [?](#) :

Is global admin [?](#) :

Is forbidden [?](#) :

Is deleted [?](#) :

角色属性

每个角色都有以下属性：

- 所有者
- 名称
- 创建时间
- 显示名称
- 已启用
- Users：属于此角色的子用户数组
- Roles：属于此角色的子角色数组

Managing Roles via API

Roles are managed as separate resources in Casdoor. When you retrieve a user object, the `Roles` field is populated dynamically by extending the user data with information from the Roles resource.

To assign or update roles for users, use the Roles API endpoints rather than the User API. You can manage roles through:

1. Web UI: Navigate to the Roles management page (e.g.,
<https://door.casdoor.com/roles>)
2. API: Use the role-specific endpoints documented in the [Casdoor API reference](#)

The Role resource allows you to define roles with specific users assigned to them. When a user is added to a role's `Users` array, that role will automatically appear in the user's `Roles` field when retrieving user data.

权限

每个用户可能有多个权限。 您可以在他们的个人资料上查看用户的权限。

Bio [?](#) :

Tag [?](#) : staff

Signup application [?](#) : app-built-in

Roles [?](#) : [role_test](#) [role_test2](#)

Permissions [?](#) : [permission_test](#)

3rd-party logins [?](#) :

Is admin [?](#) :

Is global admin [?](#) :

Is forbidden [?](#) :

Is deleted [?](#) :

权限属性

权限具有以下属性：

- 所有者
- 名称
- 创建时间
- 显示名称
- 已启用
- 模型
- Users: An array of users belonging to this permission

- `Roles`: An array of roles belonging to this permission
- 资源类型
- `Resources`: 资源的数组
- `Actions`: 一个动作数组
- 效果

Managing Permissions via API

Permissions are managed as separate resources in Casdoor. When you retrieve a user object, the `Permissions` field is populated dynamically by extending the user data with information from the Permissions resource.

To assign or update permissions for users, use the Permissions API endpoints rather than the User API. You can manage permissions through:

1. Web UI: Navigate to the Permissions management page (e.g.,
<https://door.casdoor.com/permissions>)
2. API: Use the permission-specific endpoints documented in the [Casdoor API reference](#)

The Permission resource allows you to define permissions with specific users and roles assigned to them. When a user is added to a permission's `Users` array or belongs to a role in the permission's `Roles` array, that permission will automatically appear in the user's `Permissions` field when retrieving user data.

Forms

The Forms feature is a tool, built to customize the display and configuration of list pages for the system's core entities. Administrators use the Forms feature to configure list page layouts and preview their final appearance.

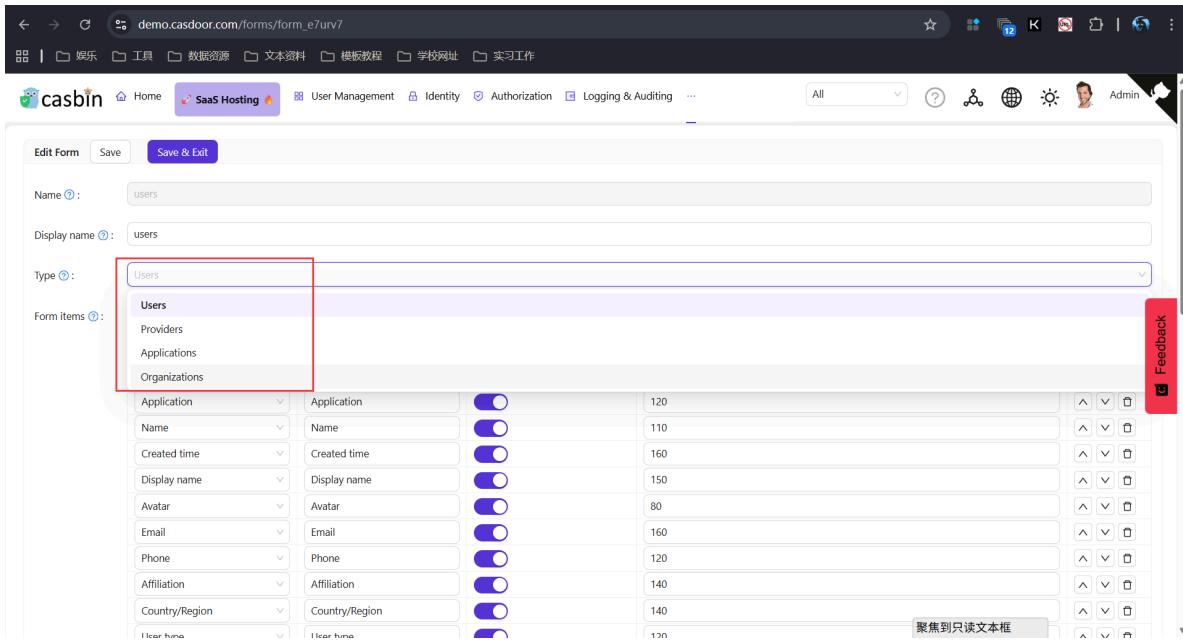
1. Forms Overview

The initial landing page of the Forms feature provides a comprehensive overview of all existing Forms in the system.

The screenshot shows the Casdoor web application interface. The URL in the browser is `demo.casdoor.com/forms`. The top navigation bar includes links for Home, SaaS Hosting, User Management, Identity, Authorization, Logging & Auditing, and Admin. The main content area is titled "Forms" and shows a table with one row. The row contains the name "form_e7urv7", the display name "New Form - e7urv7", and a note "(empty)". To the right of the table is a "System Info" sidebar with sections for Forms, Syncers, Webhooks, and Swagger. A context menu is open over the first row, with the "Forms" option highlighted. At the bottom of the page, there is a footer bar with the Casdoor logo and a "Feedback" button.

2. Form Type Selection

To customize a specific list page, administrators first select the relevant **Form Type**—a classification that maps directly to the entity's list page (e.g., "User List Page", "Provider List Page").



3. Form Items Management

- **Modify Existing Form Items:** Update properties like `Label` (e.g., rename "User ID" to "Employee ID"), `Width` (adjust pixel column width), and `Visible` (toggle column display on/off).
- **Delete Unneeded Form Items:** Remove irrelevant columns to declutter the list page.
- **Reorder Form Items:** Use "Move Up" or "Move Down" controls to adjust the left-to-right sequence of columns on the list page.

The screenshot shows the Casdoor form configuration interface. At the top, there's a navigation bar with links like 'demo.casdoor.com', 'Form items', 'Reset to Default', and 'Add'. Below this is a table titled 'Form items' with columns: Name, Label, Visible, Width, and Action. A red border highlights the first row, which contains 'Organization' as the name, 'Big Organization' as the label, a visible switch (on), a width of 250, and an action column with edit and delete icons. The table also includes other fields like Application, Name, Created time, Display name, Avatar, Email, Phone, Affiliation, Country/Region, User type, Tag, Is admin, Is forbidden, and Is deleted.

4. Form Preview

The preview page mirrors the live system's list page layout, ensuring that column order, labels, widths, and visibility align with requirements before finalizing changes.

The screenshot shows the Casdoor form preview interface. At the top, there's a navigation bar with links like 'demo.casdoor.com', 'Users', 'Add', 'Upload (xlsx)', and 'Preview'. Below this is a search/filter section with fields for 'Is deleted' and a toggle switch. The main area is a table titled 'Preview' with columns: Users, Application, Name, Created time, Display name, Avatar, and Action. The table lists several user entries, each with an 'Edit' and 'Delete' button. The columns correspond to the form items defined in the configuration table above. The preview interface also includes a 'Feedback' button on the right side.



>

邀请码

邀请码

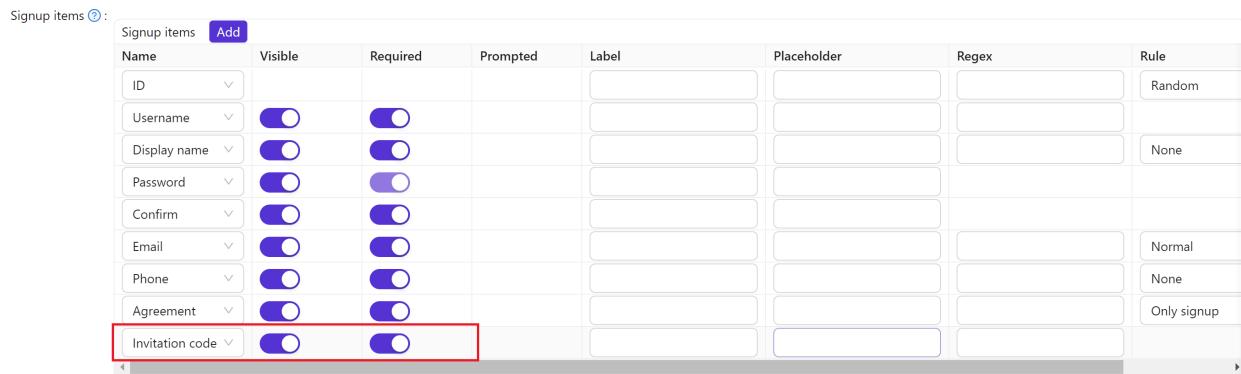


概述

在casdoor中管理邀请

概述

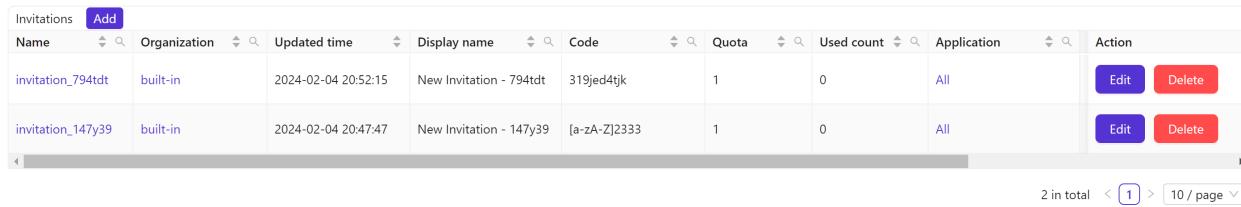
目前，casdoor已经支持更灵活的邀请码方式进行用户注册。一旦管理员以邀请码为必选项打开注册页面，用户只有拥有有效的邀请码才能注册。



The screenshot shows the 'Signup items' configuration section. A table lists various fields: Name, Visible, Required, Prompted, Label, Placeholder, Regex, and Rule. The 'Invitation code' row is highlighted with a red box around its 'Visible' and 'Required' columns, both of which have the value 'true'.

Name	Visible	Required	Prompted	Label	Placeholder	Regex	Rule
ID							Random
Username	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
Display name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					None
Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
Confirm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					Normal
Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					None
Agreement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					Only signup
Invitation code	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					

使用邀请码的主要有两种方式，默认添加的是一个随机字符串码，由随机数字和字母组成。为了更灵活，邀请码还支持正则匹配来匹配多个不同的邀请码。



The screenshot shows the 'Invitations' management page. It displays a table with columns: Name, Organization, Updated time, Display name, Code, Quota, Used count, Application, and Action. There are two entries:

Name	Organization	Updated time	Display name	Code	Quota	Used count	Application	Action
invitation_794tdt	built-in	2024-02-04 20:52:15	New Invitation - 794tdt	319jed4tjk	1	0	All	<button>Edit</button> <button>Delete</button>
invitation_147y39	built-in	2024-02-04 20:47:47	New Invitation - 147y39	[a-zA-Z]2333	1	0	All	<button>Edit</button> <button>Delete</button>

Page navigation: 2 in total | < 1 > | 10 / page

邀请属性

Casdoor通过以下属性管理邀请

- `Organization`: 拥有邀请的组织
- `Name`: 唯一的邀请名称
- `Display name`: 显示的邀请名称

- **Code**: 邀请码，你可以填写具体的邀请码字符串，也可以填写正则表达式
- **Default code**: 用于在邀请链接中填充默认的邀请码。对于随机生成的邀请码，
默认码与邀请码相同。对于正则表达式形式的代码，你需要自己填写符合代码中的
正则表达式规则的默认代码
- **Quota**: 邀请码可以使用的最大次数
- **Used count**: 邀请码已被使用的次数
- **Application**: 允许使用此邀请码的应用。选择 **ALL** 使其对组织下的所有应用都可
用
- **Username**: 使用此邀请注册时需要的特定用户名
- **Email**: 使用此邀请注册时需要的特定电子邮件
- **Phone**: 使用此邀请注册时需要的特定电话
- **State**: 邀请的状态

默认邀请

默认邀请中的邀请码是一个随机生成的数字和字母的字符串，且 **Quota** 设置为1，只能使
用一次。应用默认设置为 **ALL**，这意味着对应此邀请的组织下的所有应用都可以使用此
邀请码。

New Invitation Save Save & Exit Copy signup page URL Cancel

Organization ②: built-in

Name ②: invitation_lxgdf

Display name ②: New Invitation - lxgdf

Code ②: yo8hrfa7sf

Default code ②: yo8hrfa7sf

Quota ②: 1

Used count ②: 0

Application ②: All

Username ②:

Email ②:

Phone ②:

State ②: Active

如果邀请码是为特定用户设置的，你希望用户使用给定的 `username`、`email`、`phone` 和 `invitation code` 注册，你可以通过填写相应的字段来限制用户的注册。如果字段为空或者在注册页面上没有配置，casdoor不会强制验证这些字段

Username ②: Bob

Email ②: bob@qq.com

Phone ②: 15295959595

当需要重复使用邀请码时，你可以将 `Quota` 设置为一个较大的值，例如，如果你希望这个邀请码被使用10次，那么你可以将 `Quota` 设置为10。当你希望停止使用此邀请码注册时，你也可以通过修改邀请的状态为 `Suspended` 来实现。

Quota ②: 10

Used count ②: 0

Application ②: application_ph9si

Username ②:

Email ②:

Phone ②:

State ②: Suspended

⚠ 注意事项

当在邀请中配置了 `username`、`email` 或 `phone` 时，`quota` 不应大于一。这是因为用户的 `username`、`email` 和 `phone` 应该是唯一的，多个用户不应该能够使用相同的 `username`、`email` 或 `phone` 进行注册。

正则匹配邀请

有时候需要大量的邀请码进行用户注册，一一生成邀请码可能非常低效。Casdoor 支持通过正则表达式匹配来验证邀请码。例如，通过将 `Code` 设置为 "[a-z]2333"，任何匹配此正则表达式的邀请码都将被成功匹配为有效的邀请码。

Code ⓘ:	[a-z]2333
Default code ⓘ:	a2333
Quota ⓘ:	2
Used count ⓘ:	0

ⓘ 备注

在使用正则表达式验证邀请码时，每个匹配正则表达式的邀请码只能使用一次，`Quota` 仍然可以限制使用次数。例如，当 `Code` 是 "[a-z]2333" 且 `Quota` 是 2 时，只有最多两个匹配正则表达式的邀请码可以成功使用。

邀请链接

Casdoor 支持复制对应邀请的邀请链接。邀请链接中的邀请码对应于 `Default code` 字段。因此，对于使用正则表达式的邀请，必须手动填写 `Default code` 以生成正确的邀请链接。此外，当使用邀请链接注册时，注册页面将自动填充由对应邀请码的邀请设置的某些字段信息。

New Invitation Cancel

Organization [?](#): built-in

Name [?](#): invitation_lxxgdh

Display name [?](#): New Invitation - lxxgdh

Code [?](#): [a-z]2333

Default code [?](#):

Quota [?](#):

① localhost:7001/signup/app-built-in?invitationCode=a2333 ☆ ⌂ ⌚ ⌚ 无痕模式



* Username:

* Password:

* Email:

* Phone:

* Invitation code:

Have account? [sign in now](#)

Powered by  Casdoor

演示



>

IP Whitelist

IP Whitelist



Overview

Support IP limitation for user entry pages.

Overview

Casdoor supports the ip whitelist function of the entry page. When a user accesses the entry page (login/signup/forget-password), Casdoor will decide whether to allow the user to access the entry page based on whether the client IP is in the whitelist. Here, we will show you how to enable the option to specify the ip whitelist function of the entry page at the user, application and organization levels.

Configuration

User Level

Casdoor will first determine whether the client address meets the user-level ip whitelist requirements.

If you want to specify user-level ip whitelist, you first need to add the "IP whitelist" account item on the edit page of the organization to which the user belongs. Then specify your ip whitelist by filling in the comma separated CIDR list, such as 192.168.1.0/24,25.112.0.0/16. If the ip whitelist is empty, it means there is no restriction on the client IP address.

Is forbidden [?](#) :



IP whitelist [?](#) :

10.201.146.108/16

[Save](#)

[Save & Exit](#)



信息

If you forget how to customize users' account items, Please refer to the [Account Customization](#)

Application Level

If the client IP address passes the user-level check, Casdoor will proceed to perform application-level check. You can specify the ip whitelist through the [IP whitelist](#) configuration option on the application edit page.

Affiliation URL [?](#) :



IP whitelist [?](#) :

192.168.1.0/24

Terms of Use [?](#) :



Organization Level

Organization-level check will be performed last. You can use the [IP whitelist](#) configuration option on the organization edit page to specify organization-level ip whitelist.

Master verification code [?](#) :

IP whitelist [?](#) : 192.168.1.0/24

Init score [?](#) : 2000

Here is a demo video that shows how to use ip whitelist:



>

同步器

同步器

概述

在Casdoor中同步用户

数据库

使用数据库同步器同步数据库

Azure AD

Using Azure AD Syncer to synchronize users from Azure Active Directory

Keycloak

使用 Keycloak Syncer 同步 Keycloak

 **WeCom**

Using WeCom Syncer to synchronize users from WeCom

概述

作为一个认证平台，Casdoor可以轻松管理存储在数据库中的用户。

同步器

Casdoor将用户存储在`user`表中。所以，当你计划使用Casdoor作为认证平台时，无需担心将你的应用程序的用户数据迁移到Casdoor。Casdoor提供了一个**同步器**，可以快速帮助您将用户数据同步到Casdoor。

Casdoor supports multiple syncer types to import users from different sources:

- **Database**: Synchronize users from any database supported by Xorm (MySQL, PostgreSQL, SQL Server, Oracle, SQLite). See [database syncer](#).
- **Azure AD**: Synchronize users from Azure Active Directory using Microsoft Graph API. See [Azure AD syncer](#).
- **Keycloak**: Import users directly from Keycloak databases. See [Keycloak syncer](#).
- **WeCom**: Fetch users from WeCom organizations via API. See [WeCom syncer](#).

同步哈希值

Casdoor使用哈希函数来确定如何更新用户。此哈希值是根据表中每个用户的信息（如密码或手机号码）计算得出的。

如果特定 `Id` 的用户的计算哈希值与原始值相比发生了变化，Casdoor确认用户表已经被更新。随后，数据库更新旧信息，从而实现Casdoor用户表和原始用户表之间的**双向同步**。

数据库

数据库同步器

我们创建的用户表作为演示，是从模板[XLSX文件](#)导入的。

owner	name	created_time	updated_time	id	type	password	password_salt	display_name	first_name	last_name	avatar	permanent_avatar	email
built-in	einstein	2022-03-20T20:46:29+08:00		1c57cc37-37f5-4def-9e9f-082189ef63d2	normal-user	123		Albert Einstein			https://casbin.org		z6mive@
built-in	euler	2022-03-20T20:47:08+08:00		bb7831b4-0d24-4e96-b043-f8fd8d15eb	normal-user	123		Leonhard Euler			https://casbin.org		3dzw4j@
built-in	galileo	2022-03-20T20:47:58+08:00		7920eb6c-f9f5-40ef-8e18-3ac99f49bd15	normal-user	123		Galileo Galilei			https://casbin.org		8p4f38@
built-in	gauss	2022-03-20T20:48:33+08:00		f0c28816-2c0d-479b-b545-cb4cf96db36	normal-user	123		Carl Friedrich Gau			https://casbin.org		vqdsan@
built-in	tesla	2022-03-20T20:49:03+08:00		687c3068-fd21-4d32-b2ba-e13e8b369a	normal-user	123		Nikola Tesla			https://casbin.org		9v73hn@

要创建新的同步器，请转到[同步器选项卡](#)，并按照下面的示例填写所有必需的信息。然后，保存更改。

Organization :

Name :

Type :

Host :

Port :

User :

Password :

Database type :

Database :

Table :

Table columns :

Column name	Add	Column type	Casdoor column	Is key	Is hashed	Action
name		string	Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
id		string	Id	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
first_name		string	FirstName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	



一般来说，你需要至少在Casdoor列中填写 **ID** 和 **Name**。其他重要字段包括

`createdTime`、`Password`和`DisplayName`。

以下字段是必需的:

- `Organization`: 用户将被导入的组织
- `Name`: 同步器名称
- `Type`: 选择"数据库"
- `Host`: 原始数据库主机地址
- `Port`: 原始数据库端口
- `User`: 原始数据库用户名
- `Password`: 原始数据库密码
- `Database type`: 所有Xorm支持的数据库, 如MySQL、PostgreSQL、SQL Server、Oracle和SQLite
- `Database`: 原始数据库名称
- `Table`: 原始用户表名称
- 表格列
- `Column name`: 原始用户列名称
- `Column type`: 原始用户列类型
- `Casdoor Column`: Casdoor用户列名称

可选字段:

- `Is hashed`: 是否计算哈希值. 当此选项启用时, 同步器只有在原始表中的用户字段更新时才会同步用户。如果此选项被禁用, 即使只更新了字段, 同步器仍然会同步用户。简而言之, 只有在参与哈希计算的字段(启用"Is hashed")更新时, 用户才会被同步。
- `Is key`: 是否是原始表中的用户和Casdoor表中的用户的主键。在同步数据库时, 根据选择了"Is key"选项的字段来确定。字段的"Is key"按钮应至少选择一个。如果没有选择, 那么默认选择第一个"Is key"选项。

- **Avatar base URL**: 当同步用户时, 如果**Avatar base URL**不为空且原始**user.avatar**没有"http"前缀, 新的**user.avatar**将被**Avatar base URL + user.avatar**替换。
- **Affiliation table**: 用于从数据库中的此表同步用户的隶属关系。由于隶属关系可能是"Affiliation table"中的int类型代码, 因此需要映射为字符串。参考[getAffiliationMap\(\)](#)。Casdoor有一些冗余字段可以借用, 所以[这里](#)我们使用**score**将int代码映射为字符串名称。

配置好同步器后, 启用**Is enable**选项并保存。同步器将开始工作。

Name	Organization	Created time	Type	Host	Port	User	Password	Database type	Database	Action
syncer_qmpox9	built-in	2023-08-09 18:57:36	Database	localhost	3306	root	password	mysql	auth	<button>Sync</button> <button>Edit</button> <button>Delete</button>

你也可以使用"Sync"按钮进行数据库同步。

更新

当**Table columns**设置如下图所示时, 执行更新操作。

Table columns ②:					
Table columns	Add	Column name	Column type	Casdoor column	Action
<input type="text" value="name"/>	<input type="button" value="▼"/>	<input type="text" value="string"/>	<input type="button" value="▼"/>	<input type="text" value="Name"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="✖"/>
<input type="text" value="id"/>	<input type="button" value="▼"/>	<input type="text" value="string"/>	<input type="button" value="▼"/>	<input type="text" value="Id"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="✖"/>
<input type="text" value="first_name"/>	<input type="button" value="▼"/>	<input type="text" value="string"/>	<input type="button" value="▼"/>	<input type="text" value="FirstName"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="✖"/>
<input type="text" value="password"/>	<input type="button" value="▼"/>	<input type="text" value="string"/>	<input type="button" value="▼"/>	<input type="text" value="Password"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="✖"/>

如果两个表中的关键数据不同, 可以根据主键在两个表之间同步数据。

- 在原始表中更新用户
- 在Casdoor表中更新用户

添加

当 Table columns 设置如下图所示时，执行添加操作。

Table columns ②:						
Column name	Column type	Casdoor column	Is key	Is hashed	Action	
name	string	Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
id	string	Id	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
first_name	string	FirstName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
password	string	Password	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

如果两个表之间的数据数量不同，可以根据主键将数据添加到数据量较少的表中。

- 在原始表中添加用户
- 在Casdoor表中添加用户

Azure AD

Azure AD Syncer enables automatic user synchronization from Azure Active Directory (Microsoft Entra ID) to Casdoor. The syncer uses the Microsoft Graph API to fetch user information and keeps your user directory up to date.

Prerequisites

Before configuring the Azure AD syncer, you need to set up an application registration in Azure Portal with the appropriate permissions.

Step 1: Register an Application

Navigate to [Azure Portal](#) and register a new application:

1. Go to Azure Active Directory → App registrations → New registration
2. Enter a name for your application
3. Select the appropriate account type (typically "Accounts in this organizational directory only")
4. Click Register

Step 2: Create a Client Secret

After registration, create a client secret:

1. In your application, go to Certificates & secrets
2. Click New client secret
3. Add a description and select an expiration period

4. Click Add and copy the secret value immediately (it won't be shown again)

Step 3: Grant API Permissions

Configure the required Microsoft Graph API permissions:

1. Go to API permissions → Add a permission
2. Select Microsoft Graph → Application permissions
3. Add the `User.Read.All` permission
4. Click Grant admin consent for your organization



The `User.Read.All` permission allows the syncer to read all user profiles in your Azure AD tenant.

Configuration

To create an Azure AD syncer in Casdoor:

1. Navigate to the Syncers tab
2. Click Add to create a new syncer
3. Fill in the following required fields:

Field	Description
Organization	The Casdoor organization where users will be imported
Name	A unique identifier for this syncer

Field	Description
Type	Select "Azure AD"
Tenant ID	Your Azure AD tenant ID (found in Azure Portal → Azure Active Directory → Overview)
Client ID	The Application (client) ID from your app registration
Client Secret	The client secret value you created earlier

Other database-related fields (Database type, Port, Database, Table) are not used for Azure AD syncer and can be left empty.

Field Mappings

The syncer automatically maps Azure AD user attributes to Casdoor user fields:

Azure AD Field	Casdoor Field	Description
id	Id	User's unique identifier
userPrincipalName	Name	User principal name
displayName	DisplayName	User's display name
givenName	FirstName	First name

Azure AD Field	Casdoor Field	Description
surname	LastName	Last name
mail	Email	Email address
mobilePhone	Phone	Mobile phone number
jobTitle	Title	Job title
officeLocation	Location	Office location
preferredLanguage	Language	Preferred language
accountEnabled	IsForbidden	Account status (inverted)

① 信息

The `accountEnabled` field is inverted when mapped to `IsForbidden`.

When a user is disabled in Azure AD (`accountEnabled: false`), they will be marked as forbidden in Casdoor (`IsForbidden: true`).

Running the Syncer

After configuration:

1. Click **Test Connection** to verify your credentials and permissions
2. Enable the syncer by toggling **Is enabled**
3. Click **Sync** to trigger an immediate synchronization

4. The syncer will automatically fetch all users from your Azure AD tenant

The syncer handles pagination automatically, retrieving all users regardless of the total count.

Keycloak

Keycloak 同步器

Keycloak同步器本质上与数据库同步器相同，增加了对Keycloak的Tables和Table columns的自动配置功能。

此外，Keycloak同步器将从credential表，keycloak_group表和user_group_membership表中获取数据，因为Keycloak中的用户信息是存储在多个表中的。

The screenshot shows the configuration page for a Keycloak syncer. At the top, there are fields for Organization (built-in), Name (keycloak), Type (Keycloak), Host (localhost), Port (3306), User (root), Password (root), Database type (MySQL), and Database (keycloak). A red box highlights the 'Table' field containing 'user_entity'. An arrow points from this field to a note: 'configured automatically after selecting Keycloak as syncer type'. Below this, the 'Table primary key' field is empty. At the bottom, a large red box encloses the 'Table columns' section. This section contains a table with columns: Table columns, Add, Column name, Column type, Casdoor column, Is hashed, and Action. The table lists various user attributes: ID (string, Id, Yes, edit), USERNAME (string, Name, Yes, edit), USERNAME (string, DisplayName, Yes, edit), EMAIL (string, Email, Yes, edit), EMAIL_VERIFIED (boolean, EmailVerified, Yes, edit), FIRST_NAME (string, FirstName, Yes, edit), LAST_NAME (string, LastName, Yes, edit), CREATED_TIMESTAMP (string, CreatedTime, Yes, edit), and ENABLED (boolean, IsForbidden, Yes, edit). Each row has up/down arrows for reordering and a delete icon in the Action column.

Table columns	Add	Column name	Column type	Casdoor column	Is hashed	Action
ID		string	Id	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
USERNAME		string	Name	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
USERNAME		string	DisplayName	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
EMAIL		string	Email	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
EMAIL_VERIFIED		boolean	EmailVerified	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
FIRST_NAME		string	FirstName	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
LAST_NAME		string	LastName	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
CREATED_TIMESTAMP		string	CreatedTime	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙
ENABLED		boolean	IsForbidden	Yes	<input checked="" type="checkbox"/>	▲ ▼ ⏙

WeCom

WeCom Syncer allows you to automatically import users from your WeCom (企业微信) organization into Casdoor. The syncer fetches user information from all departments in your WeCom organization through the WeCom API and keeps the user data synchronized.

Configuration

以下字段是必需的：

- Organization: The Casdoor organization where users will be imported
- Name: A unique name for this syncer
- Type: Select "WeCom"
- Corp ID: Your WeCom organization's Corp ID
- Corp Secret: The secret for your WeCom application

Setup Steps

Step 1: Obtain WeCom Credentials

In your WeCom management platform, navigate to **My Company**, get Corp ID in **Company Information**.

WeCom

Service Provider Console | API Documentation | CSR | Quit

Homepage Contacts Collaboration App Management Customers and Partners Advanced Features Security and Management My Company

Company Information

Permissions

Chat Management

Contacts Management

Workspace Management

WeChat Workplace

External Communication Management

Security and Confidentiality

Setting

Company Information

Company Logo  Recommended size: 702*180 [Go to verify](#)

Company short name **usher** (未认证) [Modify](#) Company not verified. After verification, the number of users can be increased.

Company address [Add](#)

Phone No. [Add](#)

Company Domain Na... [Add](#)

Company member **1 member(s)** [Statistics](#)

Company Department **1 dept(s)**

Added/Max. **1/1000** [Verify now to increase the limit](#)

Invoice Title [Add](#) Set VAT invoice titles for company members [?](#)

Industry Type **Internet and Related Services** [Modify](#)

Company Size **1-50** [Modify](#)

Creation time **2023-6-18**

Company ID **ww752595f99d89b1ca**

Already a WeCom service provider. [Go to Service Provider Platform](#)

In your Self-build App, get App secret (Corp Secret).

WeCom

Service Provider Console | API Documentation | CSR | Quit

Homepage Contacts Collaboration App Management Customers and Partners Advanced Features Security and Management My Company

Casdoor

« Back

 Casdoor ↴
No app info Enabled

AgentId **1000003** [Edit](#)

Secret [View](#)

Allowed users 

Optionally, in Sync of Contacts Management Tool, you can get Sync of Contacts secret for advanced configurations.

The screenshot shows a web-based management tool for WeCom. At the top, there's a navigation bar with links for 'Homepage', 'Contacts', 'Collaboration', 'App Management', 'Customers and Partners', 'Advanced Features', 'Security and Management' (which is underlined), and 'My Company'. Below the navigation is a header bar with a back button and the title 'Sync of Contacts'. The main content area has a section titled 'Sync of Contacts' with a green icon. It says 'Companies can sync contacts through APIs or authorized third-party service providers' and provides a link to 'API Documentation'. There are two tabs: 'Sync method' (selected) and 'API Sync'. Under 'Sync method', there's a 'Permission' section with a 'Read and edit Contacts' button and 'Edit' and 'View Permission Details' links. A 'Secret' field is highlighted with a red border. Below this, there's a section for 'Company's Trusted IP' which states '3 IP address(es) are configured.' with a 'Settings' link. It also mentions that only configured IP addresses can access company data via API. Another section allows setting an 'event receiving server' URL to push data to Casdoor. At the bottom, there's a 'Disable API sync' link.

Step 2: Configure the Syncer in Casdoor

Go to Syncers tab, select WeCom type and fill in the required information:

- Enter your WeCom Corp ID in the Corp ID field
- Enter your application Secret (App secret) in the Corp Secret field

Then save the changes.

Edit Syncer
Save
Save & Exit

Organization [?](#) : built-in

Name [?](#) : wecom_syncer

Type [?](#) : WeCom

Database type [?](#) : MySQL

Host [?](#) :

Port [?](#) :

User [?](#) : Company ID

Password [?](#) : App secret

Client secret [?](#) : Sync of contacts secret

Database [?](#) :

Table [?](#) :

Click **Test Connection** to verify your credentials before enabling the syncer.

Field Mappings

The syncer automatically maps WeCom user fields to Casdoor user fields:

WeCom Field	Casdoor Field	Description
userid	Id	User's unique identifier
name	DisplayName	User's display name
email	Email	Email address
mobile	Phone	Phone number

WeCom Field	Casdoor Field	Description
avatar	Avatar	Profile picture URL
position	Title	Job title
gender	Gender	Gender (1=Male, 2=Female)
status/enable	IsForbidden	Account status

The syncer automatically handles user account status based on WeCom's status and enable fields:

- Activated users (status=1, enable=1): Normal Casdoor users
- Disabled, not activated, or quit users (status=2/4/5 or enable=0): Marked as forbidden in Casdoor

Running the Syncer

After configuration, you can:

- Enable `Is enabled` to allow automatic synchronization on schedule
- Use the `Sync` button to manually trigger a synchronization
- The syncer will fetch users from all departments and deduplicate them automatically



>

Certificates

Certificates



Overview

Managing Certificates in Casdoor

Overview

Certificates (Certs) in Casdoor are used for signing and verifying tokens, as well as for securing communications in various integrations. They contain cryptographic keys that are essential for authentication and encryption processes.

Certificate Properties

Each certificate in Casdoor has the following properties:

- **Owner:** The organization that owns the certificate
- **Name:** The unique name of the certificate
- **CreatedTime:** When the certificate was created
- **DisplayName:** A human-readable name for the certificate
- **Scope:** The scope of the certificate (e.g., `JWT`, `SAML`, `Payment`)
- **Type:** The type of certificate (e.g., `x509`, `Payment`)
- **CryptoAlgorithm:** The cryptographic algorithm used (e.g., `RS256`, `RSA`)
- **BitSize:** The key size in bits (e.g., 2048, 4096)
- **ExpiresInYears:** The expiration period of the certificate in years
- **Certificate:** The public certificate content
- **PrivateKey:** The private key content (stored securely)

Certificate Scopes

Certificates in Casdoor serve different purposes based on their scope:

JWT Certificates

JWT certificates are used to sign and verify JSON Web Tokens (JWT) for authentication. When a user logs in through Casdoor, the access token is signed using the private key of the JWT certificate.

Use cases:

- Signing access tokens for OAuth/OIDC authentication
- Verifying tokens in backend applications
- Securing API communications

The JWT public key is required when configuring Casdoor SDK in your application. You can find and download the public key from the certificate edit page.

Name	Created time	Display name	Scope	Type	Crypto algorithm	Bit size	Expire in years	Action
cert_rjeegc	2022-02-16 11:04:10	New Cert - rjeegc	JWT	x509	RSA	4096	20	<button>Edit</button> <button>Delete</button>
cert-built-in	2022-02-15 12:31:46	Built-in Cert	JWT	x509	RSA	4096	20	<button>Edit</button> <button>Delete</button>

Public key [?](#)

[Copy public key](#)
[Download public key](#)

```
-----BEGIN CERTIFICATE-----
MIIEltCAUgBgAwAgIBAeJAMA0GCSqGSIb3DQEBCwUAUMLYxHTAbBgNVBAoTFENh
c2Rvb3IgT3JnYXSpemF0uW9uMRUewYDVQVQDewvYXXNkb2y9ENcnQwHvNjMjEx
MDExMDgxMTUwWhNNDEmADE1MDgxMTUwJA2MRowGwxDVQKExrDXNkb29yIE9
Z2FuaxPhdGbjEVMBMGAAUEAxMMQzFzZG9vcIBDZXJ0MIIcJcANBgkqhkiG9w0B
AQEEAOCgAg8AMlCCgKAQgAsinpb5E1/ymlt1RISDSSEIRy+lw+RjI4e5ej
rq4b82Myk7heCjzrhmNEVeVxnhXuP0mBq5ypp/Qgo8vgEmjAEiTmz2k1NjQOQ
CjCyvUras0/MmltC0j13x6mY1Kh2jSksMhYY1vatxTEP3+VB8Hjg3MHFWb07
uvFMCleSw-0KErZCKTR8+9VB3janeBz//zQePPVh79bfZate/hLirPKOG9P1g
OwlioCTASasHTP4Qm/LQR0tHqZfbydySpwAQvhnAdFEf/mTsRSB/wuJNCUDP7SLVjC
PTSLVjC027kmbsPtj+btvcqsRAgtwdsB9h62kptjs1Yn7Auol3qt4zo
4W1l5f6nkfko27kmbsPtj+btvcqsRAgtwdsB9h62kptjs1Yn7Auol3qt4zo
Kb1URyXkQJXvwCqzEtUuk5ew5zuPSIDRLoByQTlx0uQlAFNw3g/pzSDjg/
60d6HtmwZn45mjdyfxCdb1Kn7N+xtjnfahkewp2REV+RMcof4GuhsLsmk
mUDeyZ9a8L9j11YEQfMj2/ZEq+RVtU+wB848K/D1bCY+IfrG5fBpwDp526b
oq4SRsvb3Ztbw04ZxvOf/1UOrfjhjblf0hfr/AeZMHPiKQXvz4y+hqz6
8wfD0V9xYcRbSAT72320sYnjyEgn1RohnRgCpjk/Mt2k84BkDwn8CawEA
AQKCAGAHPTjxVINRvYdCfZ1Ytd+IMlMjmpQH9wro86e04Upuxselpbx1Cp0Yu
npf7xjLtzC0u6fDqz82bkt6GOT71xitFymNy4zWkn75gIgw5rmqTr0wwxb
AltXp4ZVM8t53W7mvbhabHAu5050RvBNVn+zrl7/JVdm5wXah3fLQW
aYEltQVn3WWk/Pf2A8WFDF49HKAATgUSk40eccccbaclL6CQ1FnYSb6/pBBG
khadtAkooGwVkcEmldkRzuaau48gBs7dzJkAv7jBW+IK5fRwPfHmySAKLah
bu9Mrr6hdHzlxrHbmD0ahoTwEFmsobuJ26caGEhufo4YIMk+Ba6E6QsmNsNR9
MsauqkSlprY06MjtQ7y1q3Sh18Sz2Ba3kkhby8Zs9Jkj+Dbtq2akQWzDG
JLEttbGgdeYUMS2yc/C/FUVUN/PCdnt765kw7lmOrR2k156wpbFwR9jYgnQzbjd
4AOrgsR3AduXvD0178ce324WVusvxNCjVruBY/Dk0/W7jxjlvXevHGrhe
1Gc+FkKeBnFq6DzDlkx6N80nyzUzLyrmvRuavn9yVcrab5Xh55fIEOHOWo0gH
5GdesqMugTSOeve1R1UmcfcWVMMvvPeEushWjBjL38Bh4wLsQKCAQEAy4x+c+F8
IcbaktsrnHPRMYUJWve39tOvHdtm/3xs60yrsrExLsJaqQ27nOlJF7Xj0H+
vc0GGAA0ojwA6J+QdeEf8lev04t56uMa3dFPWP4J0000HVClrgAo9GC2H0c940/n
6EqWYqz2Axu156RA3P/XetgsixVCFjGzpxFylbzqk871Yb9hc5zz26G3k8+FVZ
dp+DfYfB6jLrVuXdkX/GqUx7fR7zfqvkhmr5ZqvcKXfWSp4H71kQAUTQE
cJ8lgvqFlouOpID6DB10P/Btg5g9a+jSnnxcpcJ9yjchGsj1Tz5Dm0d
ha/rkyN4dNhY20KCAQEA3gekrRODglocoametrwlplrxysK1SMrhAgjBeJidp
98HhNj08wra5XuMS6ZC7R0xOkikSQLp4gtT22W59lq/nPQ7PNSPdN2Rz0lrmHcS
-----END CERTIFICATE-----
```

[Save](#)
[Save & Exit](#)

Private key [?](#)

[Copy private key](#)
[Download private key](#)

```
-----BEGIN PRIVATE KEY-----
MIUKQBAAKCgAgEaInpb5E1/ymlt1RISDSSEIRy+lw+RjI4e5ejrq4b8zMY
k7HejCzrhnNewEVXhXu1P0mbe5ypp/QGo8vgEmjAEiTmz2k1NjQOQjCjyWra
sOf/Mnl1C0j13x6mY1Kh2jSksMhYY1vatxTEP3+VB8Hjg3MHFWb07uvMcje5
W8+0rKeRZCKTR8+9VB3janeBz//zQePPVh79bfZate/hLirPKOG9P1gOvwloC1A
3sarHTP4Qm/LQR0tHqZfbydySpwAQvhnAdFEf/mTsRSB/wuJNCUDP7SLVjC
4W1l5f6nkfko27kmbsPtj+btvcqsRAgtwdsB9h62kptjs1Yn7Auol3qt4zo
Kb1URyXkQJXvwCqzEtUuk5ew5zuPSIDRLoByQTlx0uQlAFNw3g/pzSDjg/
60d6HtmwZn45mjdyfxCdb1Kn7N+xtjnfahkewp2REV+RMcof4GuhsLsmk
mUDeyZ9a8L9j11YEQfMj2/ZEq+RVtU+wB848K/D1bCY+IfrG5fBpwDp526b
oq4SRsvb3Ztbw04ZxvOf/1UOrfjhjblf0hfr/AeZMHPiKQXvz4y+hqz6
8wfD0V9xYcRbSAT72320sYnjyEgn1RohnRgCpjk/Mt2k84BkDwn8CawEA
AQKCAGAHPTjxVINRvYdCfZ1Ytd+IMlMjmpQH9wro86e04Upuxselpbx1Cp0Yu
npf7xjLtzC0u6fDqz82bkt6GOT71xitFymNy4zWkn75gIgw5rmqTr0wwxb
AltXp4ZVM8t53W7mvbhabHAu5050RvBNVn+zrl7/JVdm5wXah3fLQW
aYEltQVn3WWk/Pf2A8WFDF49HKAATgUSk40eccccbaclL6CQ1FnYSb6/pBBG
khadtAkooGwVkcEmldkRzuaau48gBs7dzJkAv7jBW+IK5fRwPfHmySAKLah
bu9Mrr6hdHzlxrHbmD0ahoTwEFmsobuJ26caGEhufo4YIMk+Ba6E6QsmNsNR9
MsauqkSlprY06MjtQ7y1q3Sh18Sz2Ba3kkhby8Zs9Jkj+Dbtq2akQWzDG
JLEttbGgdeYUMS2yc/C/FUVUN/PCdnt765kw7lmOrR2k156wpbFwR9jYgnQzbjd
4AOrgsR3AduXvD0178ce324WVusvxNCjVruBY/Dk0/W7jxjlvXevHGrhe
1Gc+FkKeBnFq6DzDlkx6N80nyzUzLyrmvRuavn9yVcrab5Xh55fIEOHOWo0gH
5GdesqMugTSOeve1R1UmcfcWVMMvvPeEushWjBjL38Bh4wLsQKCAQEAy4x+c+F8
IcbaktsrnHPRMYUJWve39tOvHdtm/3xs60yrsrExLsJaqQ27nOlJF7Xj0H+
vc0GGAA0ojwA6J+QdeEf8lev04t56uMa3dFPWP4J0000HVClrgAo9GC2H0c940/n
6EqWYqz2Axu156RA3P/XetgsixVCFjGzpxFylbzqk871Yb9hc5zz26G3k8+FVZ
dp+DfYfB6jLrVuXdkX/GqUx7fR7zfqvkhmr5ZqvcKXfWSp4H71kQAUTQE
cJ8lgvqFlouOpID6DB10P/Btg5g9a+jSnnxcpcJ9yjchGsj1Tz5Dm0d
ha/rkyN4dNhY20KCAQEA3gekrRODglocoametrwlplrxysK1SMrhAgjBeJidp
98HhNj08wra5XuMS6ZC7R0xOkikSQLp4gtT22W59lq/nPQ7PNSPdN2Rz0lrmHcS
-----END PRIVATE KEY-----
```

Once you have created a JWT certificate, you can select it in your application settings:

Edit Application [Save](#) [Save & Exit](#)

Name ? :	app-built-in
Display name ? :	Casdoor
Logo ? :	URL: https://cdn.casbin.com/logo/logo_1024x256.png
	
Home ? :	https://casdoor.org
Description ? :	
Organization ? :	built-in
Client ID ? :	c2ab05e8460fd3ff9ddc
Client secret ? :	c9199f102508f089d253638f1a72b4c3e926d05
Cert ? :	cert-built-in (highlighted)
Redirect URLs ? :	cert_rjeqc cert-built-in Redirect URL

Action

SAML Certificates

SAML certificates are used for signing and encrypting SAML assertions in Single Sign-On (SSO) integrations.

Use cases:

- SAML-based SSO integrations
- Signing SAML responses
- Encrypting SAML assertions for security

When configuring SAML, you need to create certificates for both the Identity Provider (IdP) and Service Provider (SP) to ensure secure communication.

For more information about SAML configuration, see the [SAML documentation](#).

Payment Certificates

Payment certificates are used to secure payment transactions with payment providers like Alipay and WeChat Pay.

Use cases:

- Securing API communications with payment gateways
- Signing payment requests
- Verifying payment callbacks

For example, when integrating with Alipay, you need to create certificates for:

- App Cert: Contains the application's public certificate and private key
- Root Cert: Contains the payment provider's certificates

For more details, refer to the [Alipay Payment Provider](#) and [WeChat Pay Provider](#) documentation.

Creating a Certificate

To create a new certificate in Casdoor:

1. Navigate to the Certs page in the Casdoor admin console
 2. Click the Add button to create a new certificate
 3. Fill in the required fields:
 - Name: A unique identifier for the certificate
 - Display Name: A human-readable name
 - Scope: Select the appropriate scope (JWT, SAML, Payment)
 - Type: Select the certificate type
 - Crypto Algorithm: Choose the cryptographic algorithm (e.g., RS256 for JWT)
 - Bit Size: Set the key size (typically 2048 or 4096 bits)
 - Expire In Years: Set the expiration period

4. You can either:
 - Generate a new certificate automatically by saving the form
 - Upload an existing certificate and private key

Using Certificates

In Applications

After creating a JWT certificate, you need to associate it with your application:

1. Go to the Applications page
2. Edit your application
3. In the Cert field, select the certificate you created
4. Save the application

The certificate will now be used to sign all tokens issued by that application.

In SDK Configuration

When configuring Casdoor SDK in your backend application, you need to provide the public key from the JWT certificate:

```
var CasdoorEndpoint = "https://door.casdoor.com"
var ClientId = "541738959670d221d59d"
var ClientSecret = "66863369a64a5863827cf949bab70ed560ba24bf"
var CasdoorOrganization = "casbin"
var CasdoorApplication = "app-casnoded

//go:embed token_jwt_key.pem
var JwtPublicKey string
```

You can download the public key from the certificate edit page in Casdoor.

For more information about SDK configuration, see the [SDK documentation](#).

In Payment Providers

When setting up payment providers, you need to configure the appropriate certificates:

1. Create the required certificates (e.g., App Cert and Root Cert for Alipay)
2. Go to the Providers page
3. Edit or create your payment provider
4. In the Cert field, select the certificate you created
5. Save the provider

Best Practices

- **Key Size:** Use at least 2048-bit keys for RSA certificates. For higher security, consider 4096-bit keys.
- **Expiration:** Set appropriate expiration periods. For production environments, 1-5 years is typical.
- **Security:** Keep private keys secure and never expose them in client-side code or public repositories.
- **Rotation:** Regularly rotate certificates before they expire to maintain security.
- **Backup:** Keep secure backups of your certificates and private keys.
- **Separate Certificates:** Use different certificates for different purposes (JWT, SAML, Payment) to limit the impact of potential key compromise.

Certificate Management

You can manage certificates through:

- **Web UI:** The Casdoor admin console provides a user-friendly interface for certificate management
- **API:** Use the [Casdoor REST API](#) to programmatically manage certificates
- **Data Initialization:** Certificates can be included in initialization files for automated deployments

For more information about data initialization, see the [Data Initialization documentation](#).



>

令牌

令牌



概述

Casdoor令牌简介

概述

Casdoor是基于OAuth构建的，并使用令牌作为用户的OAuth令牌。

Access Token and ID Token

In Casdoor, the `access_token` and `id_token` are identical. Both tokens contain the same JWT payload with user information and claims. This is a design choice in Casdoor that simplifies token management.

This approach means:

- Both tokens contain the same user information and custom claims
- Both tokens can be used interchangeably for authentication and authorization
- The token format and expiration settings apply to both tokens equally
- You cannot configure separate claims for `access_token` and `id_token`

Token Fields

以下是Casdoor中可用的令牌字段：

- `Owner`
- `Name`
- `CreatedTime`
- `Application`
- `Organization`

- `User`
- `Code`
- `AccessToken`
- `ExpireIn` (令牌将在几小时后过期)
- `Scope` (授权范围)
- `TokenType` (例如, `Bearer` 类型)

登录应用程序后，有三种生成JWT令牌的选项：

- `JWT`
- `JWT-Empty`
- `JWT-Custom`
- `JWT-Standard`

选项如下：JWT将生成一个包含所有用户字段的令牌，JWT-Empty将生成一个包含用户所有非空值的令牌，而JWT-Custom将生成一个包含自定义用户令牌字段的令牌（您可以在令牌字段中选择属性）。JWT-Standard will generate a token with some standard OIDC token fields include email, phone, gender and Address (Address value in other format is not standard).

Token format ②: `JWT-Custom`

Token fields ②:

- `Owner`
- `CreatedTime`
- `DisplayName`
- `UpdatedTime`
- `Owner`
- `Name`
- `CreatedTime`
- `UpdatedTime`
- `Id`
- `Type`
- `Password`
- `PasswordSalt`

Token expire ②:

Refresh token expire ②:

Failed signin limit ②:

Failed signin frozen time ②:



>

Webhooks

Webhooks



Webhooks Overview

Configuring Webhooks in Casdoor

Webhooks Overview

概述

Casdoor provides an event-driven system that allows you to integrate with external applications using webhooks. Webhooks enable real-time communication by sending HTTP `POST` requests with a JSON payload to a configured endpoint whenever a specified event occurs. This allows your application to react to Casdoor events such as user sign-ups, logins, logouts, and profile updates.

How Webhooks Work

When an event is triggered in Casdoor:

1. Casdoor sends a `POST` request to the specified webhook URL.
2. The request contains a JSON payload with event details.
3. Your application processes the payload and executes relevant actions based on the event type.

Supported Events

Casdoor webhooks support various user-related events, which are stored in the `action` field of the request payload.

Event	Description
<code>signup</code>	Triggered when a user signs up
<code>login</code>	Triggered when a user logs in
<code>logout</code>	Triggered when a user logs out
<code>update</code>	Triggered when user details are updated

Setting Up a Webhook

To configure a webhook in Casdoor:

1. Navigate to the Casdoor Webhooks Section:

- Open your Casdoor instance.
- Go to **Settings > Webhooks**.

2. Create a New Webhook:

- Click on **Add Webhook**.
- Enter the **Webhook URL** where Casdoor should send event data.
- Select the events you want to listen to (e.g., `signup`, `login`).
- (Optional) Add custom headers for authentication.

3. Save the Webhook Configuration:

- Once saved, Casdoor will start sending event notifications to the specified endpoint.

Example Webhook Payload

Here's an example of a JSON payload sent to your webhook when a user logs in:

```
{  
  "event": "login",  
  "timestamp": 1709452800,  
  "user": {  
    "id": "12345",  
    "username": "johndoe",  
    "email": "johndoe@example.com"  
  }  
}
```

Your application should parse this payload and perform necessary actions, such as logging the event or notifying another service.

Testing Your Webhook

Before deploying your webhook integration, you can test it using tools like:

- [Beeceptor](#) – Allows you to create a custom webhook URL and inspect incoming requests.
- [Webhook.site](#) – Provides an instant webhook endpoint for testing.

Example Test with Beeceptor

1. Visit [Beeceptor](#) and create a new endpoint.
2. Copy the generated webhook URL and configure it in Casdoor.
3. Trigger a test event (e.g., log in to Casdoor).

4. Check Beeceptor's dashboard to inspect the received request.

Handling Webhooks in Your Application

Your server should be able to process incoming webhook requests. Below is a simple example in Node.js:

```
const express = require('express');
const app = express();

app.use(express.json());

app.post('/webhook', (req, res) => {
  console.log('Received webhook:', req.body);
  res.status(200).send('Webhook received');
});

app.listen(3000, () => console.log('Server running on port 3000'));
```

Conclusion

Casdoor webhooks provide a powerful way to integrate with external applications by enabling event-driven interactions. Whether you need to sync user data, trigger notifications, or update external systems, webhooks allow seamless automation.

To ensure a smooth integration, always validate incoming requests and test your webhooks with tools like Beeceptor or Webhook.site before deploying them in production.



>

LDAP

LDAP

概述

Casdoor与LDAP服务器合作

配置和同步LDAP用户

在Casdoor中配置LDAP以进行用户同步

LDAP 服务器

如何在Casdoor中连接LDAP客户端

概述

Casdoor已经引入了对LDAP服务器的支持。 Casdoor能够将用户从LDAP服务器同步到Casdoor，以便将它们用作登录的用户账户，并使用LDAP服务器对它们进行身份验证。 Casdoor还支持设置定时任务，以定期自动同步用户。

关于Casdoor-LDAP同步机制的详细信息

Casdoor如何与LDAP服务器合作的方式如下所述：

1. 同步：Casdoor可以连接到LDAP服务器，获取用户信息，并读取所有用户信息（包括`uidNumber`、`uid`、`cn`、`gidNumber`、`mail`、`email`、`emailAddress`、`telephoneNumber`、`mobile`、`mobileTelephoneNumber`、`registeredAddress`、`postalAddress`）。然后，它会为LDAP中的每个用户创建Casdoor账户，并将这些账户存储在数据库中。
2. 身份验证：正如我们所看到的，Casdoor并不获取LDAP用户的密码。当一个从LDAP服务器同步的账户试图通过Casdoor登录时，Casdoor不会检查存储在其数据库中的密码，而是连接到LDAP服务器并验证用户的密码是否正确。
3. 用户识别：Casdoor使用`uid`来唯一识别用户。因此，请确保每个LDAP用户都有一个唯一的`uid`。

一旦用户被同步到Casdoor中，他们的信息就会与LDAP用户独立开来。这意味着，如果你在Casdoor中修改了用户的信息，LDAP中的用户信息将不会被修改，反之亦然（除了LDAP用户的密码，因为我们依赖它来验证用户）。

配置和同步LDAP用户

LDAP配置因每个组织而异，因为LDAP用户将被同步到这些组织中。

要修改配置，您需要使用全局管理员用户。在“组织”页面上输入以下信息进行LDAP用户同步。

LDAPs						
Server name	Server	Base DN	Auto Sync	Last Sync	Action	
Example LDAP Server	example.com:389	ou=People,dc=example,dc=com	Disable		<button>Sync</button>	<button>Edit</button> <button>Delete</button>

配置连接到LDAP服务器

Edit LDAP Save Save & Exit Sync LDAP

Organization : built-in

ID : 691edec0-f1ab-4e23-8f9f-a824a383032f

Server name : Example LDAP Server

Server host : example.com

Server port : 389

Enable SSL :

Base DN : ou=built-in,dc=example,dc=com

Search Filter : (objectClass=posixAccount)

Filter fields : uid Email

Admin : cn=admin,dc=example,dc=com

Admin Password :

Auto Sync : 0 mins

服务器名称

管理者可以用来识别不同服务器的友好名称。

Example: Example LDAP Server

服务器主机

LDAP服务器的主机名或IP地址。

Example: example.com

服务器端口

LDAP服务器的端口号。 只允许数字值。

Example: 389

基础 DN

Casdoor在LDAP中搜索时默认使用Sub搜索模式。 Base DN是用于搜索的基本可分辨名称。 Casdoor将返回指定Base DN下的所有用户。

在Casdoor中配置的管理员账户应至少具有对基础DN的只读权限。

Example: ou=Example,dc=example,dc=com

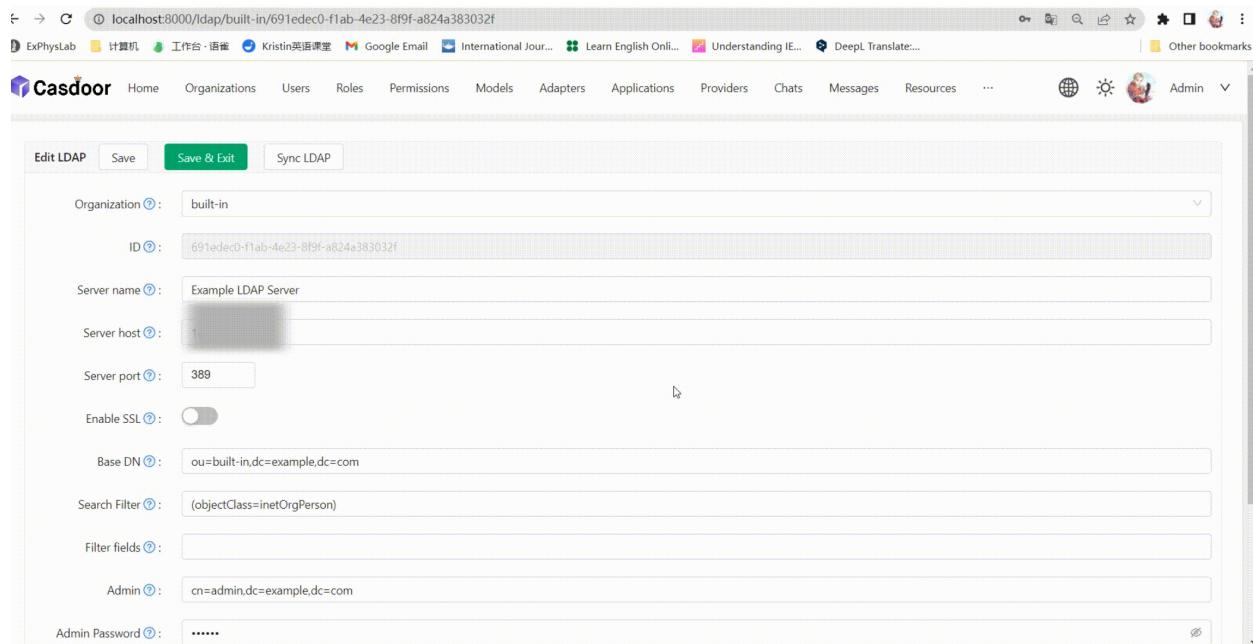
搜索过滤器

Casdoor使用搜索过滤器来查询LDAP用户。

Example: (objectClass=posixAccount)

过滤字段

过滤字段是用户在LDAP服务器中的标识符。当以LDAP用户身份登录Casdoor时，输入的登录用户名被视为LDAP用户的uid。您也可以配置其他字段，例如mail或mobile。



The screenshot shows the 'Edit LDAP' configuration page in Casdoor. The 'Save & Exit' button is highlighted. The configuration fields include:

- Organization: built-in
- ID: 691edec0-f1ab-4e23-8f9f-a824a383032f
- Server name: Example LDAP Server
- Server host: 127.0.0.1
- Server port: 389
- Enable SSL: Off
- Base DN: ou=built-in,dc=example,dc=com
- Search Filter: (objectClass=inetOrgPerson)
- Filter fields: (empty)
- Admin: cn=admin,dc=example,dc=com
- Admin Password: (redacted)

管理员

可以登录到指定LDAP服务器的账户。

登录方法（DN或ID）取决于您想要连接的LDAP服务器的设置。

Example: cn=manager, dc=example, dc=com

管理员密码

LDAP服务器管理员账户的密码。

自动同步

设置为0以禁用自动同步。任何其他值表示每隔几分钟同步一次。

同步用户

同步表显示了在特定的ou中从LDAP服务器获取的所有用户。如果用户已经被同步，复选框将被禁用。您可以通过勾选框来选择用户，然后从LDAP服务器同步所选用户。

	CN	UidNumber / Uid	Group Id	Email	Phone	Address
<input type="checkbox"/>	zhan san	1000 / zsan	500			
<input type="checkbox"/>	li si	1001 / lsi	500			
<input type="checkbox"/>	a dmin	1002 / admin	500			
<input type="checkbox"/>	tom brown	1007 / jery	500			
<input type="checkbox"/>	wrie jerry	1003 / wjerry	500			
<input type="checkbox"/>	admin2	1004 / admin2	500			
<input type="checkbox"/>	yyyy	1005 / yyyy	500			

Default group

Group to which users belong after synchronization.

⚠ 注意事项

如果LDAP服务器中的用户的uid与Casdoor组织中现有用户的name相同，Casdoor将创建一个新用户，其name包含uid和一个随机字符串。然而，由于新同步的用户名在LDAP服务器中不存在，此用户可能无法登录。因此，建议避免这种情况。

LDAP 服务器

许多系统，如 [Nexus](#)，支持LDAP认证。 Casdoor也实现了一个简单的LDAP服务器， 支持绑定和搜索操作。

本文档描述了如何连接到Casdoor中的LDAP服务器并实现简单的登录认证。

LDAP 服务器端口号

LDAP服务器默认监听 [389](#) 端口。 You can change the default port by modifying the `ldapServerPort` value in [conf/app.conf](#).

工作原理

与Casdoor中的LDAP客户端类似， LDAP服务器中的用户都是 `posixAccount` 的子类。

当服务器接收到LDAP传输的一组数据时， 它将解析 `cn` 和 `ou`， 其中 `cn` 代表用户名， `ou` 代表组织名称。 `dc` 并不重要。

如果是绑定操作， 服务器将使用Casdoor来验证用户名和密码，并在Casdoor中授予用户权限。

如果是搜索操作， 服务器将根据绑定操作授予客户端的权限， 检查搜索操作是否合法，并返回响应。

① 信息

我们只支持简单认证。

如何绑定

在Casdoor LDAP服务器中，我们只认可类似于这种格式的DN：`cn=admin,ou=built-in,dc=example,dc=com`。

请将管理员用户的DN设置为上述格式。然后，您可以使用这个DN和用户的密码绑定到LDAP服务器，以登录到Casdoor进行验证。如果服务器验证成功，用户将在Casdoor中被授予权限。

如何搜索

一旦绑定操作成功完成，您就可以进行搜索操作。搜索和绑定操作之间存在一些差异。

- To search for a certain user, such as Alice under the built-in organization, you should use a DN like this: `ou=built-in,dc=example,dc=com`, and add `cn=Alice` in the Filter field.
- To search for all users under a certain organization, such as all users in `built-in`, you should use a DN like this: `ou=built-in,dc=example,dc=com`, and add `cn=*` in the Filter field.
- To search for all users in all organizations (assuming the user has sufficient permissions), you should use a DN like this: `ou=*,dc=example,dc=com`, and add `cn=*` in the Filter field.
- To search for all users in a specific group, you should use a filter query like this: `(memberOf=organization_name/group_name)` in the Filter field.

Supported RFC-Style Features

Partial Root DSE Query Support

The Root DSE (`baseDN=""`) provides directory capabilities.

- Query namingContexts (organization list): `ldapsearch -x -H ldap://<casdoor-host>:389 -D "cn=admin,ou=built-in" -w <passwd> -b "" -s base "(objectClass=*)" namingContexts`
Returns visible organization DNs.
- Query subschemaSubentry: `ldapsearch -x -H ldap://<casdoor-host>:389 -D "cn=admin,ou=built-in" -w <passwd> -b "" -s base "(objectClass=*)" subschemaSubentry`
Returns `subschemaSubentry: cn=Subschema`.

Schema Query Support

Query objectClasses: `ldapsearch -x -H ldap://<casdoor-host>:389 -D "cn=admin,ou=built-in" -w <passwd> -b "cn=Subschema" -s base "(objectClass=*)" objectClasses`

Returns definitions for posixAccount and posixGroup.

POSIX Filters

- `(objectClass=posixAccount)` returns user list.
- `(objectClass=posixGroup)` returns group list under organization (e.g.,
`ldapsearch -x -H ldap://<casdoor-server>:389 -D "cn=admin,ou=built-in" -w <passwd> -b "ou=<org>" "(objectClass=posixGroup)"`).

Note: `(objectClass=posixGroup)` Does not support combined searches like `(&(objectClass=posixGroup)(cn=<group>))`. Please use `memberOf` for searching members in a group.



>

RADIUS

RADIUS

概述

将Casdoor用作RADIUS服务器

概述

您可以将Casdoor用作RADIUS服务器。 RADIUS是一个客户端/服务器协议，客户端可以是NAS或运行RADIUS客户端软件的任何计算机。

Congiure

在部署Casdoor之前，您需要修改`conf/app.conf`文件中的RADIUS相关配置，包括服务器端口和密钥：

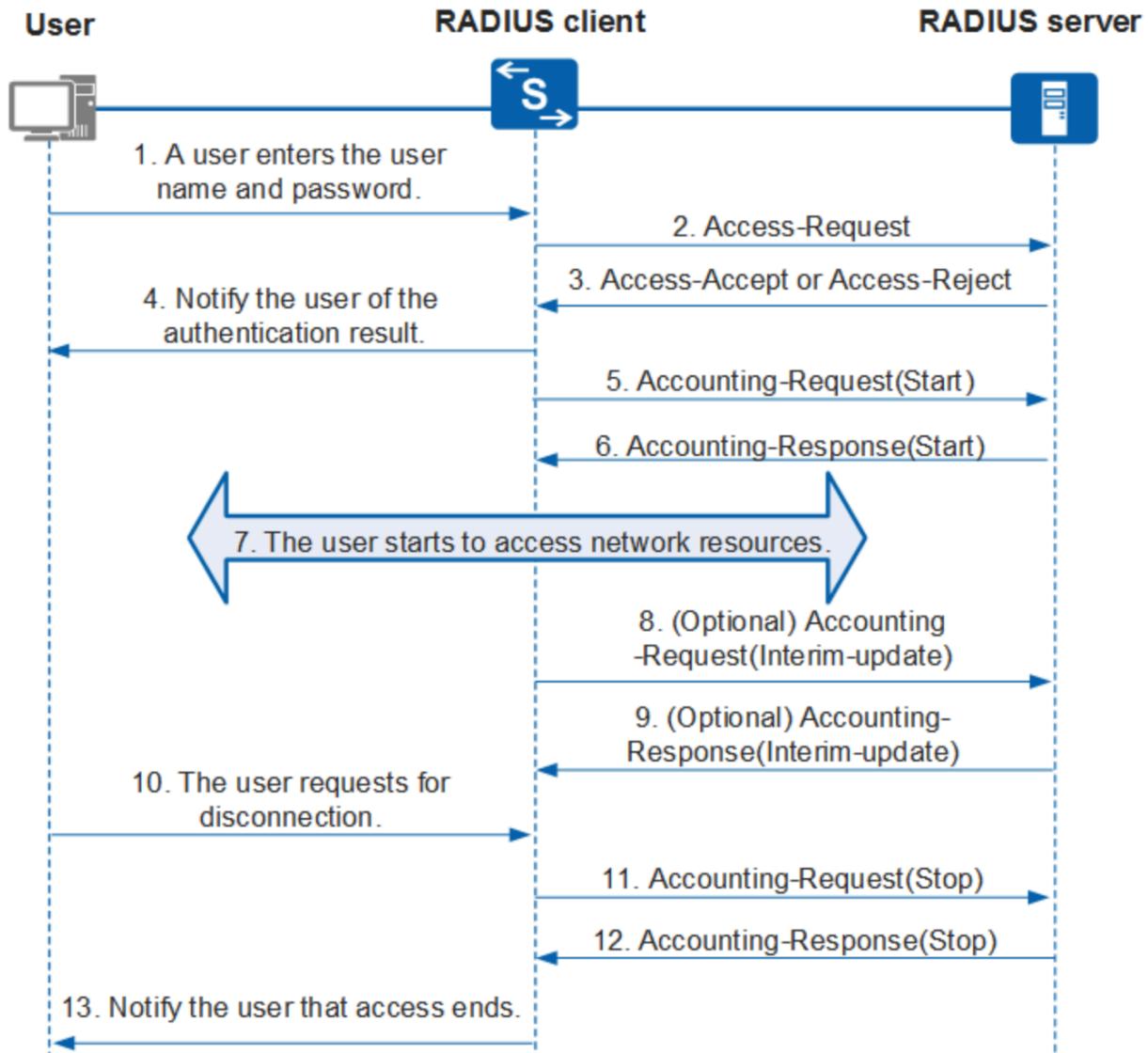
```
radiusServerPort = 1812  
radiusSecret = "secret"
```

现在您可以将Casdoor用作RADIUS服务器。

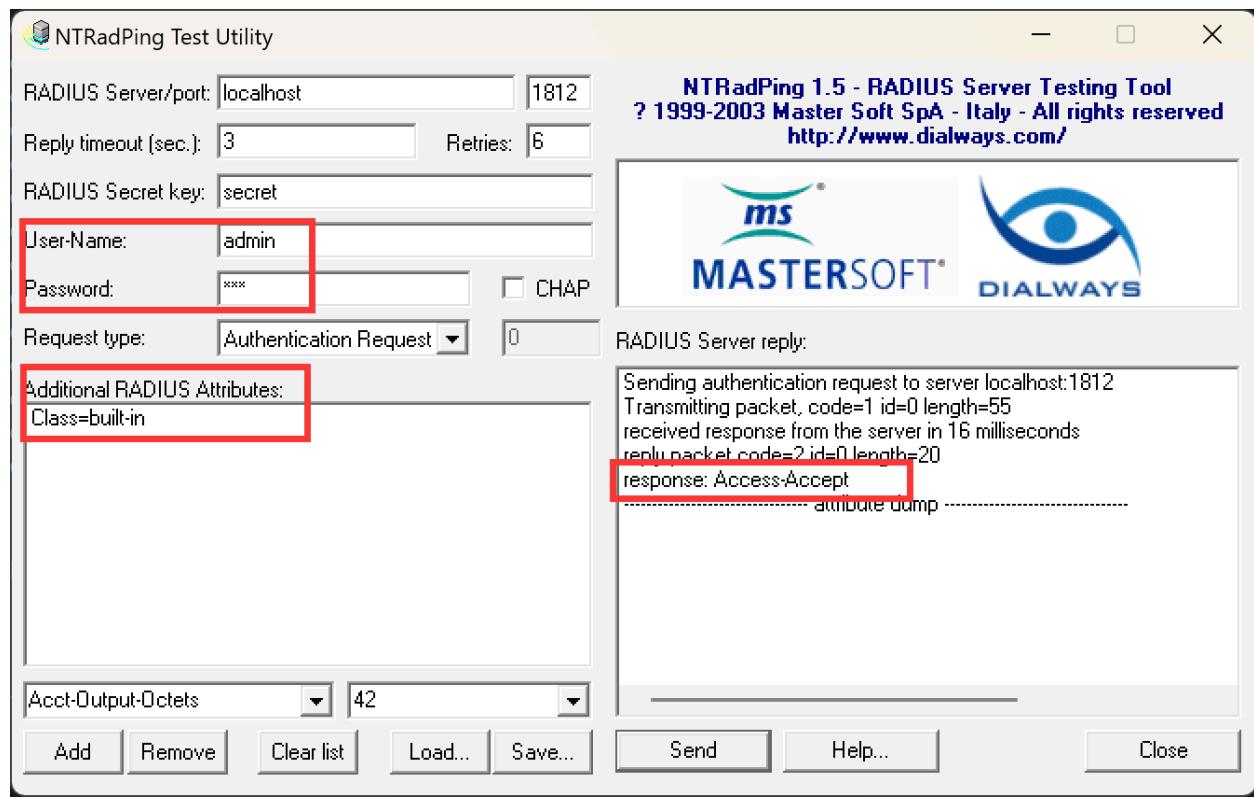
将Casdoor用作RADIUS服务器

Casdoor目前可以支持以下标准RADIUS请求：

- `Access-Request`：认证请求消息由RADIUS客户端发送给Casdoor。 Casdoor根据消息中携带的用户信息决定是否允许访问，并回复`Access-Reject`或`Access-Accept`。
- `Accounting-Request`：当用户开始或停止访问网络资源时，RADIUS客户端将发送记账请求（开始/中间更新/停止）消息给Casdoor。 Casdoor将记录相关的记账请求消息，并回复`Accounting-Response`。



由于Casdoor使用组织来管理用户，每个用户都属于特定的组织，因此请求中的 class 属性需要设置为用户的组织。





>

SCIM

SCIM

概述

将Casdoor用作SCIM服务提供商

概述

SCIM协议是一种基于HTTP的协议，用于通过SCIM模式指定的身份数据的配置和管理。您可以将Casdoor用作SCIM服务提供商。

将Casdoor用作SCIM服务提供商

目前Casdoor只支持User Resource Schema，您可以通过SCIM用户操作来管理用户。您可以通过以下端点与Casdoor进行交互：

端点	方法	描述
/scim/ ServiceProviderConfig	GET	提供关于支持的SCIM标准的特性的详细信息，例如，支持的资源。
/scim/Schemas	GET	提供有关服务提供商模式的详细信息。
/scim/ResourceTypes	GET	指定每个资源的元数据。
/scim/Users/:id	GET	使用资源标识符 id 检索用户。
/scim/Users	GET	使用查询参数查询用户（目前只支持 startIndex 和 count）。
/scim/Users	POST	创建用户。
/scim/Users/:id	PUT	使用资源标识符 id 更新用户。

端点	方法	描述
/scim/Users/:id	PATCH	通过PATCH操作使用资源标识符 <code>id</code> 修改用户。
/scim/Users/:id	DEL	删除具有资源标识符 <code>id</code> 的用户。

有关更多详细信息, 请参阅[rfc7644](#)。

用户资源

Casdoor实现了User Resource Schema (SCIM) 和User (Casdoor) 之间的映射。属性之间的映射关系如下:

用户资源模式 (SCIM)	用户 (Casdoor)
<code>id</code>	<code>Id</code>
<code>meta.created</code>	<code>CreatedTime</code>
<code>meta.lastModified</code>	<code>UpdatedTime</code>
<code>meta.version</code>	<code>UpdatedTime</code>
<code>externalId</code>	<code>ExternalId</code>
<code>userName</code>	<code>Name</code>
<code>password</code>	<code>Password</code>

用户资源模式 (SCIM)	用户 (Casdoor)
displayName	DisplayName
profileUrl	Homepage
userType	Type
name.givenName	FirstName
name.familyName	LastName
emails[0].value	Email
phoneNumbers[0].value	Phone
photos[0].value	Avatar
addresses[0].locality	Location
addresses[0].region	Region
addresses[0].country	CountryCode

由于Casdoor使用组织来管理用户，每个用户都属于特定的组织，所以应该在 `Enterprise User Schema Extension` (由模式URI `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User` 标识) 中传递 `organization` 属性。以下是用户资源模式SCIM在JSON格式中的表示：

```
{
  "active": true,
```




>

集成

集成



3 个项目



1 个项目



10 个项目



17 个项目



JavaScript

2 个项目



Lua

1 个项目



PHP

6 个项目



Ruby

1 个项目



Haskell

1 个项目



Python

1 个项目



> 集成 >

C++

C++

Nginx

使用Casdoor与Nginx

NginxCommunityVersion

使用Casdoor、Nginx（非Nginx-Plus）和Oauth2-Proxy

Envoy

在Envoy中使用Casdoor

Nginx

使用Casdoor作为身份提供者（IdP）为NGINX Plus代理的应用程序启用基于OpenID Connect的单点登录。

本指南解释了如何为NGINX Plus代理的应用程序启用单点登录（SSO）。该解决方案使用OpenID Connect作为身份验证机制，以Casdoor作为身份提供者（IdP），以及NGINX Plus作为依赖方。

另见：您可以在项目的GitHub仓库中找到有关NGINX Plus OpenID Connect集成的更多信息。

先决条件

说明假定您具有以下内容：

- 一个正在运行的Casdoor服务器。请参阅Casdoor文档中的[服务器安装和使用Docker尝试](#)。
- 一个NGINX Plus订阅和NGINX Plus R15或更高版本。有关安装说明，请参阅[NGINX Plus管理员指南](#)。
- [NGINX JavaScript模块](#)，用于处理NGINX Plus和IdP之间的交互。安装NGINX Plus后，使用适合您的操作系统的命令安装模块。

对于Debian和Ubuntu：

```
sudo apt install nginx-plus-module-njs
```

对于CentOS, RHEL和Oracle Linux:

```
sudo yum install nginx-plus-module-njs
```

- 以下指令应包含在顶级（“主”）配置上下文中的`/etc/nginx/nginx.conf`中，以便加载NGINX JavaScript模块：

```
load_module modules/ngx_http_js_module.so;
```

配置Casdoor

注意：以下过程反映了出版时的Casdoor GUI，但GUI可能会发生变化。使用此指南作为参考，并根据当前的Casdoor GUI进行调整。

要在Casdoor GUI中为NGINX Plus创建一个Casdoor客户端，请按照以下步骤操作：

- 在<http://your-casdoor-url.com/login>登录您的Casdoor帐户。
- 在顶部导航栏中，点击应用程序。在打开的应用程序页面上，点击左上角的添加按钮。



- 在打开的编辑应用程序页面上，将名称和显示名称字段的值更改为您要启用SSO的应用程序的名称。在这里，我们使用的是NGINX Plus。

Name  :	NGINX Plus
Display name  :	NGINX Plus

在重定向URL字段中，输入NGINX Plus实例的URL，包括端口号，并以/_codexch结尾（在本指南中，它是https://your-site-url.com:443/_codexch）。

Redirect URLs  :	Redirect URLs 
Redirect URL	
 https://my-nginx.example.com:443/_codexch	

注意：

- 对于生产环境，我们强烈建议您使用SSL/TLS（端口443）。
- 即使您使用的是HTTP（80）或HTTPS（443）的默认端口，端口号也是必需的。

4. 记录客户端ID和客户端密钥字段中的值。您将在[配置NGINX Plus的步骤4](#)中将它们复制到NGINX Plus配置文件中。

Client ID [?](#) : 200c96d5ce5f33e0...
Client secret [?](#) 58f13a80b879e...
:

5. 点击顶部导航栏中的**角色**, 然后点击打开的页面左上角的**添加按钮**。



6. 在打开的添加页面上, 在**名称**和**显示名称**字段中输入一个值 (这里是nginx-casdoor-role) , 然后点击**保存按钮**。

Name [?](#) : nginx-casdoor-role
Display name [?](#) : nginx-casdoor-role

7. 在顶部导航栏中, 点击**用户**。在打开的**用户**页面上, 点击**编辑**编辑现有用户, 或者点击左上角的**添加按钮**创建新用户。

8. 在打开的添加页面上, 根据您的喜好修改**名称**和**显示名称** (这里是user1) 。

Name  : user1

Display name user1

 :

在注册应用程序中选择NGINX Plus。

Signup application  : NGINX Plus

在管理帐户字段中，选择应用程序中的NGINX Plus，并填写用户名和密码。

Managed accounts  :		Add
Application	Username	Password
NGINX Plus	<input type="text"/>	<input type="password"/>

9. 返回到角色页面，点击nginx-casdoor-role行上的编辑。在打开的页面中，在子用户字段中，选择您刚刚创建的用户名（这里是built-in/user1）。

Sub users  : built-in/user1 

配置NGINX Plus

要配置NGINX Plus作为OpenID Connect依赖方，请按照以下步骤操作：

- 首先，创建[nginx-openid-connect](#) GitHub仓库的克隆：

```
git clone https://github.com/nginxinc/nginx-openid-connect
```

- 将克隆中的以下文件复制到`/etc/nginx/conf.d`目录：

- `frontend.conf`
- `openid_connect.js`
- `openid_connect.server_conf`
- `openid_connect_configuration.conf`

- 从Casdoor配置中获取授权端点、令牌端点和JSON Web Key（JWK）文件的URL。打开终端并执行以下`curl`命令，将输出管道到指定的`python`命令以生成可读的配置格式。为了简洁，我们已经截断了输出，只显示相关字段。

```
curl http://<casdoor-server-address>/.well-known/openid-configuration | python -m json.tool
{
    "authorization_endpoint": "https://<casdoor-server-address>/login/oauth/authorize",
    "...": "...",
    "token_endpoint": "http://<casdoor-server-address>/api/login/oauth/access_token",
    "...": "...",
    "jwks_uri": "http://<casdoor-server-address>/.well-known/jwks",
    "...": "...",
```

4. 使用您喜欢的文本编辑器打开`/etc/nginx/conf.d/openid_connect_configuration.conf`。修改以下`map`指令的"default"参数值为指定的值：

- `map $host $oidc_authz_endpoint` - 使用**步骤3**中的`authorization_endpoint`的值（在本指南中，`https://<casdoor-server-address>/login/oauth/authorize`）
- `map $host $oidc_token_endpoint` - 使用**步骤3**中的`token_endpoint`的值（在本指南中，`http://<casdoor-server-address>/api/login/oauth/access_token`）
- `map $host $oidc_client` - 使用**配置Casdoor的步骤4**中**客户端ID**字段的值
- `map $host $oidc_client_secret` - 使用**配置Casdoor的步骤2**中**客户端密钥**字段的值
- `map $host $oidc_hmac_key` - 使用一个独特的，长的，安全的短语

5. 根据使用的NGINX Plus版本配置JWK文件：

- 在NGINX Plus R17及更高版本中，NGINX Plus可以直接从**步骤3**中指定为`jwks_uri`的URL读取JWK文件。对`/etc/nginx/conf.d/frontend.conf`进行以下更改：
 - a. 注释掉（或删除）`auth_jwt_key_file`指令。
 - b. 取消注释`auth_jwt_key_request`指令。（参数`/_jwks_uri`引用了`$oidc_jwt_keyfile`变量的值，该值将在下一步中设置。）
 - c. 将`map $host $oidc_jwt_keyfile`指令的"default"参数更新为**步骤3**中`jwks_uri`字段的值（在本指南中，`http://<casdoor-server-address>/.well-known/jwks`）。
- 在NGINX Plus R16及更早版本中，或者如果您喜欢，JWK文件必须位于本地磁盘上。按照以下步骤操作：
 - a. 将**步骤3**中`jwks_uri`字段指定的JWK文件的JSON内容复制到本地文件（例如，`/etc/nginx/my_casdoor_jwk.json`）。

- b. 在/etc/nginx/conf.d/openid_connect_configuration.conf中，将`map $host $oidc_jwt_keyfile`指令的"default"参数更改为本地文件的路径。
6. 确保在NGINX Plus配置文件（通常是/etc/nginx/nginx.conf）中指定的user指令的用户具有读取JWK文件的权限。

测试

打开浏览器并输入您的NGINX Plus实例的地址。然后，尝试使用被分配了NGINX Plus角色的用户的凭据登录。



Casdoor



username, Email or phone



Password



Auto sign in

[Forgot password?](#)

Sign In

No account? [sign up now](#)

故障排除

请参阅GitHub上nginx-openid-connect仓库中的[故障排除](#)部分。

NginxCommunityVersion

先决条件

本指南假设您具有以下条件：

- 正在运行的Casdoor服务。如果您还没有安装Casdoor服务，请参考[服务器安装](#)或者[使用Docker试用](#)。
- 在编译时启用了`ngx_http_auth_request_module`模块的Nginx开源版。如果你不知道如何启用`ngx_http_auth_request_module`模块，请参考[Nginx模块文档](#)。
- 您希望启用身份验证的网站已成功部署在Nginx上，具有[配置的域名](#)（而不是使用IP地址），并且可以正常访问。
- OAuth2-Proxy工具（目前，GitHub上有以下两个高星级的热门项目可供选择，您需要选择其中之一）：
 - oauth2-proxy/oauth2-proxy（本文中使用）[GitHub](#) 或 [官方网站](#)
 - vouch/vouch-proxy [GitHub](#)

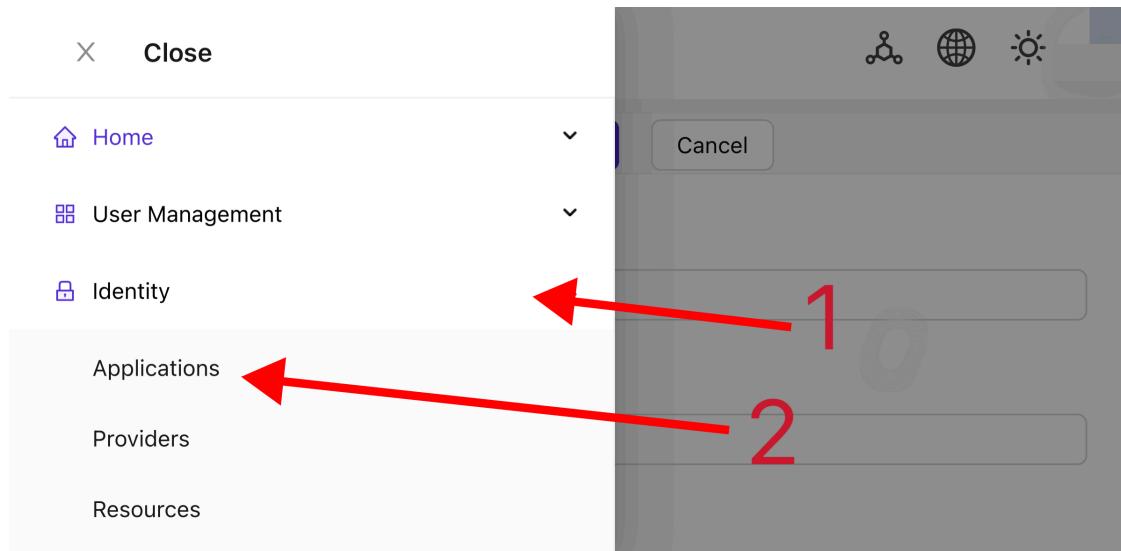
I. 配置CasDoor

注意：本文中的操作基于发布时的Casdoor GUI，但Casdoor GUI可能会根据版本变化。请按照本文中提供的参考配置您部署的Casdoor版本。

注意：本文中提到的密钥、密码、用户名和其他机密信息都是示例。出于安全原因，您在部署时必须用您自己的相关内容替换它们。

- 登录到您的Casdoor管理员账户。

2. 在顶部栏中，选择“身份验证” > “应用程序”，然后在“应用程序”页面上点击“添加”。



3. 根据您的项目信息完成应用程序配置。在本文中，我们使用“Nginx-Community”作为示例应用程序名称。

The screenshot shows the 'New Application' configuration form. At the top, it says 'New Application' with 'Save', 'Save & Exit', and 'Cancel' buttons. Below that, there are two input fields: 'Name' and 'Display name'. Both fields contain the value 'nginx-community'. Red arrows point from the text 'Set these value' to both of these input fields. The 'Name' field has a red arrow pointing to its left side, and the 'Display name' field has a red arrow pointing to its top-left corner. Below the input fields, there is a 'Logo' section with a blank input field and a horizontal line for a logo.

4. 记下“Client ID”和“Client Secret”字段的值。它们将在稍后配置OAuth2-Proxy时使用。然后将“Redirect URL”配置为 `https://project.yourdomain.com/oauth2/callback/`。

Client ID ② :
811a0b0

Client secret ② :
677ea728670 [REDACTED] ecae4eb09aa

Cert ② :
cert-built-in

Redirect URLs ② : Then, set this value to "https://project.yourdomain.com/oauth2/callback"

Redirect URLs	Action
Add	
Redirect URL	

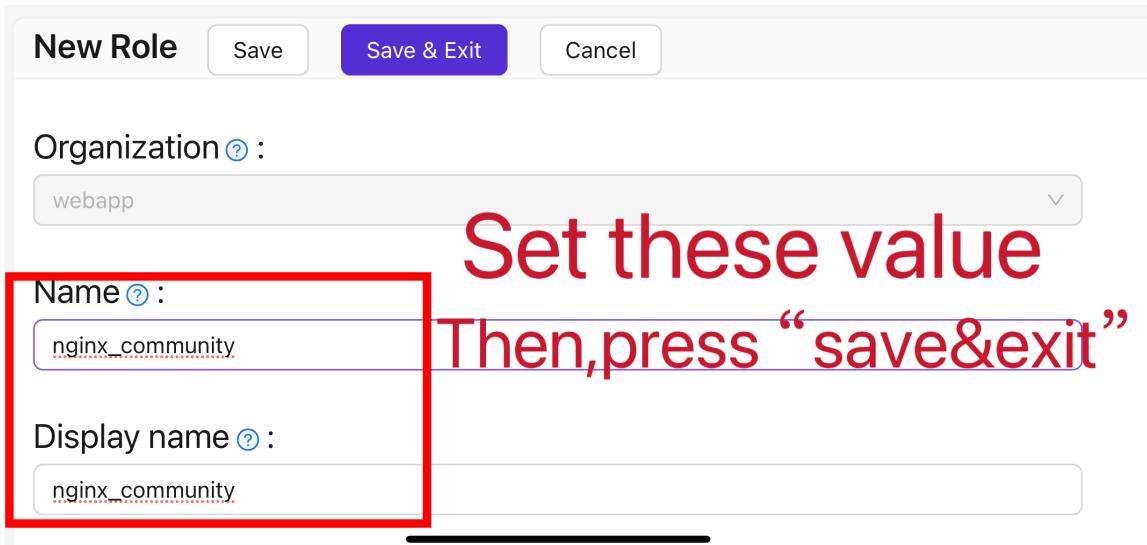
5. 在顶部栏中，选择"Casbin权限管理" > "角色"，然后在"角色"页面上点击"添加"。

Date	Display name	Sub users
14:32:48	New Role - jw3c7b	
21:07:09	管理员角色	1 / webapp/gzyzh

1 2 in total < 1 > 10 / page

2

6. 根据您的项目信息完成角色配置。在本文中，我们使用"nginx_role"作为示例角色名称。



7. (可选) 在顶部栏中, 选择"用户管理" > "用户", 然后根据您的需要添加新用户。如果您需要的用户已经存在, 您可以跳过此步骤。在本文中, 我们创建了一个名为"user"的示例用户。
8. 返回到步骤5中提到的"角色"页面, 编辑 `nginx_role` 角色, 并将您需要的用户添加到"包含的用户"选项中。在本文中, 我们在这里添加了之前创建的 `builtin/user`。

II. 配置Oauth2-Proxy

注意: 本文使用Oauth2-Proxy项目作为示例。如果你想使用Vouch代替Oauth2-Proxy, 请参考他们在[GitHub](#)上的官方文档。

注意: 本文假设您的网站配置了受信任的SSL证书并且只允许HTTPS访问, 或者您已经设置了从HTTP访问者自动重定向到HTTPS的设置。这有助于最大限度地保护cookies并防止恶意读取登录令牌。如果您的网站需要通过不安全的HTTP协议访问, 请相应地修改相关命令。关于通过HTTP部署的更多帮助, 请参考Oauth2-Proxy在[GitHub](#)上的官方文档。

提示：OAuth2-Proxy提供了各种部署方法（如源代码编译、Docker安装等）。为了便于解释，本文使用"预构建二进制文件"进行部署。

1. 转到[GitHub Releases](#)页面，下载与您的操作系统和CPU架构相对应的二进制包。

截至2024年1月1日，OAuth-Proxy的最新发布版本为v7.5.1。如果你想下载这个版本的二进制包，你可以执行以下命令，适用于AMD64的Linux：

```
wget -O oauth2-proxy-linux.tar.gz https://github.com/
oauth2-proxy/oauth2-proxy/releases/download/v7.5.1/
oauth2-proxy-v7.5.1.linux-amd64.tar.gz
```

强烈建议您在下载压缩包后检查官方网站在[GitHub Releases](#)页面提供的SHA256SUM值，并与您下载的包的SHA256SUM值逐个字符进行比较。

2. 解压下载的包：

```
tar -zxvf oauth2-proxy-*.tar.gz
```

3. 进入解压后的目录：

```
cd oauth2-proxy-v7.5.1.linux-amd64
```

4. 将获得的二进制文件移动到/usr/local/bin并配置执行权限。根据您的情况，您可能需要使用sudo提升权限。

```
cp ./oauth2-proxy /usr/local/bin
cd /usr/local/bin
chmod +x ./oauth2-proxy
```

5. 测试二进制安装。如果安装成功，执行以下命令后，您应该看到类似于

oauth2-proxy v7.5.1 (built with go1.21.1) 的输出。

```
cd ~  
oauth2-proxy --version
```

6. 使用命令行参数运行oauth2-proxy。标记为[required]的参数必须根据您的具体情况进行配置，而标记为[optional]的参数可以优化性能，但也可以省略。为确保oauth2-proxy可以在后台运行，您可以使用Screen或Supervisor等进程监控工具或终端工具。

```
oauth2-proxy \  
--provider=oidc \ #[required] 不要更改  
--client-id=abc123456def \ #[required] 上面步骤I.4中获得的"Client  
ID"  
--client-secret=abc123456def \ #[required] 上面步骤I.4中获得  
的"Client Secret"  
--oidc-issuer-url=https://auth.yourdomain.com \ #[required] 您的  
Casdoor URL (域名或公共IP)  
--redirect-url=https://project.yourdomain.com/oauth2/callback  
\ #[required] https://domain-of-the-project-to-protect/oauth2/  
callback  
--scope=email+profile+groups+openid \ #[required] 从Casdoor获  
得: 用户电子邮件, 用户配置文件, 组和登录认证  
--cookie-domain=project.yourdomain.com \ #[required] 您想要保护的  
项目的域名  
--whitelist-domain=project.yourdomain.com \ #[required] 您想要保  
护的项目的域名  
--cookie-secret=abc123456def \ #[required] 请生成一个随机的数字和字  
母字符串并在这里填写  
--email-domain=* \ #[required] 可接受的用户电子邮件域的列表 (*表示接  
受所有域)。如果用户的电子邮件后缀不在此列表中, 即使登录成功也会返回403错  
误。  
--insecure-oidc-allow-unverified-email=true \ #[required] 是否接  
受未验证电子邮件地址的用户
```

III. 配置Nginx

注意：请再次确认您的Nginx在编译和安装源代码时已启用
`ngx_http_auth_request_module` 模块（编译命令包括`--with-http_auth_request_module`）。如果你不知道如何启用
`ngx_http_auth_request_module` 模块，请参考[Nginx模块文档](#)。

提示：使用宝塔面板工具安装的Nginx默认不启用此模块。

1. 打开您已经部署并希望保护的网站的配置文件，并进行以下修改：

注意：您需要根据您的具体情况调整此配置文件。由于Nginx版本和其他因素，此配置文件可能无法在所有Nginx实例上顺利工作。请根据您自己的Nginx信息调整相关内容。

```
server {
    listen 443 ssl http2;

    include /path/to/ssl.conf;

    # 添加以下内容
    location ^~ /oauth2/ {
        proxy_pass          http://127.0.0.1:65534; # 将此更改为步骤
II.6中配置的"--http-address"

        proxy_set_header Host                      $host;
        proxy_set_header X-Real-IP                $remote_addr;
        proxy_set_header X-Scheme                 $scheme;

        proxy_set_header X-Auth-Request-Redirect $request_uri;
        # 或者，如果你正在处理多个域名：
        # proxy_set_header X-Auth-Request-Redirect
$scheme://$host$request_uri;
```

2. 保存文件并重新加载您的Nginx。

测试

- 接下来，您可以测试您的实现。
- 在正常情况下，您的用户在登录您的服务时将经历以下过程：
- 在浏览器中打开URL `project.yourdomain.com` → 只看到一个需要登录的页面，包括一个名为"Sign in with OpenID Connect"的按钮 → 点击按钮并被重定向到您的Casdoor地址，那里将要求他们登录 → 用户输入他们的用户名和密码，Casdoor验证他们的凭据 → 自动重定向回您的URL `project.yourdomain.com` → 成功访问您的服务 → 当您设置的 `--cookie-expire` 时间到期时，用户将被要求再次登录。

故障排除

- 如果您的项目没有按预期运行，请检查您的Nginx配置和Oauth2-Proxy配置参数是否正确。
- 您也可以参考Oauth2-Proxy在[GitHub](#)上的官方文档。
- 如果您发现本文档中有任何错误，请随时在[GitHub](#)上请求编辑。

Envoy

先决条件

正在运行的Casdoor服务器。请参考Casdoor文档中的[服务器安装](#)和[使用Docker试用](#)。

配置Casdoor

1. 添加**Envoy**应用程序。在**重定向URL**字段中，输入Envoy实例的URL，包括端口号，并以`/oauth2/callback`结束（例如，`http://%REQ(:authority%)/oauth2/callback`）。记下客户端ID和客户端密钥的值。
2. 添加**envoy-casdoor-role**角色。
3. 添加**user1**用户。在注册应用程序中选择**Envoy**。在**管理账户**字段中，从应用程序下拉菜单中选择**Envoy**，并填写用户名和密码。返回到**角色**页面，点击**envoy-casdoor-role**行上的“编辑”。在打开的页面中，**子用户**字段中，选择你刚刚创建的用户名（在这个例子中，它是**built-in/user1**）。

配置Envoy

1. 修改**envoy.yaml**文件中的`token_endpoint`、`authorization_endpoint`和`client_id`。
2. 将**token-secret.yaml**文件中的`inline_string`修改为Casdoor的Envoy客户端密钥。
3. 将**hmac-secret.yaml**文件中的`inline_bytes`修改为一个独特的、长的、安全的短语。
4. 将**envoy.yaml**、**token-secret.yaml**和**hmac-secret.yaml**文件添加到你的Envoy路

径中。

如何运行

1. 使用`envoy.yaml`文件启动Envoy。
2. 访问Envoy正在监听的网站。你应该立即被重定向到Casdoor进行用户身份验证。

C#

Unity

使用Casdoor-dotnet-sdk进行Unity开发。

Unity

步骤1：部署Casdoor

首先，应部署Casdoor。

您可以参考Casdoor官方文档中的[服务器安装](#)。请在**生产模式**下部署您的Casdoor实例。

成功部署后，请确保：

- 打开您喜欢的浏览器并访问<http://localhost:8000>，您将看到Casdoor的登录页面。
- 输入 `admin` 和 `123` 来测试登录功能。

或者，您可以使用[Casdoor官方演示站](#)进行快速开始。

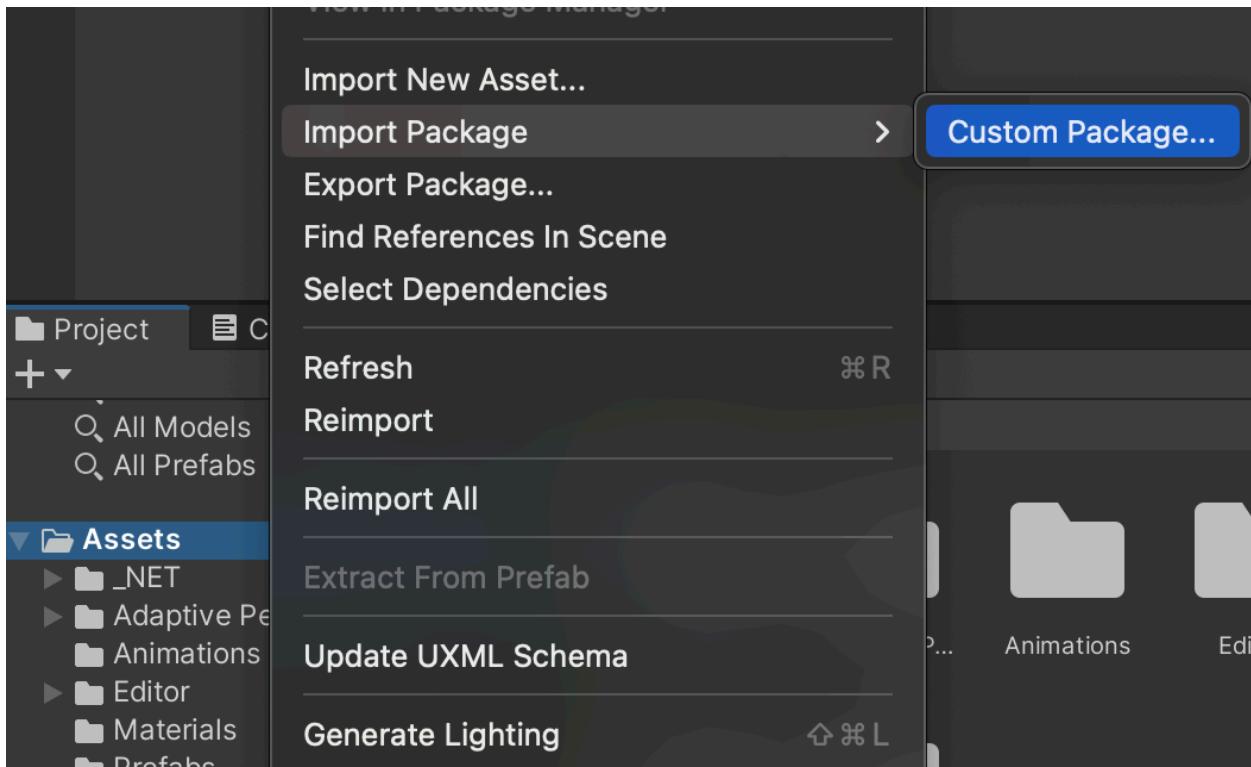
步骤2：导入Casdoor.Client

在[Casdoor-dotnet-sdk](#)中为 `.NET` 导入 [Casdoor.Client](#)。

一种可选的方法如下：

- `git@github.com:casdoor/casdoor-dotnet-sdk.git`
- 在Sample文件夹中运行ConsoleApp。
- 获取 `/casdoor-dotnet-sdk/src/Casdoor.Client/bin/Debug/net462` 文件夹。

现在，您可以通过下图所示的方法将 `net462` 文件夹导入到您的Unity项目中。当然，您也可以选择其他版本的文件夹。

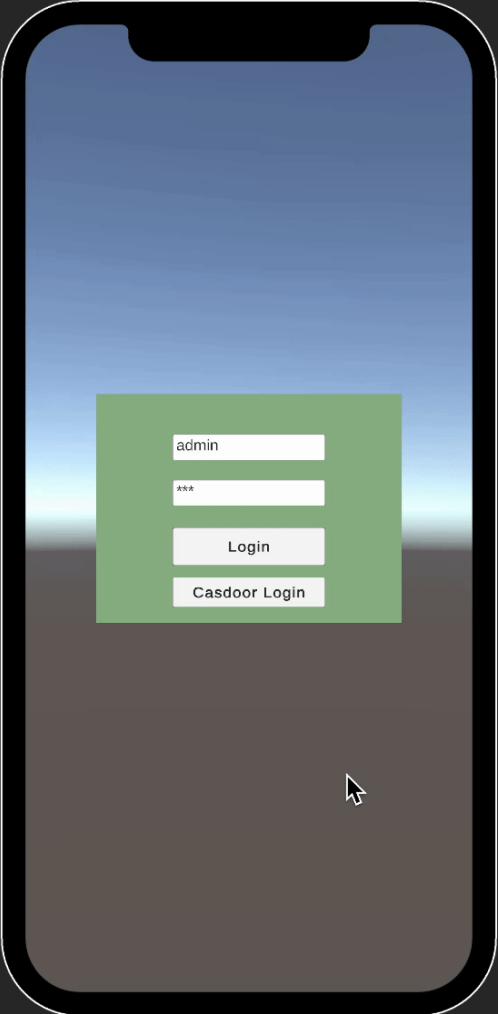
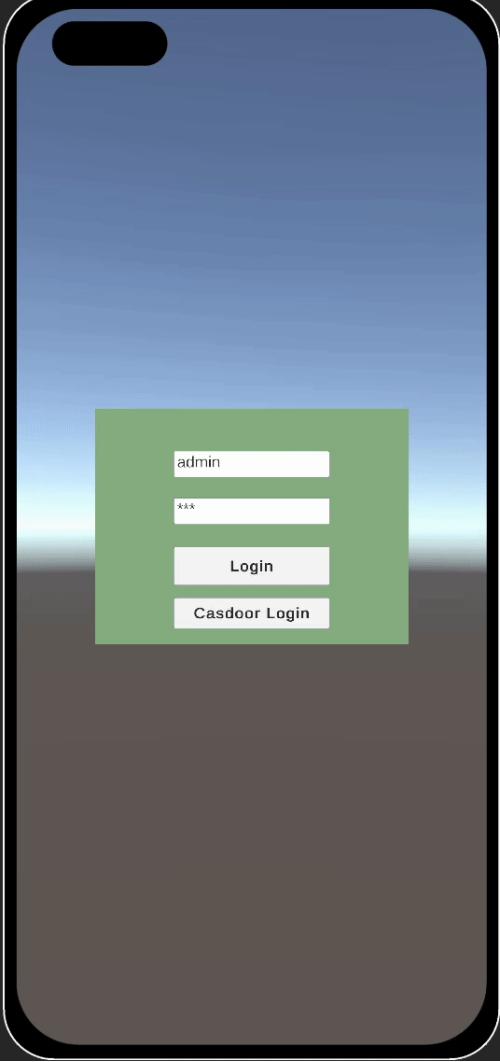


步骤3：使用

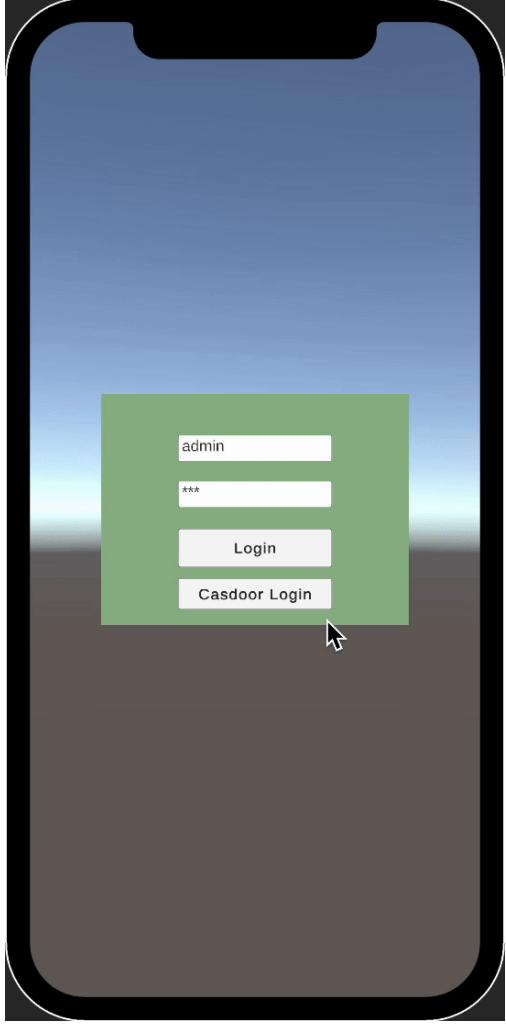
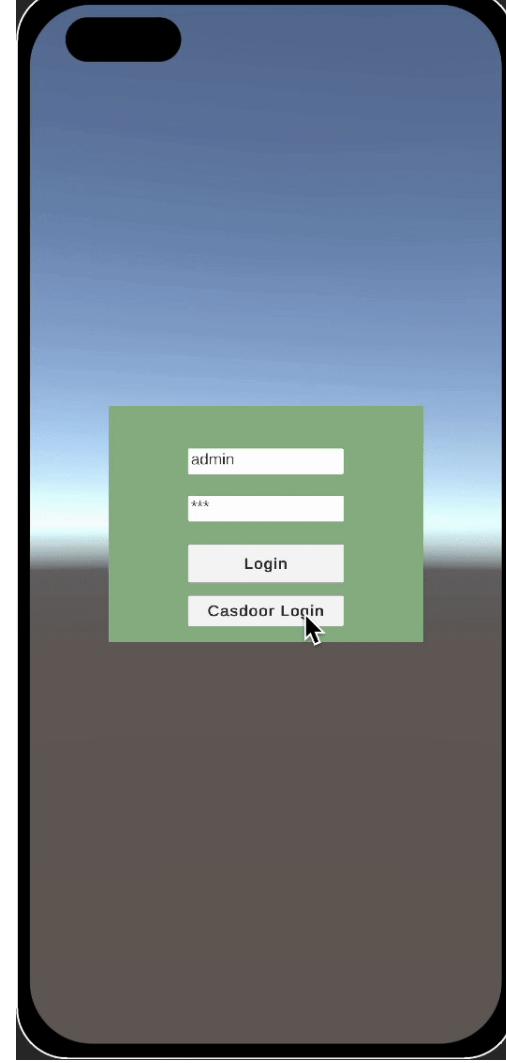
通过查看[casdoor-unity-example](#)来了解如何使用 `Casdoor.Client` SDK 进行 Unity 3D 移动开发。

运行 `casdoor-unity-example` 后，您将看到以下界面：

- 使用用户名和密码登录：

iOS	Android
 An iPhone X-style smartphone displaying a Casdoor login interface. The screen has rounded corners and a notch at the top. A green overlay box contains two input fields: one for 'admin' and one for a password (with three asterisks). Below these are two buttons: 'Login' and 'Casdoor Login'. A cursor arrow is positioned at the bottom center of the phone's body.	 A Pixel 3-style smartphone displaying a Casdoor login interface. The screen has rounded corners and a circular camera cutout at the top. A green overlay box contains two input fields: one for 'admin' and one for a password (with three asterisks). Below these are two buttons: 'Login' and 'Casdoor Login'.

- 使用Casdoor网页登录：

iOS	Android
 A screenshot of an iPhone X displaying a login interface. The interface consists of a green rectangular card with rounded corners. It contains four white rectangular input fields: the first labeled "admin", the second with three asterisks (***) as a placeholder, the third labeled "Login", and the fourth labeled "Casdoor Login". A cursor arrow is positioned directly above the "Casdoor Login" button, indicating it is about to be tapped.	 A screenshot of an Android smartphone displaying a similar login interface. The green card has the same four input fields. The "Casdoor Login" button is highlighted with a white mouse cursor arrow pointing directly at its center.

Go



Kubernetes

在Kubernetes中使用Casdoor进行身份验证



OpenShift

在OpenShift中使用Casdoor进行身份验证



BookStack

在 BookStack 中使用 Casdoor 进行身份验证



Bytebase

使用OAuth2连接各种应用程序，如Bytebase

 **ELK**

Casdoor/elk-auth-casdoor概览

 **Gitea**

在 Gitea 中使用 Casdoor 进行身份验证

 **Grafana**

在 Grafana 中使用 Casdoor 进行身份验证

 **MinIO**

将Casdoor配置为身份提供商以支持MinIO

 **Traefik**

Using Casdoor for authentication with Traefik reverse proxy



Portainer

在Portainer中使用Casdoor进行身份验证

Kubernetes

根据[Kubernetes文档](#), Kubernetes的API服务器可以使用OpenID Connect (OIDC)进行身份验证。本文将指导您如何使用Casdoor在Kubernetes中配置身份验证。

环境要求

在开始之前, 请确保您有以下环境:

- 一个Kubernetes集群。
- 像这样的Casdoor应用程序[演示网站](#)。
- `kubectl`命令工具（可选）。

① 备注

Kubernetes的`oidc-issuer-url`只接受使用`https://`前缀的URL。因此, 您的Casdoor应用程序应部署在HTTPS网站上。

步骤1: 创建一个Casdoor应用和用户账户进行身份验证

转到您的Casdoor应用程序并添加一个名为Kubernetes的新应用。请记住`Name`、`Organization`、`client ID`、`client Secret`, 并为此应用添加一些授权类型。

Name [?](#) : Name

Display name [?](#) :

Logo [?](#) : URL

Preview: 

Home [?](#) :

Description [?](#) :

Organization [?](#) : Organization

Client ID [?](#) : Client ID

Client secret [?](#) : Client secret

Cert [?](#) :

Grant types [?](#) : Authorization Code Password ID Token Refresh Token Client Credentials Token

接下来，向您刚刚创建的应用程序添加一个新用户。请注意，这里使用的 Organization 和 Signup application 应与之前注册的应用对应。

Organization ? :	casbin
ID ? :	202e02e9-9128-496a-a209-fdb336448f56
Name ? :	user_pnvm5i
Display name ? :	New User - pnvm5i
Avatar ? :	<p>Preview:</p>  <p>Upload a photo...</p>
User type ? :	normal-user
Password ? :	Modify password...
Email ? :	pnvm5i@example.com
Phone ? :	+1 ▼ 78005961394
Country/Region ? :	Please select country/region
Location ? :	
Affiliation ? :	Example Inc.
Title ? :	
Homepage ? :	
Bio ? :	
Tag ? :	staff
Signup application ? :	Kubernetes

步骤2：使用OIDC身份验证配置Kubernetes API服务器

要启用OIDC插件，您需要在API服务器上配置以下标志：

- `--oidc-issuer-url`: 允许API服务器发现公共签名密钥的提供者的URL。
- `--oidc-client-id`: 所有令牌必须为其发出的客户端id。

本文使用minikube进行演示。您可以使用以下命令在启动时为minikube的API服务器配置OIDC插件：

```
minikube start --extra-config=apiserver.oidc-issuer-
url=https://demo.casdoor.com --extra-config=apiserver.oidc-client-
id=294b09fbc17f95daf2fe
```

步骤3：测试OIDC身份验证

获取身份验证信息

由于kubectl缺乏前端，可以通过向Casdoor服务器发送POST请求进行身份验证。这是在Python中向Casdoor服务器发送POST请求并检索`id_token`和`refresh_token`的代码：

```
import requests
import json

url = "https://demo.casdoor.com/api/login/oauth/access_token"
payload = json.dumps({}
```

执行此代码后，您应收到类似于以下的响应：

```
{  
    "access_token": "xxx",  
    "id_token": "yyy",  
    "refresh_token": "zzz",  
    "token_type": "Bearer",  
    "expires_in": 72000,  
    "scope": ""  
}
```

现在，您可以使用刚刚获取的 `id_token` 与 Kubernetes API 服务器进行身份验证。

基于HTTP请求的身份验证

将令牌添加到请求头。

```
curl https://www.xxx.com -k -H "Authorization: Bearer $(id_token)"
```

- `https://www.xxx.com` 是 Kubernetes API 服务器的部署地址。

基于Kubectl客户端的身份验证

配置文件方法

将以下配置写入 `~/.kube/config` 文件。 您应该用您之前获得的值替换配置文件中的每个配置项。

```
users:  
- name: minikube  
  user:  
    auth-provider:
```

现在，您可以直接使用kubectl访问您的API服务器。 尝试运行一个测试命令。

```
kubectl cluster-info
```

命令行参数方法

或者，您可以通过直接将`id_token`添加到kubectl的命令行参数中进行身份验证。

```
kubectl --token=$(id_token) cluster-info
```

OpenShift

OpenShift支持OIDC，所以我们可以将Casdoor与OpenShift集成。以下步骤演示了如何使用[Casdoor在线演示](#)将Casdoor与OpenShift Local集成。

步骤1：创建一个Casdoor应用

在Casdoor中添加一个新的应用，注意以下几点：

- 记住Client ID和Client secret以备下一步使用。
- 重定向URL的格式是https://oauth-
openshift.apps.<cluster_name>.<cluster_domain>/*。根据你的情况填写。

Name [?](#) :

Display name [?](#) :

Logo [?](#) :
Preview: 

Home [?](#) :

Description [?](#) :

Organization [?](#) :

Client ID [?](#) :

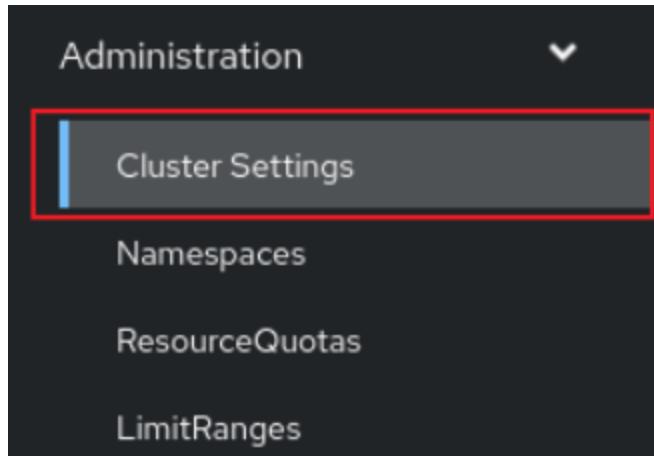
Client secret [?](#) :

Cert [?](#) :

Redirect URLs [?](#) :
Redirect URLs [Add](#)

步骤2：OpenShift OAuth配置

现在以Kubeadmin的身份登录OpenShift控制台。 登录后，浏览侧边菜单并找到集群设置。



在全局配置下，你会看到OAuth。

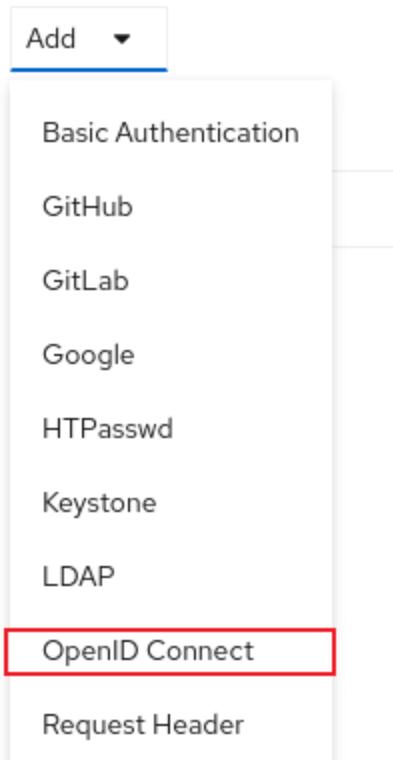
OAuth

OAuth holds cluster-wide information about OAuth. The canonical name is 'cluster'. It is used to configure the integrated OAuth server. This configuration is only honored when the top level Authentication config has type set to IntegratedOAuth. Compatibility level I: Stable within a major release for a minimum of 12 months or 3 minor releases (whichever is longer).

你会看到身份提供商部分。 在添加部分，从选项中选择OpenID Connect。

Identity providers

Identity providers determine ho



配置OIDC，注意以下几点：

- 填写上一步记住的 Client ID 和 Client Secret。
- 发行人URL必须使用https，形式为 https://<casdoor-host>，再次根据你的情况填写。

Add Identity Provider: OpenID Connect

Integrate with an OpenID Connect identity provider using an Authorization Code Flow.

Name *

casdoor

Unique name of the new identity provider. This cannot be changed later.

Client ID *

2452f2b5abb6ff131199

Client secret *

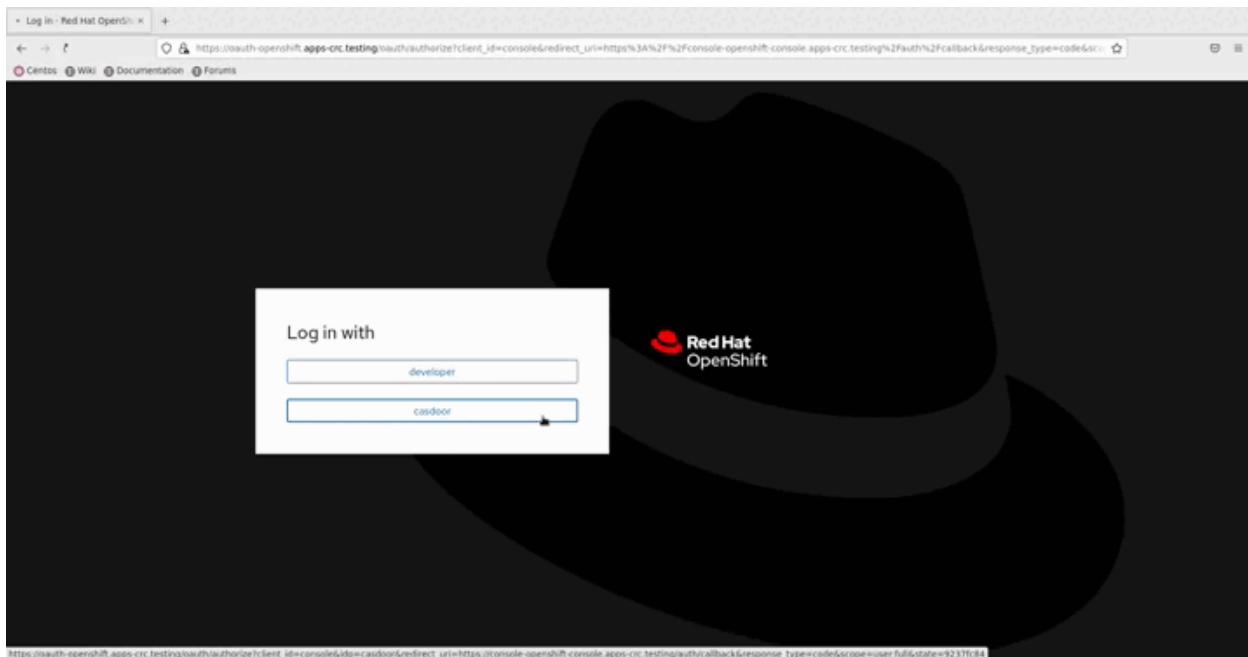
Issuer URL *

https://demo.casdoor.com/

The URL that the OpenID provider asserts as its issuer identifier. It must use the https scheme with no URL query parameters or fragment.

步骤3：测试OIDC身份验证

在浏览器中访问OpenShift控制台。你会看到Casdoor（你在上一步中配置的名称）。点击Casdoor登录选项。你将被重定向到Casdoor登录页面。



BookStack

在 BookStack 中使用 Casdoor 进行身份验证

BookStack是一个开源的书籍和文档分享网站，同时也是一个使用Go语言开发的开源应用程序，帮助您更好地管理文档阅读。

BookStack-casdoor 已经与 Casdoor 集成，现在您可以通过简单的配置快速开始使用。

步骤1：创建一个Casdoor应用

前往您的Casdoor并添加一个名为BookStack的新应用程序。这是在Casdoor中创建BookStack应用程序的一个示例。

Edit Application Save Save & Exit

Name ? : bookstack

Display name ? : bookstack

Logo ? : URL ? : https://cdn.casdoor.com/logo/casdoor-logo_1185x256.png

Preview: 

Home ? :

Description ? :

Organization ? :

Client ID ? :

Client secret ? :

请记住 **名称**, **组织**, **客户端 ID**, 和 **客户密钥**。您将在下一步中需要它们。

步骤2：配置Casdoor登录

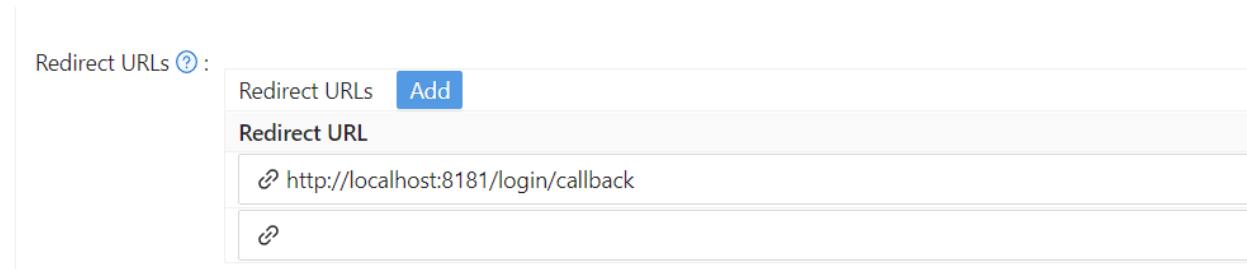
接下来，导航到BookStack并找到文件 `oauth.conf.example`。

将 `oauth.conf.example` 重命名为 `oauth.conf` 和 **修改配置** 默认情况下，内容如下：

```
[oauth]
casdoorOrganization = "<组织>"
casdoorApplication = "bookstack"
casdoorEndpoint = http://localhost:8000
clientId = <客户端 ID>
clientSecret = <客户端密钥>
redirectUrl = http://localhost:8181/login/callback
```

步骤3：在Casdoor中填写 redirectUrl

在最后一步中，返回到您添加BookStack应用程序的页面，并填写 Redirect URLs。确保 Redirect URL 与 oauth.conf 文件中的 redirectUrl 相同。



现在你已经完成了Casdoor的配置！

一旦你成功部署了BookStack，现在你可以回到你的BookStack并体验使用Casdoor进行登录验证。

Bytebase

Casdoor可以使用OAuth2连接各种应用程序。在这个例子中，我们将使用Bytebase来演示如何使用OAuth2连接到您的应用程序。

以下是配置名称：

`CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP地址。

`Bytebase_HOSTNAME`：部署Bytebase的域名或IP地址。

步骤1：部署Casdoor和Bytebase

首先，部署Casdoor和Bytebase。

成功部署后，请确保：

1. Casdoor可以正常登录和使用。
2. 在`prod`模式下部署Casdoor时，您可以将`CASDOOR_HOSTNAME`设置为`http://localhost:8000`。查看[生产模式](#)。

步骤2：配置Casdoor应用程序

1. 创建一个新的或使用现有的Casdoor应用程序。
2. 找到重定向URL：`<CASDOOR_HOSTNAME>/oauth/callback`。
3. 将重定向URL添加到Casdoor应用程序：

Client ID: e828fd6922f4292b979e
 Client secret: bab9f6c2fad67471e1bd81e074ea192e4f46dd
 Cert: cert-built-in
 Redirect URLs: <CASDOOR_HOSTNAME>/oauth/callback

在应用程序设置页面上，您将找到两个值：`Client ID` 和 `Client secret`。我们将在下一步中使用这些值。

打开您喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME/.well-known/openid-configuration`。您将看到Casdoor的OIDC配置。

步骤3：配置Bytebase

1. 找到SSO并选择OAuth 2.0：

SQL Review

- Risk Center
- Custom Approval
- Data Anonymization
- Data Access Control
- Audit Log
- Integration
- GitOps
- SSO** ←
- IM

Type

OAuth 2.0 OIDC

Use template

GitHub GitLab Google Custom

Basic information

Name *

Identity Provider ID: idp-custom-f4mw It cannot be changed later. [Edit](#)

Domain

2. 配置此应用程序：

The screenshot shows the Casdoor application's configuration interface. On the left, there is a sidebar with various tabs: Account, Profile, Workspace, General, Members, Projects, Subscription, Debug Log, Security & Policy, SQL Review, Risk Center, Custom Approval, Data Anonymization, Data Access Control, Audit Log, Integration, GitOps, SSO, IM, and Archive. The 'SSO' tab is selected. In the main area, under 'Basic Information', the 'Name' field is set to 'casdoor'. Under 'Identity provider information', the 'Identity Provider ID' is 'idp-casdoor-mels', 'Domain' is 'http://101.43.192.216:8000', and 'Auth URL' is 'http://101.43.192.216:8000/api/login/oauth/authorize'. The 'Scopes' field contains 'openid profile email'. Under 'Token URL', the 'Token URL' is 'http://101.43.192.216:8000/api/login/oauth/access_token' and the 'User information URL' is 'http://101.43.192.216:8000/api/get-account'. Under 'User information mapping', it maps 'name' to 'Bytebase user identifier', 'name' to 'Bytebase user display name', and 'email' to 'Bytebase user email'. At the bottom right, there are 'Discard changes' and 'Update' buttons.

3. 在Casdoor应用程序页面上找到Client ID和Client Secret。

- Token server URL: `http://CASDOOR_HOSTNAME/api/login/oauth/access_token`
- Authorization server URL: `http://CASDOOR_HOSTNAME/login/oauth/authorize`
- User Info server URL: `http://CASDOOR_HOSTNAME/api/get-account`
- Scopes: address phone openid profile offline_access email

退出Bytebase并测试SSO。

The screenshot shows the Bytebase login page. It features a cartoon illustration of a rocket launching from a moon surface with two characters, one labeled 'DBA' and the other 'DEV', cheering. To the right is the Bytebase logo and the word 'Bytebase'. Below the logo is a form with fields for 'Email' (containing 'jim@example.com') and 'Password'. There is a 'Forgot your password?' link and a 'Sign in' button. Below the button are links for 'New to Bytebase? Sign up' and 'Sign in with casdoor'. At the bottom, there is a copyright notice: 'English 简体中文 © 2023 Bytebase. All rights reserved.'

ELK

Casdoor/elk-auth-casdoor概览

ELK（Elasticsearch, Logstash和Kibana）最大的缺点之一是，这些产品最初没有认证机制。因此，任何知道Kibana或Elasticsearch的URL的人都可以访问Kibana仪表板。后来，ELK集成了一个名为“Xpack”的嵌入式认证系统。然而，它的高级功能（如OAuth, OIDC, LDAP, SAML）并不是免费的。只有使用一组账户和密码的普通认证是免费的，这非常不方便。这种方法不允许我们为公司中的每个人提供唯一的账户。

为了解决这个问题，我们基于Casdoor开发了一种麋鹿认证解决方案。此解决方案是免费的，开源的，正在进行持续的维护，并支持一系列高级功能。Casdoor是一个基于OAuth 2.0/OIDC的集中认证/单点登录平台。Casdoor/elk-auth-casdoor充当反向代理，旨在拦截所有朝向ELK/Kibana堆栈的HTTP数据流。它引导尚未登录的用户进行登录。只要用户已登录，这个反向代理就会透明地运行。

如果用户未被正确验证，请求将被暂时缓存，并且用户将被重定向到Casdoor登录页面。一旦用户通过Casdoor登录，缓存的请求将会被恢复并发送到Kibana。因此，如果一个POST请求（或者除GET之外的任何其他类型的请求）被拦截，用户就不需要重新填写表单并重新发送请求。逆向代理将为你记住它。

Casdoor/elk-auth-casdoor仓库位于<https://github.com/casdoor/elk-auth-casdoor>。

如何使用？

0. 确保你已经安装了Go编程语言环境。
1. 前往 [casdoor/elk-auth-casdoor](https://github.com/casdoor/elk-auth-casdoor) 并获取代码。

2. 将您的代理注册为Casdoor的应用程序。

3. 修改配置。

配置文件位于 "conf/app.conf"。 这是一个例子，你应根据自己的具体需求进行定制。

```
appname = .
# port on which the reverse proxy shall be run
httpport = 8080
runmode = dev
# EDIT IT IF NECESSARY. The URL of this reverse proxy.
pluginEndpoint = "http://localhost:8080"
# EDIT IT IF NECESSARY. The URL of the Kibana.
targetEndpoint = "http://localhost:5601"
# EDIT IT. The URL of Casdoor.
casdoorEndpoint = "http://localhost:8000"
# EDIT IT. The clientID of your reverse proxy in Casdoor.
clientID = ceb6eb261ab20174548d
# EDIT IT. The clientSecret of your reverse proxy in Casdoor.
clientSecret = af928f0ef1abc1b1195ca58e0e609e9001e134f4
# EDIT IT. The application name of your reverse proxy in
Casdoor.
appName = ELKProxy
# EDIT IT. The organization to which your reverse proxy
belongs in Casdoor.
organization = built-in
```

4. 访问 <http://localhost:8080>（在上述示例中）并按照重定向指导进行登录。然后，你应该会看到Kibana被Casdoor保护并进行了身份验证。

5. 如果一切运行正常，不要忘记通过配置防火墙（或其他方法）来阻止外部访问原始的 Kibana端口。这确保了外部人员只能通过这个反向代理来访问Kibana。

Gitea

在 Gitea 中使用 Casdoor 进行身份验证

Gitea 是一个社区管理的轻量代码托管解决方案，写入Go。采用MIT开源协议

Gitea支持第三方身份验证，包括Oauth，这样就可以使用Casdoor进行身份验证。以下是操作教程。

准备：

要配置 Gitea 使用 Casdoor 作为身份识别提供者，您需要安装 Gitea 以及访问管理员帐户。

关于如何下载、安装和运行 Gitea 的更多信息，请参阅 <https://docs.gitea.io/en-us/install-from-binary/>

您需要在安装过程中创建管理员帐户。如果您已经注册，管理员将是第一个注册用户。请使用此帐户继续以下操作。

1. 创建一个Casdoor应用程序

像这样：

Edit Application

Name ⓘ: application_9p7eai

Display name ⓘ: New Application - 9p7eai

Logo ⓘ: URL ⓘ: https://cdn.casbin.com/logo/logo_1024x256.png

Preview: 

Home ⓘ: [View](#)

Description ⓘ:

Organization ⓘ: built-in

Client ID ⓘ: 7ceb9b7fda4a9061ec1c

Client secret ⓘ: 3416238e1edf915eac08b8fe345b2b95cdba7e04

Cert ⓘ: cert-built-in

Redirect URLs

Action	Redirect URLs	Add
Edit Delete	http://localhost:3000/user/oauth2/Casdoor/callback	Add

请记住客户端ID和密码，以便下一步操作。

请不要在此步骤中填写回调url。Url取决于下一步Gitea的配置。稍后我们将返回来设置一个正确的回调url。

2. 配置 Gitea 使用 Casdoor

以管理员身份登录。通过右上角的下拉菜单转到“站点管理”页面。然后切换到“认证源”页面

你应该看到类似下面的内容：

Issues Pull Requests Milestones Explore

Dashboard User Accounts Organizations Repositories Webhooks Authentication Sources User Emails Configuration System Notices Monitoring

Authentication Source Management (Total: 0) Add Authentication Source

ID	Name	Type	Enabled	Updated	Created	Edit

按“添加认证源”按钮并填写类似的表单。

Issues Pull Requests Milestones Explore

Dashboard User Accounts Organizations Repositories Webhooks Authentication Sources User Emails Configuration System Notices Monitoring

Add Authentication Source

Authentication Type * OAuth2

Authentication Name * Casdoor

OAuth2 Provider * OpenID Connect

Client ID (Key) * 7ceb9b7fda4a9061ec1c

Client Secret * 3416238e1edf915eac08b8fe345b2b95cd8a7e04

Icon URL

OpenID Connect Auto Discovery URL * http://localhost:8000/.well-known/openid-configuration

Skip local 2FA
Leaving unset means local users with 2FA set will still have to pass 2FA to log on

Additional Scopes

请选择认证类型为“oauth2”。

请输入此认证源的名称并 **记住此名称**。此名称将在下一步骤中用于回调url。

请选择 **OpenID Connect** Oauth2 提供商。

填写上一步中记住的**客户端ID**和**客户端密码**。

在 **openid** 连接中填写自动发现URL，它应该是 `<your endpoint of casdoor>/.well-known /openid-configuration`。

按您的意愿填写其他可选配置项。然后提交它。

提交表单

3. 配置后台回调url

返回第2步中的应用程序编辑页面并添加以下回调url：

`<endpoint of gitea>/user/oauth2/<authentication source name>/callback`

`<authentication source name>` 是上一步Gitea认证源的名称。

4. 在 Gitea 上试试

退出当前管理员帐户。

您应该在登录页面中看到这一点：

The screenshot shows a top navigation bar with 'Sign In' and 'OpenID' buttons. Below is a 'Sign In' form with fields for 'Username or Email Address' and 'Password'. There is a 'Remember this Device' checkbox, a 'Sign In' button, a 'Forgot password?' link, and a 'Need an account? Register now.' link. At the bottom is an 'OpenID Connect' sign-in button.

Sign In

OpenID

Sign In

Username or Email Address *

Password *

Remember this Device

Sign In [Forgot password?](#)

[Need an account? Register now.](#)

Sign In With OpenID Connect

按“使用openid登录”按钮，您将被重定向到casdoor登录页面。

登录后您将看到这个：

The screenshot shows a 'Complete New Account' form within a Gitea interface. It includes fields for 'Username' and 'Email Address', both marked with a red asterisk indicating they are required. A 'Complete Account' button is at the bottom.

Explore Help

Register New Account [Link to Existing Account](#)

Complete New Account

Username *

Email Address *

admin@example.com

Complete Account

按照指示并用一个新的 Gitea 帐户或现有帐户绑定下级帐户。

然后一切都将正常工作。

Grafana

在 Grafana 中使用 Casdoor 进行身份验证

Grafana 支持通过 OAuth 进行身份验证。因此，用户使用 Casdoor 登录 Grafana 非常容易。只需要几个步骤和简单的配置就可以实现。

这是一个关于如何在 Grafana 中使用 Casdoor 进行身份验证的教程。在您继续之前，请确保您已安装并运行了 Grafana。

步骤1：在 Casdoor 中为 Grafana 创建一个应用

这是在 Casdoor 中创建应用的一个示例：

Edit Application Save Save & Exit

Name ⓘ: application_9p7eai

Display name ⓘ: New Application - 9p7eai

Logo ⓘ:  URL ⓘ: https://cdn.casbin.com/logo/logo_1024x256.png

Preview: 

Home ⓘ: [/](#)

Description ⓘ:

Organization ⓘ: built-in

Client ID ⓘ: 7ceb9b7fda4a9061ec1c

Client secret ⓘ: 3416238e1edf915eac08b8fe345b2b95cd8a7e04

Cert ⓘ: cert-built-in

Redirect URLs ⓘ: Add

Action	Redirect URL
▲ ▼ ✖	http://localhost:3000/login/generic_oauth

请复制客户端密钥和客户端ID以进行下一步操作。

请添加Grafana的回调URL。默认情况下，Grafana的OAuth回调是/login/generic_oauth。所以请正确地连接这个URL。

步骤2：修改Grafana的配置

默认情况下，OAuth的配置文件位于Grafana的工作目录中的<conf/defaults.ini>。

请找到部分[\[auth.generic_oauth\]](auth.generic_oauth)并修改以下字段：

```
[auth.generic_oauth]
name = Casdoor
icon = signin
enabled = true
allow_sign_up = true
```

关于HTTPS

如果你不希望为Casdoor启用HTTPS，或者你在没有启用HTTPS的情况下部署Grafana，请同时设置`tls_skip_verify_insecure = true`。

关于使用Casdoor登录后的redirectURI

如果在Grafana中使用Casdoor登录后重定向URI不正确，您可能需要配置[root_url](#)。

```
[server]
http_port = 3000
# 用于从浏览器访问Grafana的公开面向的域名
domain = <你的IP地址>
# 完整的公开面向的URL
root_url = %(protocol)s://%(domain)s:%(http_port)s/
```

相关链接：

1. [Grafana 文档](#)
2. [Grafana 默认的ini](#)

关于角色映射

您可能希望配置`role_attribute_path`，通过[role_attribute_path](#)将您的用户角色映射到Grafana。

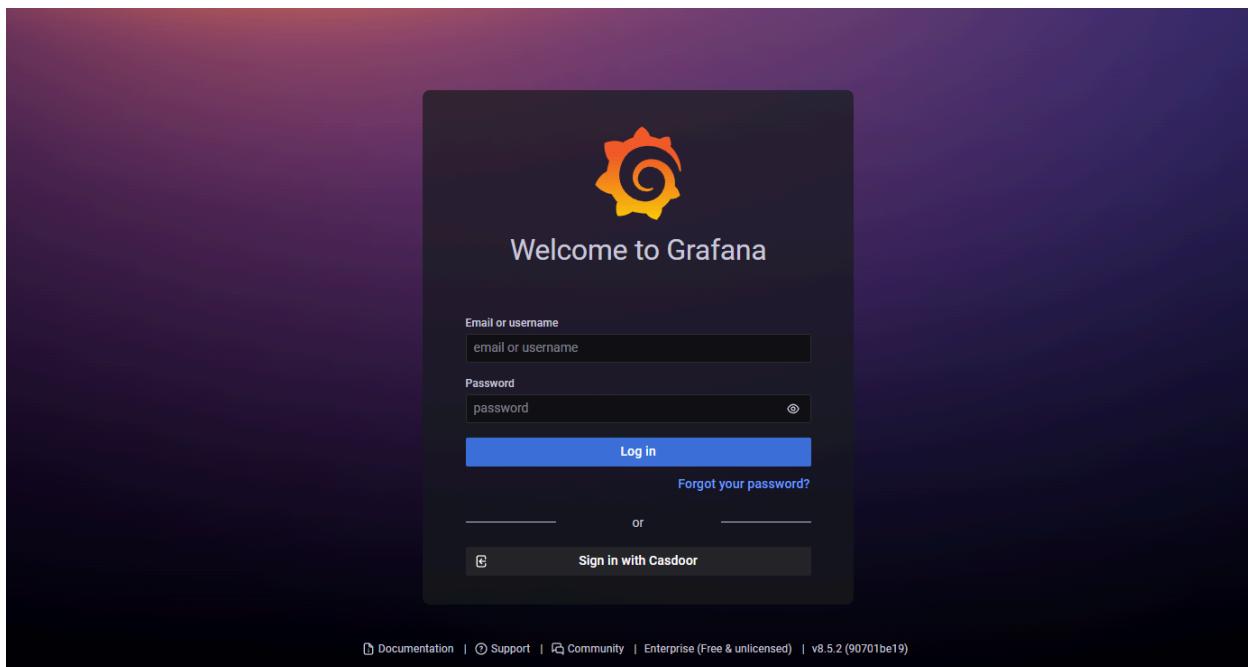
```
[auth.generic_oauth]
role_attribute_path = contains(roles[*].name, 'admin') && 'Admin'
|| contains(roles[*].name, 'editor') && 'Editor' || 'Viewer'
role_attribute_strict = true
```

这里的`role_attribute_path`后的JMESPath表达式非常重要。请参考Grafana文档。

步骤3：查看是否有效

关闭Grafana并重新启动它。

前往登录页面。你应该会看到类似这样的东西：



MinIO

MinIO 支持使用与OpenID Connect (OIDC)兼容的提供商进行外部身份管理。 本文档介绍了如何配置Casdoor作为身份提供商以支持MinIO。

步骤1：部署Casdoor & MinIO

首先，部署Casdoor。

您可以参考Casdoor官方文档中的[服务器安装](#)。

成功部署后，请确保：

- Casdoor 服务器正在 <http://localhost:8000> 上运行。
- 打开你最喜欢的浏览器，访问 <http://localhost:7001>，你将看到Casdoor的登录页面。
- 通过输入 `admin` 和 `123` 来测试登录功能。

接下来，您可以按照以下步骤在您自己的应用中快速实现基于Casdoor的登录页面。

您可以参考[这里](#)来部署您的MinIO服务器，以及[这里](#)来获取名为 `mc` 的MinIO客户端。

步骤2：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序，或使用一个已经存在的。
2. 添加您的重定向URL。

Client ID [?](#) : 24a25ea0714d92e78595 **Client ID**

Client secret [?](#) : 155... **Client Secret**

Redirect URLs [?](#) : [Add](#)
Redirect URL **Add a redirect URL for spring security**
<http://localhost:8082/ui-one/login/oauth2/code/custom>

3. 添加您想要的提供者并提供任何必要的设置。

在应用设置页面上，您会找到两个值：**Client ID** 和 **Client secret**（如上图所示）。我们将在下一步中使用这些值。

打开你最喜欢的浏览器并访问：http://CASDOOR_HOSTNAME/.well-known/openid-configuration 来查看Casdoor的OIDC配置。

4. 这个步骤对于MinIO来说是必要的。由于MinIO需要在JWT中使用一个声明属性作为其策略，您也应在Casdoor中进行配置。目前，Casdoor 使用 **tag** 作为配置 MinIO 策略的一种变通方法。

Tag [?](#) : **readwrite**

您可以在[这里](#)找到所有支持的策略。

步骤3：配置MinIO

您可以使用以下命令启动 MinIO 服务器：

```
导出MINIO_ROOT_USER=minio  
导出 MINIO_ROOT_PASSWORD=minio123  
minio server /mnt/export
```

您可以使用`--console-address`参数来配置地址和端口。

接下来，使用MinIO客户端`mc`添加一个服务别名。

```
mc alias set myminio <您的控制台地址> minio minio123
```

现在，配置MinIO的OpenID Connect。对于Casdoor，命令将是：

```
mc admin config set myminio identity_openid  
config_url="http://CASDOOR_HOSTNAME/.well-known/openid-  
configuration" client_id=<client id> client_secret=<client secret>  
claim_name="tag"
```

您可以参考[官方文档](#)以获取更详细的参数信息。

一旦成功设置，重新启动MinIO实例。

```
mc 管理服务重启myminio
```

步骤4：尝试演示！

现在，在浏览器中打开您的MinIO控制台，然后点击[使用SSO登录](#)。

您将被重定向到Casdoor用户登录页面。成功登录后，您将被重定向到MinIO页面并自动登录。您现在应该能看到您有权限访问的存储桶和对象。

注意事项

如果你在不同的端口部署Casdoor的前端和后端，你被重定向的登录页面将在后端端口上，并且它会显示 `404 not found`。您可以将端口修改为前端端口。然后，您可以成功访问Casdoor登录页面。

Traefik

Using Casdoor for authentication with Traefik

[Traefik](#) is a modern HTTP reverse proxy and load balancer that makes deploying microservices easy. This document shows how to use Casdoor as an authentication provider with Traefik using the [traefik-casdoor-auth](#) middleware.

The Traefik Casdoor Auth middleware allows you to protect your services behind Traefik with Casdoor authentication, providing a seamless Single Sign-On (SSO) experience.

Prerequisites

Before you begin, ensure you have:

- Traefik v2.x or v3.x installed and running
- A Casdoor instance deployed and accessible
- Docker and Docker Compose (if using the containerized approach)

Step 1: Deploy Casdoor

First, deploy Casdoor if you haven't already.

You can refer to the Casdoor official documentation for [Server Installation](#).

After a successful deployment, make sure that:

- The Casdoor server is running and accessible
- You can log in to the Casdoor admin interface
- Test the login functionality by entering `admin` and `123`

Step 2: Configure Casdoor Application

1. Create a new Casdoor application or use an existing one.
2. Add your redirect URL. The redirect URL should be in the format:

```
http://<your-domain>/callback
```

For example: `http://localhost:8080/callback`

3. Note down the following values from your application settings:
 - Client ID
 - Client Secret
 - Organization Name
 - Application Name

Client ID <small>?</small> :	24a25ea0714d92e78595	Client ID					
Client secret <small>?</small> :	155 [REDACTED]	Client Secret					
Redirect URLs <small>?</small> :	<table><tr><td>Redirect URLs</td><td>Add</td></tr><tr><td>Redirect URL</td><td>Add a redirect URL for spring security</td></tr><tr><td colspan="2">🔗 http://localhost:8082/ui-one/login/oauth2/code/custom</td></tr></table>	Redirect URLs	Add	Redirect URL	Add a redirect URL for spring security	🔗 http://localhost:8082/ui-one/login/oauth2/code/custom	
Redirect URLs	Add						
Redirect URL	Add a redirect URL for spring security						
🔗 http://localhost:8082/ui-one/login/oauth2/code/custom							

1. Configure your application to use the appropriate authentication providers as needed.

Step 3: Deploy traefik-casdoor-auth Middleware

There are two ways to deploy the Traefik Casdoor Auth middleware:

Option 1: Using Docker Compose (Recommended)

Create a `docker-compose.yml` file:

```
version: '3'

services:
  traefik:
    image: traefik:v2.10
    container_name: traefik
    restart: unless-stopped
    command:
      - "--api.insecure=true"
      - "--providers.docker=true"
```

Replace the placeholder values:

- <your-client-id>: Your Casdoor application client ID
- <your-client-secret>: Your Casdoor application client secret
- <your-organization>: Your Casdoor organization name
- <your-application>: Your Casdoor application name

Start the services:

```
docker-compose up -d
```

Option 2: Using Binary Deployment

1. Download the latest release from the [traefik-casdoor-auth releases page](#).
2. Create a configuration file config.yaml:

```
casdoor:  
  endpoint: "http://localhost:8000"  
  clientId: "<your-client-id>"  
  clientSecret: "<your-client-secret>"  
  organizationName: "<your-organization>"  
  applicationName: "<your-application>"  
  
server:  
  port: 8080  
  callbackUrl: "http://localhost/callback"
```

1. Run the middleware:

```
./traefik-casdoor-auth --config config.yaml
```

1. Configure Traefik to use the middleware. Add to your Traefik dynamic configuration:

```
http:  
  middlewares:  
    casdoor-auth:  
      forwardAuth:  
        address: "http://localhost:8080/verify"  
        authResponseHeaders:  
          - "X-Forwarded-User"  
  
  routers:  
    my-protected-service:  
      rule: "Host(`example.com`)"  
      middlewares:  
        - casdoor-auth  
      service: my-service
```

Step 4: Test the Integration

1. Access your protected service through Traefik (e.g., `http://localhost` if using the Docker Compose example).
2. You should be redirected to the Casdoor login page.
3. Log in with your Casdoor credentials.
4. After successful authentication, you will be redirected back to your protected service.
5. The middleware will set the `X-Forwarded-User` header with the authenticated user's information, which your backend service can use.

Configuration Options

The traefik-casdoor-auth middleware supports the following environment variables:

Variable	Description	Required
<code>CASDOOR_ENDPOINT</code>	URL of your Casdoor instance	Yes
<code>CLIENT_ID</code>	Casdoor application client ID	Yes
<code>CLIENT_SECRET</code>	Casdoor application client secret	Yes
<code>CASDOOR_ORGANIZATION</code>	Casdoor organization name	Yes
<code>CASDOOR_APPLICATION</code>	Casdoor application name	Yes
<code>CALLBACK_URL</code>	OAuth callback URL	Yes
<code>JWT_SECRET</code>	Secret for JWT token signing (auto-generated if not set)	No
<code>SESSION_TIMEOUT</code>	Session timeout in seconds (default: 3600)	No
<code>LOG_LEVEL</code>	Logging level: debug, info, warn, error (default: info)	No

Advanced Configuration

Using HTTPS

For production deployments, it's recommended to use HTTPS. Update your Traefik configuration to include TLS:

```
services:  
  traefik:  
    command:  
      - "--entrypoints.web.address=:80"  
      - "--entrypoints.websecure.address=:443"  
      - "--certificatesresolvers.myresolver.acme.tlschallenge=true"  
      - "--certificatesresolvers.myresolver.acme.email=your-  
        email@example.com"  
      - "--"  
    certificatesresolvers.myresolver.acme.storage=/letsencrypt/  
      acme.json"  
    ports:  
      - "80:80"  
      - "443:443"  
    volumes:  
      - ./letsencrypt:/letsencrypt
```

And update your service router configuration:

```
labels:  
  - "traefik.http.routers.whoami.entrypoints=websecure"  
  - "traefik.http.routers.whoami.tls.certresolver=myresolver"
```

Customizing Session Behavior

You can customize session timeout and other behaviors:

```
environment:  
- SESSION_TIMEOUT=7200 # 2 hours  
- LOG_LEVEL=debug
```

Troubleshooting

Redirect Loop

If you experience a redirect loop:

1. Verify that the `CALLBACK_URL` matches the redirect URL configured in your Casdoor application.
2. Check that cookies are enabled in your browser.
3. Ensure the middleware can reach the Casdoor endpoint.

Authentication Fails

If authentication fails:

1. Check that the `CLIENT_ID` and `CLIENT_SECRET` are correct.
2. Verify that the Casdoor organization and application names are correct.
3. Check the middleware logs for detailed error messages: `docker logs casdoor-auth`

502 Bad Gateway

If you see a 502 error:

1. Ensure the casdoor-auth service is running: `docker ps`
2. Check that all services are on the same Docker network.
3. Verify the ForwardAuth address is correct in the Traefik configuration.

Resources

- [Traefik Casdoor Auth GitHub Repository](#)
- [Traefik ForwardAuth Middleware Documentation](#)
- [Casdoor Documentation](#)

Portainer

在Portainer中使用Casdoor进行身份验证

Portainer支持通过OAuth进行身份验证。因此，用户可以轻松地使用Casdoor登录Portainer。只需要几个步骤和简单的配置就可以实现。

这里有一个关于如何在Grafana中使用Casdoor进行身份验证的教程。在你开始之前，请确保你已经安装并运行了Portainer。

以下是配置名称：

`CASDOOR_HOST`：部署Casdoor服务器的域名或IP地址。

`PORTAINER_HOST`：部署Portainer的域名或IP地址。

步骤1：在Casdoor中为Portainer创建一个应用

这是在Casdoor中创建应用的一个例子：

Name ⓘ : Portainer_test

Display name ⓘ : Portainer_test

Logo ⓘ : URL ⓘ : https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home ⓘ :

Description ⓘ :

Organization ⓘ : built-in

Tags ⓘ :

Client ID ⓘ : 2da468d1968c5f85d6b4

Client secret ⓘ : b4db599c84f978425102f161b833625faf9b6b7c

Cert ⓘ : cert-built-in

Redirect URLs ⓘ : Redirect URLs Add

Redirect URL : https://<PORTAINER_HOST>

1. 复制客户端密钥和客户端ID以备下一步使用。
2. 添加一个重定向URL。这是你的Portainer主机。

步骤2：配置Portainer

从左侧导航栏展开设置，然后从此列表中点击**身份验证**选项。

1. 启用使用SSO和自动用户配置：

The screenshot shows the Portainer.io interface with the 'Authentication' tab selected in the sidebar. The main page title is 'Authentication settings'. Under 'Authentication method', 'Microsoft Active Directory' is highlighted with an orange border. Other options like 'Internal', 'LDAP', and 'OAuth' are also shown. Below this, there are sections for 'Single Sign-On' (with 'Use SSO' checked) and 'Automatic user provisioning' (with a toggle switch checked).

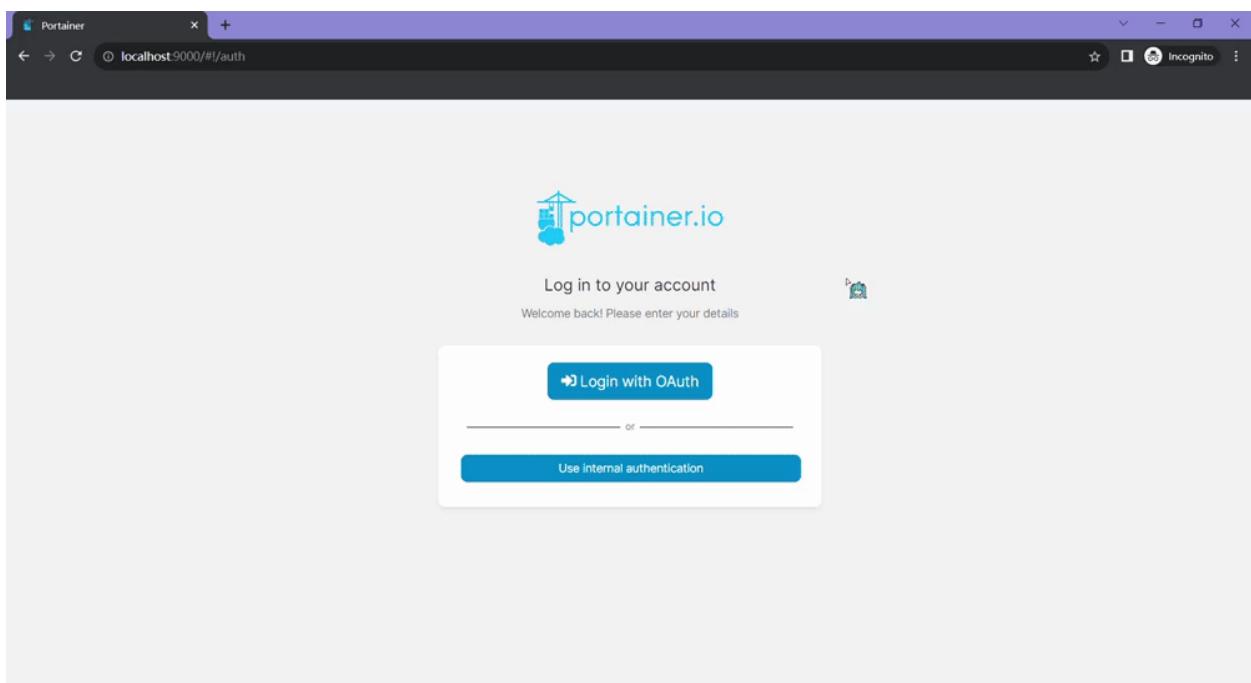
2. 按照以下方式填写必要的信息:

The screenshot shows the Portainer.io interface with the 'Authentication' tab selected in the sidebar. The main page title is 'OAuth Configuration'. Under 'Provider', 'Custom' is selected. In the 'OAuth Configuration' section, various fields are filled with specific URLs and identifiers.

Setting	Value
Client ID	89c7dba629b5722d4ea2
Client secret
Authorization URL	<a href="https://<CASDOOR_HOST>/login/oauth/authorize">https://<CASDOOR_HOST>/login/oauth/authorize
Access token URL	<a href="https://<CASDOOR_HOST>/api/login/oauth/access_token">https://<CASDOOR_HOST>/api/login/oauth/access_token
Resource URL	<a href="https://<CASDOOR_HOST>/api/userinfo">https://<CASDOOR_HOST>/api/userinfo
Redirect URL	<a href="https://<PORTAINER_HOST>">https://<PORTAINER_HOST>
User identifier	email
Scopes	openid email profile

- Authorization URL: https://<CASDOOR_HOST>/login/oauth/authorize
- Access token URL: https://<CASDOOR_HOST>/api/login/oauth/access_token
- Resource URL: https://<CASDOOR_HOST>/api/userinfo
- Redirect URL: https://<PORTAINER_HOST>

退出Portainer并进行测试。



Java

Spring Boot

在Spring Boot项目中使用Casdoor

Spring Cloud

在Spring Cloud中使用 Casdoor

Spring Cloud Gateway

在Spring Cloud Gateway中使用 Casdoor

Spring 安全

2 个项目

Jenkins 插件

使用 Casdoor 插件进行 Jenkins 安全

Jenkins OIDC

使用OIDC协议作为IDP连接各种应用，如Jenkins

Jira

2 个项目

使用OIDC协议连接应用程序 - Confluence

学习如何使用OIDC协议作为IDP连接Confluence和其他应用程序。

RuoYi

在 RuoYi-Cloud 上使用 Casdoor

Pulsar Manager

在 Pulsar Manager 中使用 Casdoor

在 ShenYu 中使用 Casdoor

如何在ShenYu中使用Casdoor

ShardingSphere

在ShardingSphere中使用 Casdoor

Apache IoTDB

使用Casdoor与Apache IoTDB

Apache DolphinScheduler

使用Casdoor进行DolphinScheduler的SSO登录



FireZone

使用OIDC协议作为IDP连接各种应用，如FireZone



Cloud Foundry

了解如何将Casdoor与Cloud Foundry集成，以保护您的应用程序。



Thingsboard

学习如何将Casdoor与Thingsboard集成，以保护您的应用程序

Spring Boot

[casdoor-spring-boot-example](#)是一个如何在Spring Boot项目中使用[casdoor-spring-boot-starter](#)的示例。我们将引导您完成以下步骤。

步骤1：部署Casdoor

首先，应部署Casdoor。

您可以参考[服务安装](#)的 Casdoor 官方文档。请在 **生产模式** 中部署您的 castor 实例。

部署成功后，请确保以下内容：

- 打开你最喜欢的浏览器，访问 <http://localhost:8000>。您将看到Casdoor的登录页面。
- 通过输入 `admin` 作为用户名和 `123` 作为密码来测试登录功能。

现在，您可以按照以下步骤在您自己的应用中快速实现基于Casdoor的登录页面。

步骤2：导入casdoor-spring-boot-starter

您可以使用Maven或Gradle导入casdoor-spring-boot-starter。

[Maven](#) [Gradle](#)

```
<!-- https://mvnrepository.com/artifact/org.casbin/casdoor-spring-
```

```
// https://mvnrepository.com/artifact/org.casbin/casdoor-spring-boot-starter
implementation group: 'org.casbin', name: 'casdoor-spring-boot-starter', version: '1.x.y'
```

步骤3：初始化配置

初始化需要按以下顺序的6个字符串类型参数： | 名称 | 必需的 | 描述 ||
----- | --- | ----- | | endpoint | 是 |
Casdoor 服务器 URL, 例如 http://localhost:8000 | | clientId | 是 | 应用程序客户
端ID | | clientSecret | 是 | 应用程序客户端密钥 | | certificate | 是 | 应用程序证书 ||
organizationName | 是 | 应用程序组织 | | applicationName | 否 | 应用程序名称 | 您可
以使用Java属性或YAML文件进行初始化。

Properties YML

```
casdoor.endpoint = http://localhost:8000
casdoor.clientId = <client-id>
casdoor.clientSecret = <client-secret>
casdoor.certificate = <certificate>
casdoor.organizationName = built-in
casdoor.applicationName = app-built-in
```

```
casdoor:
  endpoint: http://localhost:8000
  client-id: <client-id>
  client-secret: <client-secret>
  certificate: <certificate>
  organization-name: built-in
  application-name: app-built-in
```

⚠ 注意事项

将配置值替换为您自己的Casdoor实例，特别是`clientId`, `clientSecret`和`jwtPublicKey`。

步骤4：重定向到登录页面

当你需要验证访问你的应用的用户时，你可以发送目标URL并重定向到Casdoor提供的登录页面。请确保您已经在应用程序配置中添加了回调URL（例如，<http://localhost:8080/login>）。

```
@Resource  
private CasdoorAuthService casdoorAuthService;  
  
@RequestMapping("toLogin")  
public String toLogin() {  
    return "redirect:" +  
casdoorAuthService.getSigninUrl("http://localhost:8080/login");  
}
```

步骤5：获取令牌并解析

在通过Casdoor验证后，它将带着代码和状态重定向回您的应用程序。

您可以获取代码并调用`getAuthToken`方法，然后解析JWT令牌。

`Casdoor User` 包含了由Casdoor提供的有关用户的基本信息。您可以使用它来设置应用程序中的会话。

```
@RequestMapping("login")
```

服务

以下是API的示例：

- CasdoorAuthService
 - `String token = casdoorAuthService.getOAuthToken(code, "app-built-in");`
 - `CasdoorUser casdoorUser = casdoorAuthService.parseJwtToken(token);`
- CasdoorUserService
 - `CasdoorUser casdoorUser = casdoorUserService.getUser("admin");`
 - `CasdoorUser casdoorUser = casdoorUserService.getUserByEmail("admin@example.com");`
 - `CasdoorUser[] casdoorUsers = casdoorUserService.getUsers();`
 - `CasdoorUser[] casdoorUsers = casdoorUserService.getSortedUsers("created_time", 5);`
 - `int count = casdoorUserService.getUserCount("0");`
 - `CasdoorResponse response = casdoorUserService.addUser(user);`
 - `CasdoorResponse response = casdoorUserService.updateUser(user);`
 - `CasdoorResponse response = casdoorUserService.deleteUser(user);`
- CasdoorEmailService
 - `CasdoorResponse response = casdoorEmailService.sendEmail(title, content, sender, receiver);`
- CasdoorSmsService
 - `CasdoorResponse response = casdoorSmsService.sendSms(randomCode(), receiver);`

- CasdoorResourceService
 - CasdoorResponse response =
casdoorResourceService.uploadResource(user, tag, parent,
fullFilePath, file);
 - CasdoorResponse response =
casdoorResourceService.deleteResource(file.getName());

更多资源

您可以探索以下项目/文档，以了解更多关于将Java与Casdoor集成的信息：

- [casdoor-java-sdk](#)
- [casdoor-spring-boot-starter](#)
- [casdoor-spring-boot-example](#)
- [casdoor-spring-security-example](#)
- [casdoor-spring-security-react-example](#)
- [casdoor-spring-boot-shiro-example](#)

Spring Cloud

在Spring Cloud微服务系统中，通常在网关处进行身份验证。请参考 [casdoor-springcloud-gateway-example](#) 获取更多信息。

如果您想要在单个服务中使用Casdoor，您可以参考 [casdoor-spring-boot](#)示例。

无论是在网关层还是在单个服务中，都使用了[casdoor-spring-boot-starter](#)。

更多内容

您可以探索以下项目/文档，以了解更多关于将Java与Casdoor集成的信息：

- [casdoor-java-sdk](#)
- [casdoor-spring-boot-starter](#)
- [casdoor-spring-boot-example](#)
- [casdoor-spring-security-example](#)
- [casdoor-spring-security-react-example](#)
- [casdoor-spring-boot-shiro-example](#)
- [casdoor-springcloud-gateway-example](#)

Spring Cloud Gateway

`casdoor-springcloud-gateway-example`是一个示例，说明如何在Spring Cloud Gateway中使用`casdoor-spring-boot-starter`作为OAuth2插件。以下是使用它的步骤描述。

步骤1：部署Casdoor

首先，应部署Casdoor。您可以参考官方Casdoor文档中的[服务器安装](#)。请在[生产模式](#)中部署您的Casdoor实例。

成功部署后，您需要确保以下内容：

- 打开你最喜欢的浏览器，访问 <http://localhost:8000>。您将看到Casdoor的登录页面。
- 输入 `admin` 和 `123` 来测试登录功能是否正常工作。

之后，您可以按照以下步骤在您自己的应用中快速实现基于Casdoor的登录页面。

步骤2：初始化一个Spring Cloud Gateway

您可以直接使用此示例中的代码，或将其与您自己的业务代码结合使用。

您需要一个网关服务和至少一个业务服务。在这个例子中，`casdoor-gateway` 是网关服务，`casdoor-api` 是业务服务。

步骤3：包含依赖项

将 `casdoor-spring-boot-starter` 依赖项添加到您的 Spring Cloud Gateway 项目中。

对于Apache Maven:

```
/casdoor-gateway/pom.xml
```

```
<!-- https://mvnrepository.com/artifact/org.casbin/casdoor-spring-boot-starter -->
<dependency>
    <groupId>org.casbin</groupId>
    <artifactId>casdoor-spring-boot-starter</artifactId>
    <version>1.x.y</version>
</dependency>
```

对于Gradle:

```
// https://mvnrepository.com/artifact/org.casbin/casdoor-spring-boot-starter
implementation group: 'org.casbin', name: 'casdoor-spring-boot-starter', version: '1.x.y'
```

步骤4：配置您的属性

初始化需要6个参数，所有这些参数都是字符串类型。

名称(按顺序排列)	需要	描述
endpoint	是	Casdoor 服务器 URL, 例如 <code>http://localhost:8000</code>
clientId	是	Application.client_id
clientSecret	是	Application.client_secret
certificate	是	Application.certificate
organizationName	是	Application.organization
applicationName	否	Application.name

您可以使用Java属性或YAML文件来初始化这些参数。

对于属性:

```
casdoor.endpoint=http://localhost:8000
casdoor.clientId=<client-id>
casdoor.clientSecret=<client-secret>
casdoor.certificate=<certificate>
casdoor.organizationName=built-in
casdoor.applicationName=app-built-in
```

对于YAML:

```
casdoor:
  endpoint: http://localhost:8000
```

此外，您还需要配置网关路由。对于YAML：

```
spring:
  application:
    name: casdoor-gateway
  cloud:
    gateway:
      routes:
        - id: api-route
          uri: http://localhost:9091
          predicates:
            - Path=/api/**
```

步骤5：添加CasdoorAuthFilter

在网关中添加GlobalFilter接口的实现类，用于身份验证，例如本例中使用的CasdoorAuthFilter。

如果身份验证失败，它将返回401状态码给前端，以重定向他们到登录界面。

```
@Component
public class CasdoorAuthFilter implements GlobalFilter, Ordered {

  private static final Logger LOGGER =
LoggerFactory.getLogger(CasdoorAuthFilter.class);

  @Override public int getOrder() {
    return 0;
  }

  @Override public Mono<Void> filter(ServerWebExchange exchange,
GatewayFilterChain chain) {
    return exchange.getSession().flatMap(webSession -> {
      CasdoorUser user =
```

步骤6：获取服务并使用它

现在提供5项服务：`CasdoorAuthService`, `CasdoorUserService`,
`CasdoorEmailService`, `CasdoorSmsService`, 以及`CasdoorResourceService`。

您可以在Gateway项目中按照以下方式创建它们。

```
@Resource  
private CasdoorAuthService casdoorAuthService;
```

当你需要身份验证来访问你的应用时，你可以发送目标URL并重定向到Casdoor提供的登录页面。

请确保您已经提前在应用程序配置中添加了回调URL（例如，<http://localhost:9090/callback>）。

```
@RequestMapping("login")  
public Mono<String> login() {  
    return Mono.just("redirect:" +  
        casdoorAuthService.getSignInUrl("http://localhost:9090/callback"));  
}
```

在Casdoor成功验证后，它将带着代码和状态被重定向回您的应用程序。您可以获取代码并调用`getOAuthToken`方法来解析出JWT令牌。

`CasdoorUser`包含了Casdoor提供的用户基本信息。您可以将其用作关键字，以在您的应用程序中设置会话。

```
@RequestMapping("callback")  
public Mono<String> callback(String code, String state,
```

以下是API的示例。

- CasdoorAuthService

- `String token = casdoorAuthService.getOAuthToken(code, "app-built-in");`
- `CasdoorUser casdoorUser = casdoorAuthService.parseJwtToken(token);`

- CasdoorUserService

- `CasdoorUser casdoorUser = casdoorUserService.getUser("admin");`
- `CasdoorUser casdoorUser = casdoorUserService.getUserByEmail("admin@example.com");`
- `CasdoorUser[] casdoorUsers = casdoorUserService.getUsers();`
- `CasdoorUser[] casdoorUsers = casdoorUserService.getSortedUsers("created_time", 5);`
- `int count = casdoorUserService.getUserCount("0");`
- `CasdoorResponse response = casdoorUserService.addUser(user);`
- `CasdoorResponse response = casdoorUserService.updateUser(user);`
- `CasdoorResponse response = casdoorUserService.deleteUser(user);`

- CasdoorEmailService

- `CasdoorResponse response = casdoorEmailService.sendEmail(title, content, sender, receiver);`

- CasdoorSmsService

- `CasdoorResponse response = casdoorSmsService.sendSms(randomCode(), receiver);`

- CasdoorResourceService

- `CasdoorResponse response = casdoorResourceService.uploadResource(user, tag, parent,`

```
fullFilePath, file);  
◦ CasdoorResponse response =  
casdoorResourceService.deleteResource(file.getName());
```

步骤7：重启项目

启动项目后，打开你最喜欢的浏览器并访问 <http://localhost:9090>。然后点击任何请求来自 `casdoor-api` 的资源的按钮。



Casdoor

[Get Resource](#)

[Update Resource](#)

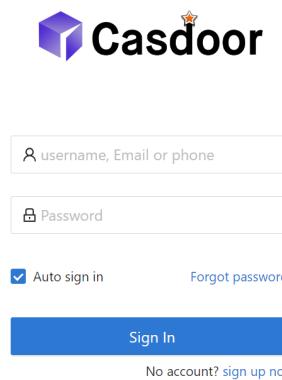
将触发网关认证逻辑。由于您尚未登录，您将被重定向到登录界面。点击登录按钮。



Click to login

Login

随后您可以看到Cassdoor统一的登录平台。



成功登录后，您将被重定向到主界面。现在你可以点击任何按钮。



Casdoor

[Get Resource](#)

[Update Resource](#)

"success get resource1"

更多内容

您可以探索以下项目/文件来了解更多关于Java与Casdoor一体化的信息。

- [casdoor-java-sdk](#)
- [casdoor-spring-boot-starter](#)
- [casdoor-spring-boot-example](#)
- [casdoor-spring-security-example](#)
- [casdoor-spring-security-react-example](#)
- [casdoor-spring-boot-shiro-example](#)
- [casdoor-springcloud-gateway-example](#)

Spring 安全

Spring Security OAuth

以Spring Security为例，演示如何使用OIDC连接到您的应用程序

使用OIDC集成的Spring Security过滤器与Casdoor

本文解释了如何使用Spring Security过滤器通过OIDC将您的应用程序与Casdoor连接。

Spring Security OAuth

Casdoor可以使用OIDC协议作为IDP连接各种应用程序。 在本指南中，我们将以Spring Security为例，向您展示如何使用OIDC连接到您的应用程序。

步骤1：部署Casdoor

首先，您需要部署Casdoor。

您可以参考Casdoor 官方文档 [Server Installation](#)。

成功部署Casdoor后，请确保：

- Casdoor服务器正在`http://localhost:8000`上运行。
- 打开您喜欢的浏览器并访问`http://localhost:7001`，您将看到Casdoor的登录页面。
- 通过输入 `admin` 和 `123` 来验证登录功能是否正常工作。

现在，您可以按照以下步骤在自己的应用中快速实现基于Casdoor的登录页面。

步骤2。配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序或使用现有的一个。
2. 添加您的重定向URL（您可以在下一节中找到如何获取重定向URL的更多详细信息）。 ``

The screenshot shows the Casdoor configuration interface for a client application. It includes fields for Client ID (24a25ea0714d92e78595), Client secret (155...), and Redirect URLs (http://localhost:8082/ui-one/login/oauth2/code/custom). A red box highlights the Client ID and Client Secret fields.

Client ID ② :	24a25ea0714d92e78595	Client ID
Client secret ② :	155...	Client Secret
Redirect URLs ② :	Redirect URLs Add	
Redirect URL Add a redirect URL for spring security		
http://localhost:8082/ui-one/login/oauth2/code/custom		

3. 添加所需的提供者并填写任何其他设置。

在应用设置页面上，您将找到两个值：`Client ID` 和 `Client secret`，如上图所示。我们将在下一步中使用这些值。

打开您喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME/.well-known/openid-configuration`。在这里，您将找到Casdoor的OIDC配置。

步骤3。 配置Spring Security

Spring Security原生支持OIDC。

您可以自定义Spring Security OAuth2 客户端的设置：

⚠ 注意事项

您应该用您自己的 Casdoor 实例替换配置，特别是 `<Client ID>` 等。

`application.yml` `application.properties`

```
spring:
  security:
    oauth2:
      client:
        registration:
          casdoor:
            client-id: <Client ID>
            client-secret: <Client Secret>
            scope: <Scope>
            authorization-grant-type: authorization_code
            redirect-uri: <Redirect URL>
        provider:
          casdoor:
            authorization-uri: http://CASDOOR_HOSTNAME:7001/login/oauth/
      authorize
        token-uri: http://CASDOOR_HOSTNAME:8000/api/login/oauth/
      access_token
        user-info-uri: http://CASDOOR_HOSTNAME:8000/api/get-account
```

```
spring.security.oauth2.client.registration.casdoor.client-id=<Client ID>
spring.security.oauth2.client.registration.casdoor.client-secret=<Client Secret>
spring.security.oauth2.client.registration.casdoor.scope=<Scope>
spring.security.oauth2.client.registration.casdoor.authorization-grant-type=authorization_code
spring.security.oauth2.client.registration.casdoor.redirect-uri=<Redirect URL>

spring.security.oauth2.client.provider.casdoor.authorization-uri=http://CASDOOR_HOSTNAME:7001/login/oauth/authorize
spring.security.oauth2.client.provider.casdoor.token-uri=http://CASDOOR_HOSTNAME:8000/api/login/oauth/access_token
spring.security.oauth2.client.provider.casdoor.user-info-uri=http://CASDOOR_HOSTNAME:8000/api/get-account
spring.security.oauth2.client.provider.casdoor.user-name-attribute=name
```

⚠ 注意事项

对于Spring Security的默认情况，`<Redirect URL>`应该像`http://<Your Spring Boot Application Endpoint>/<Servlet Prefix if it is configured>/login/oauth2/code/custom`这样。例如，对于下面的演示来说，重定向URL应该是`http://localhost:8080/login/oauth2/code/code/custom`。您也应该在`casdoor`应用程序中配置这个。

您还可以在代码中使用`ClientRegistration`来自定义设置。您可以在这里找到映射

步骤4：开始使用演示

1. 我们可以创建 Spring Boot 应用程序。
2. 我们可以添加一个配置，保护所有端点，除了`/`和`/login**`供用户登录。

```
@EnableWebSecurity
public class UiSecurityConfig extends WebSecurityConfigurerAdapter {

    @Override
```

3. 我们可以为用户添加一个简单的登录页面。

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Spring OAuth Client Thymeleaf - 1</title>
<link rel="stylesheet"
      href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/
bootstrap.min.css" />
</head>
<body>
<nav
    class="navbar navbar-expand-lg navbar-light bg-light shadow-sm
p-3 mb-5">
    <a class="navbar-brand" th:href="@{/foos/}">Spring OAuth Client
        Thymeleaf - 1</a>
</nav>
<div class="container">
    <label>Welcome!</label> <br /> <a th:href="@{/foos/}"
        class="btn btn-primary">Login</a>
</div>
</body>
</html>
```

当用户点击 `login` 按钮时，他们将被重定向到 `casdoor`。

4. 接下来，我们可以定义我们的受保护资源。我们可以公开一个名为 `/foos` 的端点和一个用于显示的网页。

数据模型

```
public class FooModel {
    private Long id;
    private String name;

    public FooModel(Long id, String name) {
        super();
        this.id = id;
        this.name = name;
```

控制器

```
@Controller
public class FooClientController {
    @GetMapping("/foos")
    public String getFoos(Model model) {
        List<FooModel> foos = new ArrayList<>();
        foos.add(new FooModel(1L, "a"));
        foos.add(new FooModel(2L, "b"));
        foos.add(new FooModel(3L, "c"));
        model.addAttribute("foos", foos);
        return "foos";
    }
}
```

网页

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Spring OAuth Client Thymeleaf - 1</title>
<link rel="stylesheet"
      href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/
bootstrap.min.css" />
</head>
<body>
    <nav
        class="navbar navbar-expand-lg navbar-light bg-light shadow-sm
p-3 mb-5">
        <a class="navbar-brand" th:href="@{/foos/}">Spring OAuth Client
            Thymeleaf - 1</a>
        <ul class="navbar-nav ml-auto">
            <li class="navbar-text">Hi, <span
sec:authentication="name">preferred_username</span>&ampnbsp&ampnbsp&ampnbsp</li>
        </ul>
    </nav>
    <div class="container">
        <h1>All Foos:</h1>
        <table class="table table-bordered table-striped">
            <thead>
```

⚠ 注意事项

所有的网页模板都应该放在 `resources/templates` 下。

步骤5：试试演示！

首先，您可以尝试打开您喜欢的浏览器并直接访问 `/foos`。它将自动将您重定向到Casdoor的登录页面。您可以在那里登录或从根页面登录。

如果您访问您的根页面，您将看到Casdoor应用设置。` ` `

Spring OAuth Client Thymeleaf - 1

Welcome !
[Login](#)

点击 `Login` 按钮，页面将重定向您到Casdoor的登录页面。



username, Email or phone

Password

Auto sign in [Forgot password?](#)

[Sign In](#)

[Sign in with code](#) No account? [sign up now](#)

登录后，页面将重定向您到 </foos>。

Spring OAuth Client Thymeleaf -1

Hi,

Your Username

All Foos:

ID	Name
1	a
2	b
3	c

使用OIDC集成的Spring Security过滤器与Casdoor

Casdoor是一个支持OIDC和各种其他协议的开源IDP。在本文中，我们将看到如何使用Spring Security过滤器和OIDC将Casdoor与您的应用程序集成。

步骤1：部署Casdoor

首先，你需要部署Casdoor服务器。参考[官方文档](#)以获取服务器安装指南。部署成功后，确保：

- Casdoor服务器正在`http://localhost:8000`运行。
- 你可以在`http://localhost:7001`看到Casdoor登录页面。
- 你可以通过使用凭证 `admin` 和 `123` 来测试登录功能。

验证这些步骤后，按照下面的步骤将Casdoor与您的应用程序集成。

步骤2：配置Casdoor应用程序

- 创建一个新的Casdoor应用程序或使用现有的一个。
- 添加你的重定向URL。你可以在下一节中找到更多关于获取重定向URL的信息。

Name [?](#) : application_a6ftas → your application name

Display name [?](#) : New Application - a6ftas

Logo [?](#) : URL [?](#) : https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home [?](#) :

Description [?](#) :

Organization [?](#) : organization_carg1b → your organization name

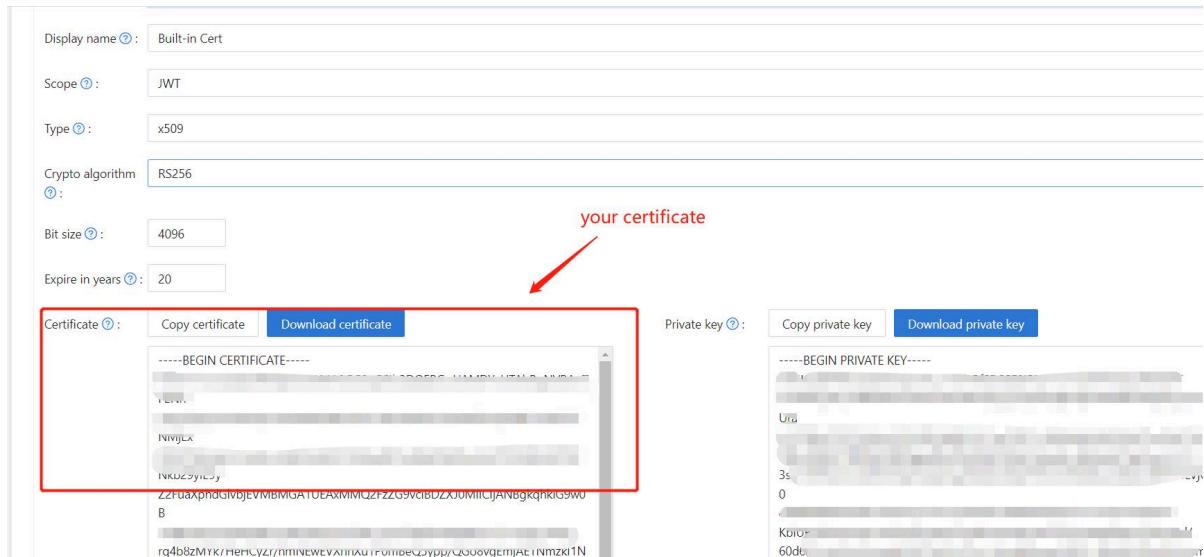
Client ID [?](#) : 3ed7314825ecf955cb19 → your client id

Client secret [?](#) : ee9314ea228 → your client secret

Cert [?](#) : cert-built-in

Redirect URLs [?](#) : Redirect URLs [Add](#)
Redirect URL [?](#) : <http://localhost:3000/callback> → your redirect url

- 在证书编辑页面上获取你的 Certificate。



- 根据需要添加提供商和其他设置。

你可以在应用程序设置页面上获取 Application Name、Organization Name、Redirect URL、Client ID、Client Secret 和 Certificate 的值。我们将在下一步中使用它们。

步骤3：配置Spring Security

你可以自定义Spring Security过滤器的设置来处理令牌：

⚠ 注意事项

确保你用你自己的Casdoor实例替换配置值，特别是 <Client ID> 和其他。

```
server:
  port: 8080
casdoor:
  endpoint: http://CASDOOR_HOSTNAME:8000
  client-id: <Client ID>
  client-secret: <Client Secret>
  certificate: <Certificate>
  organization-name: <Organization Name>
  application-name: <Application Name>
```

⚠ 注意事项

对于前端应用程序来说，`<FRONTEND_HOSTNAME>` 的默认值是 `localhost:3000`。在这个演示中，重定向URL是 `http://localhost:3000/callback`。确保在你的 `casdoor` 应用程序中配置这个。

步骤4：配置前端

你需要安装 `casdoor-js-sdk` 并按照以下方式配置SDK：

1. 安装 `casdoor-js-sdk`。

```
npm i casdoor-js-sdk
# or
yarn add casdoor-js-sdk
```

2. 设置 `SDK`。

```
import Sdk from "casdoor-js-sdk";

// Serverurl is the URL where spring security is deployed
export const ServerUrl = "http://BACKEND_HOSTNAME:8080";

const sdkConfig = {
  serverUrl: "http://CASDOOR_HOSTNAME:8000",
  clientId: "<your client id>",
  appName: "<your application name>",
  organizationName: "<your organization name>",
  redirectPath: "/callback",
};

export const CasdoorSDK = new Sdk(sdkConfig);
```

步骤5：设置演示

1. 创建一个Spring Boot应用程序。
2. 添加一些配置来处理JWT。

```
@EnableWebSecurity
public class SecurityConfig {

    private final JwtTokenFilter jwtTokenFilter;

    public SecurityConfig(JwtTokenFilter jwtTokenFilter) {
        this.jwtTokenFilter = jwtTokenFilter;
    }

    @Bean
    public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {
        // 启用CORS并禁用CSRF
        http = http.cors(corsConfig -> corsConfig
            .configurationSource(configurationSource())
            .csrf().disable());

        // 将会话管理设置为无状态
        http = http
            .sessionManagement()

        .sessionCreationPolicy(SessionCreationPolicy.STATELESS)
            .and();

        // 在端点上设置权限
        http.authorizeHttpRequests(authorize -> authorize
            .mvcMatchers("/api/redirect-url", "/api/signin").permitAll()
            .mvcMatchers("/api/**").authenticated()
        );

        // 设置未经授权的请求异常处理程序
    }
}
```

3. 添加一个简单的JWT过滤器来拦截需要令牌验证的请求。

```
@Component
public class JwtTokenFilter extends OncePerRequestFilter {

    private final CasdoorAuthService casdoorAuthService;

    public JwtTokenFilter(CasdoorAuthService casdoorAuthService) {
        this.casdoorAuthService = casdoorAuthService;
    }

    @Override
    protected void doFilterInternal(HttpServletRequest request,
                                    HttpServletResponse response,
                                    FilterChain chain)
        throws ServletException, IOException {
        // 获取授权头并验证
        final String header =
request.getHeader(HttpHeaders.AUTHORIZATION);
        if (!StringUtils.hasText(header) ||
!header.startsWith("Bearer ")) {
            chain.doFilter(request, response);
            return;
        }

        // 获取jwt令牌并验证
        final String token = header.split(" ")[1].trim();

        // 获取用户身份并将其设置在spring security上下文中
        UserDetails userDetails = null;
        try {
            CasdoorUser casdoorUser =
casdoorAuthService.parseJwtToken(token);
            userDetails = new CustomUserDetails(casdoorUser);
        } catch (CasdoorAuthException exception) {
            logger.error("casdoor auth exception", exception);
            chain.doFilter(request, response);
            return;
        }
    }
}
```

当用户访问需要身份验证的接口时，`JwtTokenFilter` 将从请求头`Authorization` 获取令牌并验证。

4. 定义一个`Controller` 来处理用户登录 Casdoor 时的情况。 用户登录后，他们将被重定向到服务器并携带`code` 和 `state`。 然后服务器需要从 Casdoor 验证用户的身份，并通过这两个参数获取`token`。

```
@RestController
public class UserController {

    private static final Logger logger =
LoggerFactory.getLogger(UserController.class);

    private final CasdoorAuthService casdoorAuthService;

    // ...

    @PostMapping("/api/signin")
    public Result signin(@RequestParam("code") String code,
@RequestParam("state") String state) {
        try {
            String token = casdoorAuthService.getOAuthToken(code,
state);
            return Result.success(token);
        } catch (CasdoorAuthException exception) {
            logger.error("casdoor auth exception", exception);
            return Result.failure(exception.getMessage());
        }
    }

    // ...
}
```

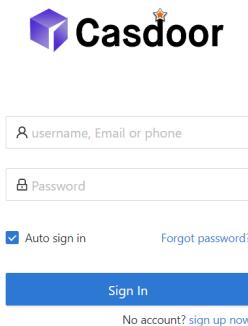
步骤6：尝试演示

你可以通过浏览器访问前端应用程序。 如果你没有登录，你会看到一个登录按钮。 点击它，你将被重定向到 Casdoor 登录页面。

如果你访问你的根页面，

[Casdoor Login](#)

点击 [Casdoor Login](#) 按钮，页面将重定向到 Casdoor 的登录页面。



Made with ❤ by [Casdoor](#)

登录后，你将被重定向到 [/](#)。



New User - rtsbx4

[Logout](#)

Jenkins 插件

Casdoor 提供了一个插件，允许用户登录到 Jenkins。在这里，我们将向您展示如何使用 Casdoor 插件进行 Jenkins 安全。

以下是一些配置设置：

`CASDOOR_HOSTNAME`：部署 Casdoor 服务器的域名或 IP。

`JENKINS_HOSTNAME`：部署 Jenkins 的域名或 IP。

步骤 1：部署 Casdoor 和 Jenkins

首先，部署 Casdoor 和 Jenkins。

成功部署后，请确保以下内容：

- 将 Jenkins URL（管理 Jenkins → 配置系统 → Jenkins 位置）设置为

`JENKINS_HOSTNAME`。

The screenshot shows the Jenkins configuration interface. In the 'Jenkins Location' section, the 'Jenkins URL' field contains the value `http://10.144.125.123:6780`, which is highlighted with a red box. Below it, the 'System Admin e-mail address' field contains the placeholder `address not configured yet <nobody@nowhere>`. In the 'Global properties' section, there is a checkbox for 'Environment variables'. At the bottom, there are 'Save' and 'Apply' buttons.

2. 验证 Casdoor 可以正常登录和使用。
3. 将 Casdoor 的 `origin` 值 (`conf/app.conf`) 设置为 `CASDOOR_HOSTNAME`。

```
conf > ⚙ app.conf
  8  dbName = casdoor
  9  redisEndpoint =
10  defaultStorageProvider =
11  isCloudIntranet = false
12  authState = "casdoor"
13  httpProxy = "127.0.0.1:10808"
14  verificationCodeTimeout = 10
15  initScore = 2000
16  logPostOnly = true
17  origin = "http://10.144.1.2:8000" | CASDOOR_HOSTNAME
```

步骤 2：配置 Casdoor 应用

1. 创建一个新的 Casdoor 应用或使用现有的一个。
2. 添加一个重定向 URL: `http://JENKINS_HOSTNAME/securityRealm/finishLogin`

The screenshot shows the Casdoor application configuration interface. A new client is being added with the following details:

- Description:** Casdoor for Jenkins
- Organization:** built-in
- Client ID:** bbd0bd66696e504dec59
- Client secret:** d2de01b01...110b47465c
- Redirect URLs:** `http://10.144.125.123:6780/securityRealm/finishLogin` (highlighted with a red box)

Below the client configuration, there is a note: `Add a redirect url for Jenkins JENKINS HOSTNAME`.

3. 添加所需的提供商并提供任何额外的设置。

在应用设置页面上，您会找到两个值：`Client ID` 和 `Client secret`，如上图所示。我们将在下一步中使用这些值。

打开您喜欢的浏览器，访问 `http://CASDOOR_HOSTNAME/.well-known/openid-configuration`，查看 Casdoor 的 OIDC 配置。

步骤 3：配置 Jenkins

现在，您可以从市场安装 Casdoor 插件，或者通过上传其 `jar` 文件。

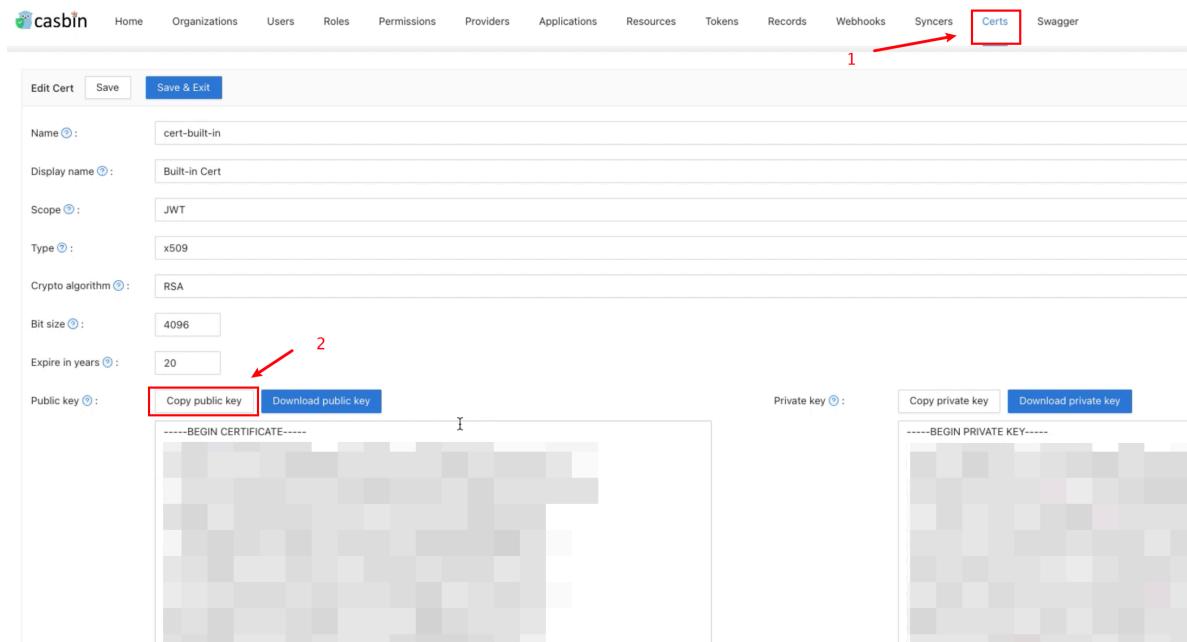
安装完成后，转到管理 Jenkins → 配置全局安全。

建议：备份 Jenkins `config.xml` 文件，并在设置错误的情况下用于恢复。

The screenshot shows the Jenkins 'Configure Global Security' page. Under the 'Authentication' section, the 'Casdoor Authentication Plugin' is selected. In the 'Security Realm' section, the 'Casdoor Endpoint' field is filled with 'http://CASDOOR_HOSTNAME'. Below it, the 'Client ID' and 'Client Secret' fields are empty and marked as required. The 'JWT Public Key' field is also empty and marked as required. At the bottom, there are 'Save' and 'Apply' buttons, and an 'Advanced...' link.

1. 在安全领域部分，选择 "Casdoor 认证插件"。
2. 在 Casdoor 端点字段中，输入前面提到的 `CASDOOR_HOSTNAME`。
3. 在 Client ID 字段中，输入前面提到的 `Client ID`。

4. 在 Client secret 字段中，输入前面提到的 `client secret`。
5. 在 JWT 公钥字段中，提供用于验证 JWT 令牌的公钥。您可以通过点击 Casdoor 顶部的 `Cert` 找到公钥。点击您的应用上的 `edit` 后，您可以从以下页面复制公钥。



6. 组织名称和应用名称是可选的。您可以指定您的组织和应用来验证其他组织和应用中的用户。如果这些字段为空，插件将使用默认的组织和应用。
7. 在授权部分，选中 "已登录用户可以做任何事"。禁用 "允许匿名读取访问"。
8. 点击 `Save`。

Jenkins 现在将自动将您重定向到 Casdoor 进行身份验证。

Jenkins OIDC

Casdoor可以使用OIDC协议作为IDP连接各种应用。 在这个例子中，我们将使用Jenkins来演示如何使用OIDC连接到你的应用。

以下是配置中使用的一些名称：

- `CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。
- `JENKINS_HOSTNAME`：部署Jenkins的域名或IP。

步骤1：部署Casdoor和Jenkins

首先，部署Casdoor和Jenkins。

成功部署后，确保以下内容：

1. 将Jenkins URL（管理Jenkins → 配置系统 → Jenkins位置）设置为

`JENKINS_HOSTNAME`。

The screenshot shows the Jenkins configuration interface. In the 'Jenkins Location' section, the 'Jenkins URL' field contains the value `http://10.144.125.123:6780`, which is highlighted with a red box. Below it, the 'JENKINS_HOSTNAME' field is empty. In the 'Global properties' section, there is a checkbox for 'Environment variables'. At the bottom, there are 'Save' and 'Apply' buttons.

- 确保Casdoor可以正常登录和使用。
- 将Casdoor的origin值（conf/app.conf）设置为CASDOOR_HOSTNAME。

```
conf > ⚙ app.conf
 8  dbName = casdoor
 9  redisEndpoint =
10 defaultStorageProvider =
11 isCloudIntranet = false
12 authState = "casdoor"
13 httpProxy = "127.0.0.1:10808"
14 verificationCodeTimeout = 10
15 initScore = 2000
16 logPostOnly = true
17 | origin = "http://10.144.1.2:8000"
    CASDOOR_HOSTNAME
```

步骤2：配置Casdoor应用

- 创建一个新的Casdoor应用或使用现有的一个。
- 添加一个重定向URL：`http://JENKINS_HOSTNAME/securityRealm/finishLogin`

Client ID	bbd0bd66696e504dec59						
Client secret	d2de01b01...110b47465c						
Redirect URLs	<table border="1"><tr><td>Redirect URLs</td><td>Add</td></tr><tr><td>Redirect URL</td><td><code>http://10.144.125.123:6780/securityRealm/finishLogin</code></td></tr><tr><td></td><td>Add a redirect url for Jenkins</td></tr></table>	Redirect URLs	Add	Redirect URL	<code>http://10.144.125.123:6780/securityRealm/finishLogin</code>		Add a redirect url for Jenkins
Redirect URLs	Add						
Redirect URL	<code>http://10.144.125.123:6780/securityRealm/finishLogin</code>						
	Add a redirect url for Jenkins						
	JENKINS_HOSTNAME						

- 添加你想要的提供商，并提供任何额外的设置。

你将从应用设置页面获取两个值：`Client ID` 和 `Client secret`。我们将在下一步中使用这些值。

打开你最喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME/.well-known/openid-configuration` 查看 Casdoor 的 OIDC 配置。

步骤3：配置 Jenkins

首先，我们需要安装 [OpenId Connect Authentication](#)，因为 Jenkins 并不原生支持 OIDC。

安装完成后，转到管理 Jenkins → 配置全局安全。

The screenshot shows the Jenkins 'Manage Jenkins' interface. In the top-left corner, there's a navigation bar with 'Dashboard' and 'Manage Jenkins'. Below this, there are several sections: 'User List', 'Build History', and a red-bordered 'Manage Jenkins' button. To the right, there's a yellow banner with the text 'Building on the built-in node can be a security issue. You should set up distributed builds. See the documentation.' with three buttons: 'Set up agent', 'Set up cloud', and 'Dismiss'. Under the 'System Configuration' heading, there are four main items: 'Configure System' (with a gear icon), 'Global Tool Configuration' (with a wrench icon), 'Manage Plugins' (with a gear icon), and 'Manage Nodes and Clouds' (with a cloud icon). At the bottom, under the 'Security' heading, there are three items: 'Configure Global Security' (with a lock icon, also red-bordered), 'Manage Credentials' (with a key icon), and 'Configure Credential Providers' (with a gear icon).



确保备份 Jenkins 的 `config.xml` 文件，以防任何设置错误。

- 在访问控制中，选择 `使用 OpenId Connect 登录` 作为安全领域。

2. 在**Client ID**字段中指定上面记下的**Client ID**。
3. 在**Client secret**字段中指定上面记下的**Client secret**。
4. 在配置模式中，选择**自动配置**，并输入**http://CASDOOR_HOSTNAME/.well-known/openid-configuration**作为已知配置端点。

Security Realm

Delegate to servlet container ?

Jenkins' own user database ?

Login with Openid Connect Select this ?

Client id

Input your Client ID

Client secret

 Concealed ? Input your Client secret Change Password

Configuration mode

Automatic configuration ?

Well-known configuration endpoint ?

CASDOOR_HOSTNAME ?

Manual configuration ?

如果你的Casdoor是本地部署的，你可能需要选择**手动配置**并提供以下信息：

- 令牌服务器URL: **http://CASDOOR_HOSTNAME/api/login/oauth/access_token**
- 授权服务器URL: **http://CASDOOR_HOSTNAME/login/oauth/authorize**
- 用户信息服务器URL: **http://CASDOOR_HOSTNAME/api/get-account**
- 范围: **address phone openid profile offline_access email**

Configuration mode

Automatic configuration ?

Manual configuration ?

Token server url

CASDOOR_HOSTNAME ?

Authorization server url

?

Userinfo server url

?

Scopes

5. 点击高级设置并填写以下内容：

- 在用户名字段中，指定 `name`。
- 在全名字段中，指定 `displayName`。
- 在电子邮件字段中，指定 `email`。

The screenshot shows a configuration form with five input fields:

- User name field name: A text input field containing "name".
- Full name field name: A text input field containing "displayName".
- Email field name: A text input field containing "email".
- Groups field name: A text input field containing an empty string.
- Token Field Key To Check: A text input field containing an empty string.

6. 在**授权**部分，启用“已登录用户可以做任何事情”并禁用“允许匿名读取访问”。你可以稍后配置更复杂的授权，但现在，检查OpenID是否正常工作。

退出Jenkins，它应该将你重定向到Casdoor进行身份验证。

 username, Email or phone Password Auto sign in[Forgot password?](#)[Sign In](#)[Sign in with code](#) [No account? sign up now](#)

Jira

通过内置的SSO

使用OIDC协议作为IDP连接各种应用程序，如Jira

使用miniOrange插件

使用OIDC协议作为IDP连接casdoor和Jira

通过内置的SSO

这是连接Casdoor的免费方法，但您的网站必须使用HTTPS。

Casdoor可以使用OIDC协议作为IDP连接各种应用程序。这里有一个[Jira教程](#)。

以下是配置中的一些名称：

- `CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。
- `Jira_HOSTNAME`：部署Jira的域名或IP。

步骤1：部署Casdoor和Jira

首先，部署Casdoor和Jira。

成功部署后，请确保以下内容：

1. Casdoor可以正常登录和使用。
2. 在`prod`模式下部署Casdoor时，您可以将`CASDOOR_HOSTNAME`设置为`http://localhost:8000`。查看[生产模式](#)。

步骤2：配置Casdoor应用程序

1. 创建或使用现有的Casdoor应用程序。
2. 找到认证方法：

Jira Software

Administration

Applications Projects Issues Manage apps User management Latest upgrade report **System** 2

General configuration Find more admin tools Jira mobile app

SYSTEM SUPPORT System info Instrumentation Monitoring Database monitoring Integrity checker Logging and profiling Scheduler details Troubleshooting and support tools Clean up Audit log Clustering

SECURITY Project roles Global permissions Password Policy User sessions **Authentication methods**

<https://test.v2tl.com/plugins/servlet/applications/licenses>

Authentication methods

Manage how users authenticate. Save authentication configurations using SAML, OpenID Connect, or Crowd as the identity provider. [Learn more about using multiple identity providers.](#)

Make authentication safer

Authenticating with username and password is less secure than through single sign-on. Now that you've configured the latter, consider disabling product login form and basic authentication.

Communicate this change to your users.

[How to disable](#) · [Dismiss](#)

Login options

Name	Type	Last updated	Show on login page	Actions
Username and password	Product login form	Never	<input checked="" type="checkbox"/>	...
casdoor	OpenID Connect	25 April 2023 4:33 PM	<input checked="" type="checkbox"/>	...

Authentication on API calls

Allow basic authentication on API calls. You can use personal access tokens as a safer alternative method of authentication. See [Using personal access tokens](#).

3

3. 添加一个配置，并在认证方法中选择OpenID连接单点登录

Add new configuration

Name *

Use a unique name for this configuration.

Authentication method

OpenID Connect single sign-on



Users log in using OpenID Connect

4. 找到重定向URL:

Give these URLs to your identity provider

Redirect URL



Location where the client is sent to after successful account authentication.

5. 添加一个重定向URL:

The screenshot shows a configuration interface for a client application. It includes fields for 'Client ID' (642ec5d6779a2f0e879d), 'Client secret' (26cb47985c47ae3844580536ce2f59872969e109), 'Cert' (cert-built-in), and a 'Redirect URLs' section. The 'Redirect URLs' section contains a table with one entry: 'https://test.v2ti.com/plugins/servlet/oidc/callback'. There are buttons for 'Add' and 'Action' (with icons for up/down sorting and delete).

不出所料，您可以在应用设置页面上获取两个值：`Client ID` 和 `Client secret`，如上图所示。 我们将在下一步中使用它们。

打开您最喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME.well-known/openid-configuration`。 您将看到Casdoor的OIDC配置。

步骤3：配置Jira

1. 我们需要继续在Jira中配置我们的配置

Edit existing configuration

Name *

casdoor

Use a unique name for this configuration.

Authentication method

OpenID Connect single sign-on

Users log in using OpenID Connect

OpenID Connect settings

Issuer URL *

https://demo.casdoor.com

your casdoor url

The complete URL of the OpenID Provider. Needs to be unique.

Client ID *

642ec5d6779a2f0e879d

application client ID

The client identifier, as registered with the OpenID Provider.

Client secret *

.....

application client secret [Change](#)

Client secret is used in conjunction with the Client ID to authenticate the client application against the OpenID Provider.

Username mapping *

\${preferred_username}

Used to map IdP claims to the username, e.g. \${sub}

Additional scopes

phone ✕ email ✕ address ✕ profile ✕

✖ ▾

The default scope is 'openid'. Add more scopes if needed to obtain the username claim.

Redirect URL
 Copy it to casdoor

Location where the client is sent to after successful account authentication.

Initiate login URL

URL used for OpenID Provider-initiated login.

Additional settings
The authorization, token, and user info endpoints will be filled automatically if your Identity provider offers this option. If not, you will be asked to provide this information.

Fill the data automatically from my chosen identity provider.

JIT provisioning
Just-in-time user provisioning allows users to be created and updated automatically when they log in through SSO to Atlassian Data Center applications. [Learn more](#).

Create users on login to the application

OpenID Connect behaviour

Remember user logins
If checked, successful login history will be saved and users will be logged in automatically without the need for reauthentication.

Login page settings
Decide if the IdP should be visible on login page and customize what the user will see on the button.

Show IdP on the login page

Login button text *

The text is shown to the user on the login page. Remaining characters: 33.

Save configuration Cancel

2. 您可以稍后配置更复杂的授权。 现在，检查OpenID是否真的有效。

⚠ You have temporary access to administrative functions. [Drop access](#) if you no longer require it. For more information, refer to the [documentation](#).

Jira Software Dashboards ▼ Projects ▼ Issues ▼ Boards ▼ Plans ▼ Create

Search Jira admin

Administration Applications Projects Issues Manage apps User management Latest upgrade report System

General configuration

- Find more admin tools
- Jira mobile app

SYSTEM SUPPORT

- System info
- Instrumentation
- Monitoring
- Database monitoring
- Integrity checker
- Logging and profiling
- Scheduler details
- Troubleshooting and support tools
- Clean up
- Audit log
- Clustering

SECURITY

- Project roles
- Global permissions

Authentication methods

Manage how users authenticate. Save authentication configurations using SAML, OpenID Connect, or Crowd as the identity provider. [Learn more about using multiple identity providers.](#)

⚠ **Make authentication safer**

Authenticating with username and password is less secure than through single sign-on. Now that you've configured the latter, consider disabling product login form and basic authentication.

Communicate this change to your users.

[How to disable](#) - Dismiss

Login options

Name	Type	Last updated	Show on login page	Actions
Username and password	Product login form	Never	<input checked="" type="checkbox"/>	...
casdoor	OpenID Connect	26 April 2023 7:20 PM	<input checked="" type="checkbox"/>	...

Authentication on API calls

Allow basic authentication on API calls.

You can use personal access tokens as a safer alternative method of authentication. See [Using personal access tokens](#).

Add configuration

使用miniOrange插件

本教程解释如何使用miniOrange连接casdoor和Jira。

Casdoor可以使用OIDC协议作为IDP连接各种应用程序。你可以参考这个[Jira教程](#)以获取更多信息。

以下是配置中的一些重要名称：

`CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。

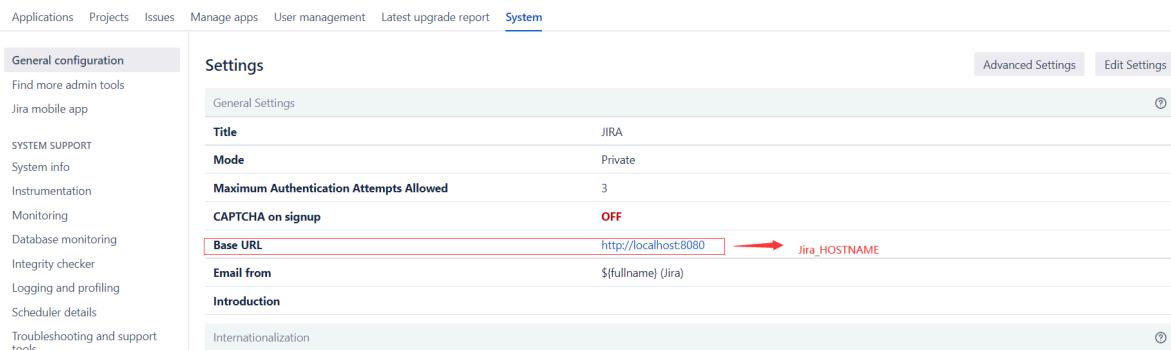
`Jira_HOSTNAME`：部署Jira的域名或IP。

步骤1：部署Casdoor和Jira

首先，部署Casdoor和Jira。

成功部署后，请确保：

- 将Jira URL（计划 → 管理 → 系统 → 通用配置）设置为 `Jira_HOSTNAME`。



The screenshot shows the Jira system settings page. On the left, there's a sidebar with links like Applications, Projects, Issues, Manage apps, User management, and Latest upgrade report. The main area has tabs for General configuration, System support, Monitoring, and Troubleshooting. The 'System' tab is selected. Under 'General configuration', there's a 'General Settings' section with fields for Title (set to JIRA), Mode (set to Private), Maximum Authentication Attempts Allowed (set to 3), CAPTCHA on signup (set to OFF), and Base URL (highlighted with a red box and a red arrow pointing to the placeholder \${fullname} (Jira)). Below that is an 'Email from' field set to \${fullname} (Jira). At the bottom, there's an 'Introduction' section and an 'Internationalization' section.

- Casdoor 可以正常登录使用。
- 当在 `prod` 模式下部署Casdoor时，你可以将 `CASDOOR_HOSTNAME` 设置为

<http://localhost:8000>。详见 [生产模式](#)。

步骤2：配置Casdoor应用程序和Jira

1. 创建一个新的Casdoor应用程序或使用现有的一个。
2. 安装[miniOrange](#)应用程序以支持OAuth。你可以在计划→管理→查找新应用→搜索中找到这个应用程序

The screenshot shows the Jira Administration interface. The top navigation bar includes 'Administration', 'Search Jira admin', 'Applications', 'Projects', 'Issues', 'Manage apps' (which is highlighted), 'User management', 'Latest upgrade report', and 'System'. On the left, there's a sidebar with 'ATLASSIAN MARKETPLACE' and a 'Find new apps' button. The main content area displays the 'Atlassian Marketplace for JIRA' search results for 'Oauth'. A red arrow points to the 'Find new apps' button. Another red arrow points to the 'Manage apps' tab in the top navigation. A third red arrow points to the 'Oauth' search term in the search bar. The results show an app named 'mO Jira OAuth SSO, Jira OpenID Connect SSO, Jira OIDC SSO' by 'miniOrange'. This app has a rating of ★★★★ (56), 607 installations, and is categorized under 'ADMIN TOOLS', 'INTEGRATIONS', 'JIRA SERVICE DESK', 'JIRA SOFTWARE', 'SECURITY', and 'UTILITIES'. A red arrow points to the app title.

3. 将 [Selected Application](#) 设置为Custom OpenId。
4. 找到重定向URL：

The screenshot shows the 'miniOrange OAuth Configuration' page. The top navigation bar includes 'Manage apps', 'Ask Us On Forum', and 'Frequently Asked Questions'. Below is a 'OAuth/OIDC Configurations' section. A red arrow points to the 'OAuth/OIDC Configurations' link. Another red arrow points to the 'Callback URL' field, which contains the value 'http://localhost:8080/plugins/servlet/oauth/callback'.

5. 添加重定向URL：

6. 按以下方式配置应用程序：

Selected Application: **Custom Openid**

Provider ID: **5c881c25-2e02-42c9-af06-0a71e0beb516**

Custom App Name: casdoor

Client Id: **514e09591ee5554b16fe**

Client Secret: **e7f05b14a68fb23e526f08515aefb73bbab7814a**

Scope: **openid email profile address phone offline_access**

Authorize Endpoint: **http://localhost:8000/login/oauth/authorize**

Access Token Endpoint: **http://localhost:8000/api/login/oauth/access_token**

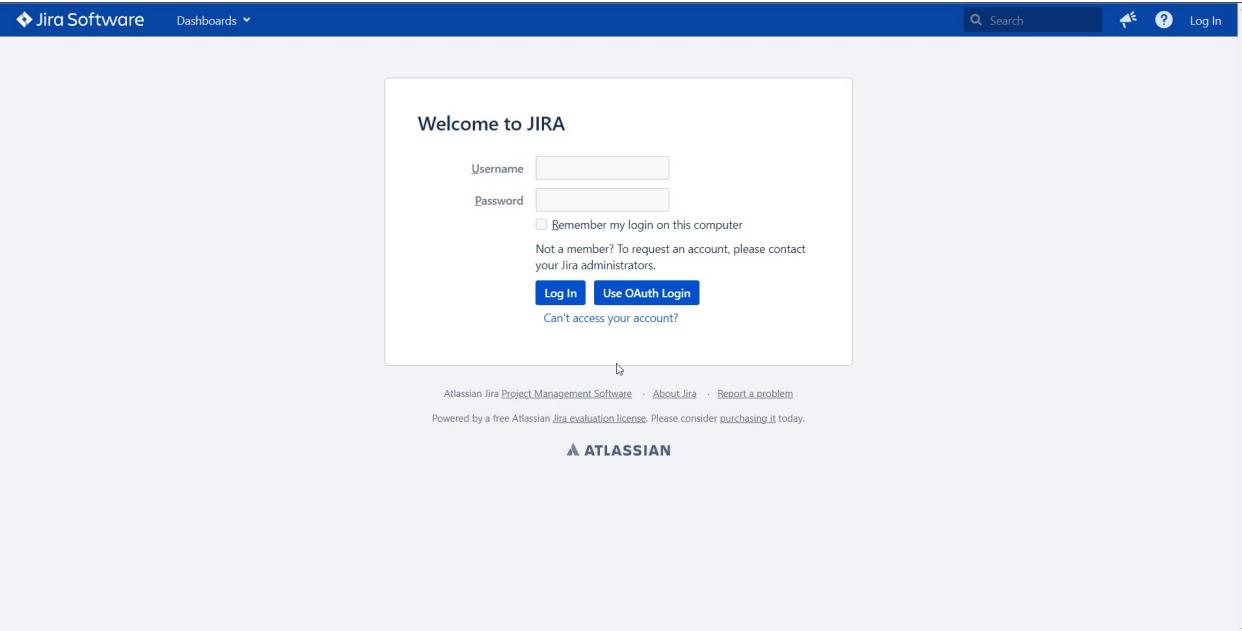
Logout Endpoint: Enter the Logout Endpoint URL

Save Test Configuration

- Token server URL: http://**CASDOOR_HOSTNAME**/api/login/oauth/**access_token**
- Authorization server URL: http://**CASDOOR_HOSTNAME**/login/oauth/**authorize**
- UserInfo server URL: http://**CASDOOR_HOSTNAME**/api/get-account
- Scopes: **address phone openid profile offline_access email**

打开你最喜欢的浏览器并访问: http://**CASDOOR_HOSTNAME**.well-known/openid-configuration。你将看到Casdoor的OIDC配置。

退出Jira并测试SSO。



使用OIDC协议连接应用程序 - Confluence

Casdoor可以使用OIDC协议作为IDP连接各种应用程序。在本指南中，我们将使用Confluence作为示例，演示如何使用OIDC连接您的应用程序。

首先，确保您已成功部署Casdoor和Confluence。以下是您需要记住的一些配置名称：

- `CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。
- `Confluence_HOSTNAME`：部署Confluence的域名或IP。

步骤1：部署Casdoor和Confluence

首先，部署Casdoor和Confluence。

成功部署后，请确保以下内容：

1. 将Confluence URL设置为`Confluence_HOSTNAME`。

The screenshot shows the 'General Configuration' section of the Confluence administration interface. On the left, a sidebar lists various configuration options. The 'General Configuration' option is highlighted with a blue arrow pointing to it. The main content area is titled 'General Configuration' and contains a 'Site Configuration' section. Under 'Site Configuration', there is a 'Server Base URL' field set to 'http://localhost:8090'. A blue arrow points to this field.

2. Casdoor可以正常登录和使用。
3. 如果您在 prod 模式下部署Casdoor，可以将 CASDOOR_HOSTNAME 设置为 `http://localhost:8000`。有关更多详细信息，请参阅[生产模式](#)。

步骤2：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序或使用现有的一个。
2. 找到一个重定向URL：

The screenshot shows the 'OAuth/OIDC Configurations' page. At the top, there is a 'Back to common setting' button. Below it, the title 'OAuth/OIDC Configurations' is displayed. A 'Callback URL' field contains the value 'http://localhost:8090/plugins/servlet/oauth/callback'. A blue arrow points to this field.

3. 将重定向URL添加到应用程序中：

The screenshot shows the 'OAuth/OIDC Configurations' page with several input fields.
 - 'Client ID' field: '01ae4bd048734ca2dea' (with a blue arrow pointing to it).
 - 'Client secret' field: 'f26a4115725867b7bb7b668c81e1f8f7fae1544d' (with a blue arrow pointing to it).
 - 'Cert' field: 'cert-built-in'.
 - 'Redirect URLs' section: It has an 'Add' button and a list containing the URL 'http://localhost:8090/plugins/servlet/oauth/callback' (with a blue arrow pointing to it).

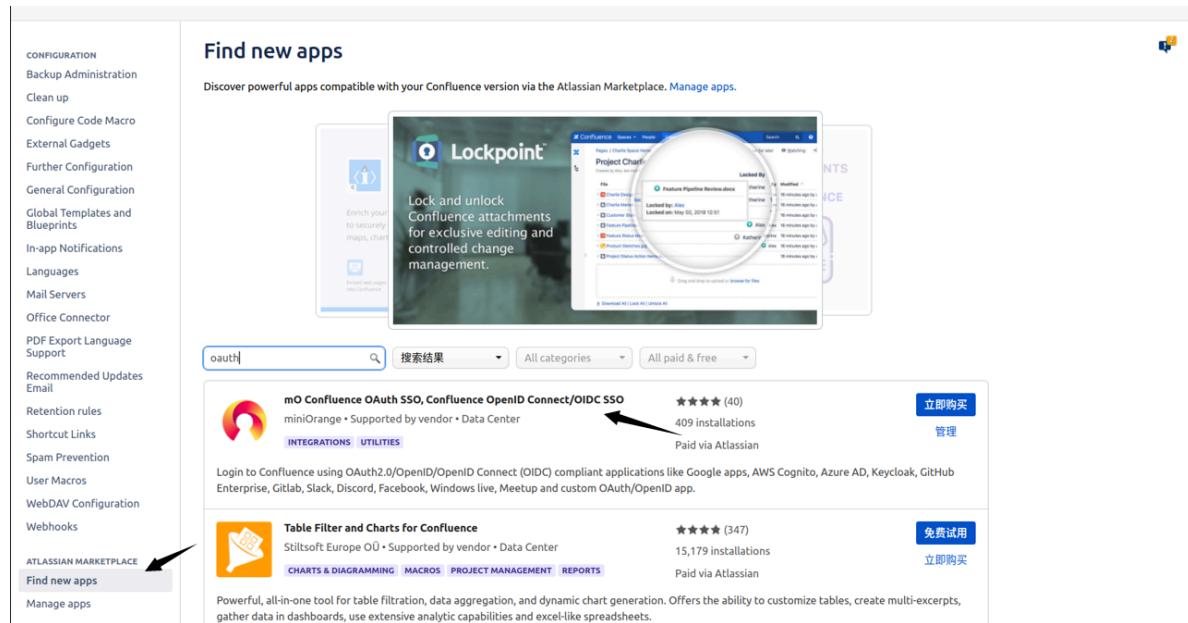
4. 添加所需的提供者并相应地配置其他设置。

在应用程序设置页面上，您将找到两个值：`Client ID`和`Client Secret`。我们将在下一步中需要这些。

打开您喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME/.well-known/openid-configuration`以查看Casdoor的OIDC配置。

步骤3：配置Confluence

1. 安装[miniOrange](#)应用程序以支持OAuth。 您可以在以下位置找到此应用程序：



The screenshot shows the Confluence Configuration interface. On the left, there's a sidebar with various configuration options like 'Backup Administration', 'External Gadgets', and 'Find new apps'. A red arrow points from the text 'Find new apps' to this sidebar item. The main area is titled 'Find new apps' and contains a search bar with 'oauth' typed in. Below the search bar, there are two app cards. The first card is for 'Lockpoint', which is described as 'Lock and unlock Confluence attachments for exclusive editing and controlled change management.' The second card is for 'mO Confluence OAuth SSO, Confluence OpenID Connect/OIDC SSO', developed by miniOrange. This card includes a star rating of 4.0 (40 reviews), 409 installations, and a 'Buy Now' button. A black arrow points from the text '立即购买' (Buy Now) to this button.

2. 配置应用程序：

Selected Application:	Custom OpenId	Import Details	Setup Guide
Provider ID:	4f6b30c1-eba8-4b89-ac02-4a4b7a137b97		
Custom App Name: [*]	Casdoor SSO		
Client Id: [*]	014ae4bd048734ca2dea		
Client Secret: [*]	f26a4115725867b7bb7b668c81e1f8f7fae1544d		
Scope: [*]	openid profile email		
Authorize Endpoint: [*]	https://door.casdoor.com/login/oauth/authorize		
Access Token Endpoint: [*]	https://door.casdoor.com/api/login/oauth/access_token		
Logout Endpoint:	Enter the Logout Endpoint URL		
<small>Enter the Logout endpoint of your OAuth/OpenID Provider. Leave blank if Logout endpoint not supported by provider. e.g. If Keycloak Logout endpoint is configured with {hostname}/auth/realm/{realm-name}/{protocol}/openid-connect/logout URL then on!</small>			

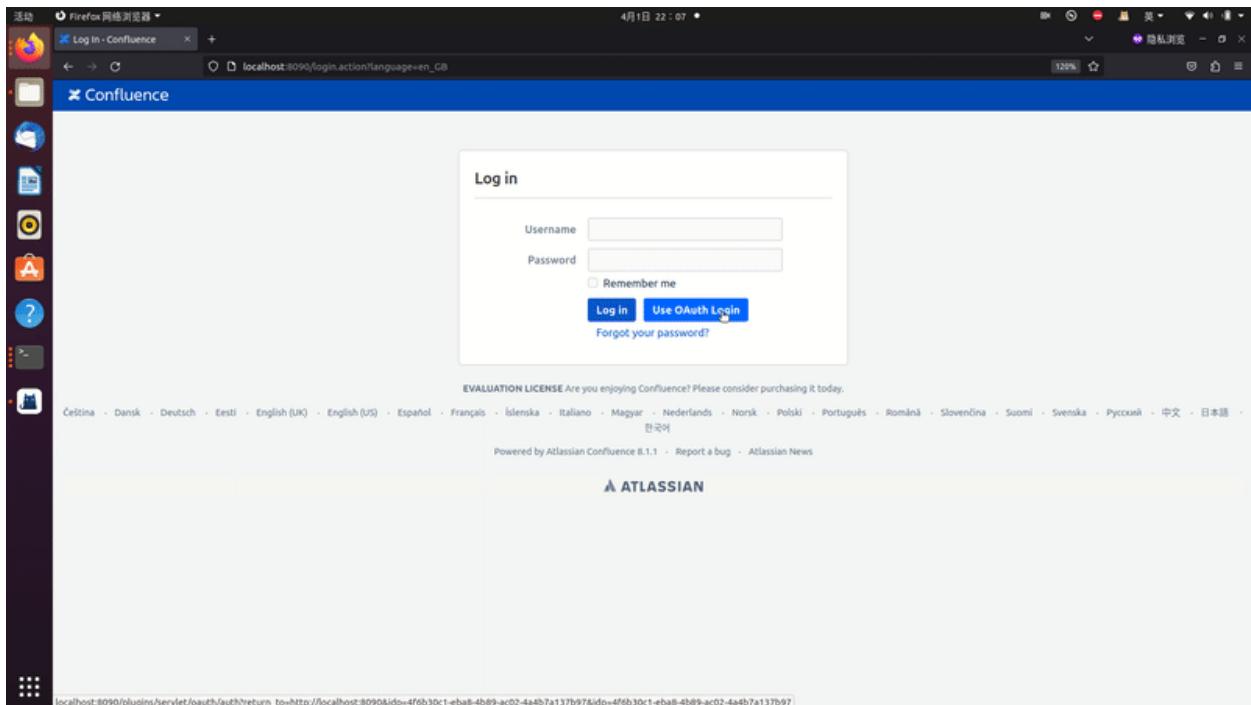
3. 将 Selected Application 设置为 Custom OpenID。
4. 从 Casdoor 应用程序页面获取 Client ID 和 Client Secret。

为 Confluence 配置以下设置：

- Token server URL : http://CASDOOR_HOSTNAME/api/login/oauth/access_token
- Authorization server URL : http://CASDOOR_HOSTNAME/login/oauth/authorize
- UserInfo server URL : http://CASDOOR_HOSTNAME/api/get-account
- Scopes : address phone openid profile offline_access email

您可以稍后配置更高级的授权设置。现在，检查 OpenID 是否真的有效。

退出 Confluence 并测试 SSO：



RuoYi

Casdoor可以轻松地与RuoYi-cloud集成。

步骤1：部署Casdoor

首先，部署Casdoor。

您可以参考Casdoor 官方文档 [Server Installation](#)。

部署成功后，请确保以下内容：

- Casdoor 服务器正在运行于 <http://localhost:8000>。
- 打开你最喜欢的浏览器，访问 <http://localhost:7001> 来访问Casdoor登录页面。
- 通过输入 `admin` 和 `123` 来测试登录功能。

接下来，你可以按照以下步骤在你自己的应用中快速实现一个基于Casdoor的登录页面。

步骤2：配置Casdoor

要配置Casdoor，请按照以下步骤操作：

1. 通过点击[这里](#)在浏览器中打开Casdoor。建议使用与您的开发浏览器不同的浏览器。
2. 在Casdoor中配置一个组织，一个应用程序和同步器。您可以在[这里](#)找到详细的操作指南。

以下是一些需要记住的额外要点：

1. 编辑同步器时，请务必检查表格列：

Table columns (3):	Add	Column name	Column type	Casdoor column	Is hashed	Action
		user_id	integer	Id	<input checked="" type="checkbox"/>	
		dept_id	integer	Affiliation	<input checked="" type="checkbox"/>	
		user_name	string	Name	<input checked="" type="checkbox"/>	
		nick_name	string	DisplayName	<input checked="" type="checkbox"/>	
		user_type	string	Type	<input checked="" type="checkbox"/>	
		email	string	Email	<input checked="" type="checkbox"/>	
		phonenumber	string	Phone	<input checked="" type="checkbox"/>	
		sex	string	Gender	<input checked="" type="checkbox"/>	
		avatar	string	Avatar	<input checked="" type="checkbox"/>	
		password	string	Password	<input checked="" type="checkbox"/>	
		del_flag	string	IsDeleted	<input checked="" type="checkbox"/>	
		login_ip	string	CreatedIp	<input checked="" type="checkbox"/>	
		create_time	string	CreatedTime	<input checked="" type="checkbox"/>	
		password	string	Password	<input checked="" type="checkbox"/>	

○

2. 在编辑组织时，确保选择正确的密码类型：

Password type (?:

○

3. 最后，确保你已启用软删除。

请确保仔细遵循这些指示，以正确配置Casdoor。

步骤3. 前端改造

3.1 跳转到Casdoor的登录页面

我们可以使用一个前端SDK，以vue-sdk为例。在你初始化 vue-sdk 之后，你可以通过使用 `getSignInUrl()` 函数来获取 Casdoor 登录页面的 URL。

您可以按照您喜欢的方式进行链接，并随时删除Ruoyi-Cloud中不再需要的任何原始代码，例如原始的账户和密码el-input。

3.2 接受Casdoor返回的代码和状态

通过Casdoor成功登录后，Casdoor会将代码和状态发送到我们设置的页面。我们可以使用create()函数来获取代码和状态。

```
created() {
    let url = window.document.location.href; // 获取URL
    let u = new URL(url);
    this.loginForm.code = u.searchParams.get('code'); // 获取code和
state
    this.loginForm.state = u.searchParams.get('state');
    if (this.loginForm.code != null && this.loginForm.state != null) { // 如果code和state不为null, 执行handleLogin
        this.handleLogin();
    }
}
```

对于RuoYi-Cloud，我们只需修改其原来的发送账号和密码的方法，改为发送代码和状态。因此，变化仅在于与原始登录相关的发送到后端的内容。

步骤4：重构你的后端

4.1 接受前端返回的代码和状态

```
@PostMapping("login")
public R<?> callback(@RequestBody CodeBody code) {
    String token =
casdoorAuthService.getOAuthToken(code.getCode(), code.getState());
    CasdoorUser casdoorUser =
casdoorAuthService.parseJwtToken(token);
    如果 (casdoorUser.getName() != null) {
```

在这个方法中，我们使用了casdoor-SpringBoot-sdk方法，并对RuoYi-Cloud方法进行了轻微的修改。

例如，RuoYi-Cloud原始方法使用密码注册账户。我已将其更改为使用casdoorRegister方法注册账户。

我还添加了一个方法getUserByCasdoorName来检查账户是否存在，并将方法executeUserInfo更改为executeWithAccount以反映这一变化。

这是一个简单的修改，因为我们只需要删除检查密码的部分。

步骤5：总结

5.1 前端

- 需要移除现有的登录和注册页面。
- 此外，前端需要接受代码和状态参数，并将它们发送到后端。

5.2 后端

RuoYi后端已经实现了完善的登录和注册功能。我们只需要做一些小修改，这使得整个过程非常方便。

步骤6：详细步骤

1. 部署并配置Casdoor。确保为组织选择bcrypt密码类型，因为RuoYi-Cloud也使用bcrypt来处理密码。
2. 使用Casdoor同步器将数据库用户复制到您的Casdoor组织。这将把原始账户导入到Casdoor。

- 部署Casdoor后，对前端进行更改。禁用 RuoYi 检查代码。

```
// checkcode switch  
captchaEnabled: false,  
// register switch  
register: true,
```

请注意，RuoYi-Cloud的验证码需要再次在Nacos中禁用。另外，RuoYi-Cloud的注册功能需要通过设置`sys.account.registerUser`为`true`来启用。

- 为用户添加一个用Casdoor登录的按钮，并修改数据的`loginForm`。

```
</el-button>  
<a href="http://localhost:7001/login/oauth/authorize?client_id=d509b6b3edc8a3d4cce9&response_type=code&redirect_uri=http%3A%2F%2Flocalhost:7001/casdoor">casdoor</a>  
  
<el-form-item label="用户名" prop="username">  
    <el-input v-model="loginForm.username" placeholder="请输入用户名" type="text" style="width: 200px;"></el-input>  
</el-form-item>  
  
<el-form-item label="密码" prop="password">  
    <el-input v-model="loginForm.password" placeholder="请输入密码" type="password" style="width: 200px;"></el-input>  
</el-form-item>  
  
<el-form-item label="验证码" prop="checkcode">  
    <el-input v-model="loginForm.checkcode" type="text" style="width: 100px;"></el-input>  
    <img alt="验证码" style="vertical-align: middle; margin-left: 10px;">  
</el-form-item>  
  
<el-form-item>  
    <el-button type="primary" @click="handleLogin">登录</el-button>  
</el-form-item>
```

```
        loginForm: {  
            code: "",  
            state: ""  
        },
```

这里，我已经写下了URL，但你可以使用Casdoor-Vue-SDK或Casdoor-SpringBoot-SDK来获取它。

- 由于我们不再使用原始的登录方法，删除`cookie`和`checkcode`方法。

新的`created`函数应该如下所示：

```
created() {  
    let url = window.document.location.href; // 获取URL  
    let u = new URL(url);  
    this.loginForm.code = u.searchParams.get('code'); // 获取code和state  
    this.loginForm.state = u.searchParams.get('state');  
    if (this.loginForm.code != null && this.loginForm.state != null) { // 如果code和state不为null, 执行handleLogin  
        handleLogin();  
    }  
}
```

6. 事实上，我们只需要更改我们发送到后端的参数，并删除不必要的函数。不需要进行其他更改。

```
handleLogin() {
  console.log("进入handleLogin")
  this.$store.dispatch("Login", this.loginForm).then(() => {
    this.$router.push({ path: this.redirect || "/" }).catch(()=>{});
  }).catch(() => {
    this.loading = false;
    if (this.captchaEnabled) {
      this.getCode();
      console.log(this.getCode)
    }
  });
}
```

```
Login({ commit }, userInfo) {
  const code = userInfo.code
  const state = userInfo.state
  return new Promise((resolve, reject) => {
    login(code, state).then(res => {
      console.log("LOGIN")
      let data = res.data
      setToken(data.access_token)
      commit('SET_TOKEN', data.access_token)
      setExpiresIn(data.expires_in)
      commit('SET_EXPIRES_IN', data.expires_in)
      resolve()
    }).catch(error => {
      reject(error)
    })
  })
},
```

```
export function login(code, state) {
  return request({
    url: '/auth/login',
    headers: {
      isToken: false
    },
    method: 'post',
    data: {code, state}
  })
}
```

7. 在后端导入所需的依赖项。

pom.xml

```
<dependency>
  <groupId>org.casbin</groupId>
  <artifactId>casdoor-spring-boot-starter</artifactId>
  <version>1.2.0</version>
</dependency>
```

您还需要在资源文件中配置Casdoor。

8. 将回调函数定义为重定向函数。对 `sysLoginService` 中的一些方法进行更改。删除密码检查步骤，因为它不再需要。

```
@PostMapping("login")
public R<?> callback(@RequestBody CodeBody code) {
  // 定义一个带有code和state的CodeBody实体
  String token =
  casdoorAuthService.getOAuthToken(code.getCode(),
```

9. 向 `SysLoginService` 添加新方法。

```
public LoginUser casdoorLogin(String username) {
    R<LoginUser> userResult =
remoteUserService.getUserInfo(username,
SecurityConstants.INNER);
    // 执行用户
    if (R.FAIL == userResult.getCode()) {
        throw new ServiceException(userResult.getMsg());
    }

    if (StringUtils.isNull(userResult) ||
StringUtils.isNull(userResult.getData())) {
        recordLogService.recordLoginInfo(username,
Constants.LOGIN_FAIL, "该用户不存在");
        throw new ServiceException("用户 " + username + " 不存在");
    }
    LoginUser userInfo = userResult.getData();
    SysUser user = userResult.getData().getSysUser();
    if
(UserStatus.DELETED.getCode().equals(user.getDelFlag())) {
        recordLogService.recordLoginInfo(username,
Constants.LOGIN_FAIL, "对不起，您的账户已被删除");
        throw new ServiceException("对不起，您的账户 " + username
+ " 已被删除");
    }
    if (UserStatus.DISABLE.getCode().equals(user.getStatus()))
{
        recordLogService.recordLoginInfo(username,
Constants.LOGIN_FAIL, "您的账户已被禁用。请联系管理员");
        throw new ServiceException("对不起，您的账户 " + username
+ " 已被禁用");
    }
    recordLogService.recordLoginInfo(username,
Constants.LOGIN_SUCCESS, "登录成功");
    return userInfo;
}
```

```
public String getUserByCasdoorName(String casdoorUsername) {
    R<LoginUser> userResult =
    remoteUserService.getUserInfo(casdoorUsername,
    SecurityConstants.INNER);
    if (StringUtils.isNull(userResult) ||
    StringUtils.isNull(userResult.getData())) {
        // 如果用户不在Ruoyi-Cloud数据库中，但在Casdoor中存在，则在数
        // 据库中创建用户
        return null;
    }
    String username =
    userResult.getData().getSysUser().getUserName();
    return username;
}
```

```
public void casdoorRegister(String username) {
    if (StringUtils.isAnyBlank(username)) {
        throw new ServiceException("用户必须提供用户名");
    }
    SysUser sysUser = new SysUser();
    sysUser.setUserName(username);
    sysUser.setNickName(username);
    R<?> registerResult =
    remoteUserService.registerUserInfo(sysUser,
    SecurityConstants.INNER);
    System.out.println(registerResult);
    if (R.FAIL == registerResult.getCode()) {
        throw new ServiceException(registerResult.getMsg());
    }
    recordLogService.recordLogininfor(username,
    Constants.REGISTER, "注册成功");
}
```

Pulsar Manager

Casdoor 可以轻松连接到 Pulsar Manager。

连接 Casdoor 的代码已经添加到 Pulsar Manager 中，所以我们只需要在后端配置 `application.yml` 文件并启用前端开关。

步骤 1：部署 Casdoor

首先，部署 Casdoor。

您可以参考官方 Casdoor 文档中的 [服务器安装](#)。

部署成功后，请确保以下内容：

- Casdoor 服务器在 <http://localhost:8000> 成功运行。
- 打开您喜欢的浏览器并访问 <http://localhost:7001>。 您应该看到 Casdoor 的登录页面。
- 通过输入 `admin` 和 `123` 来测试登录功能。

现在，您可以使用以下步骤在您自己的应用中快速实现基于 Casdoor 的登录页面。

步骤 2：配置 Casdoor

要配置 Casdoor，请参考 [Casdoor](#)（建议使用与开发浏览器不同的浏览器）。

您还应该配置一个组织和一个应用。您可以参考 [Casdoor](#) 获取详细的操作指南。

步骤 2.1：创建一个组织

Edit Organization Save Save & Exit

Name ⓘ: pulsar

Display name ⓘ: pulsar

Favicon ⓘ: URL ⓘ: <https://cdn.casbin.org/img/favicon.png>

Preview: 

Website URL ⓘ: <http://localhost:9527/#/login?redirect=%2F>

Password type ⓘ: plain

Password salt ⓘ:

Phone prefix ⓘ: + 86

步骤 2.2：创建一个应用

Name ⓘ: app-pulsar

Display name ⓘ: app-pulsar

Logo ⓘ: URL ⓘ: https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home ⓘ: [/](#)

Description ⓘ:

Organization ⓘ: pulsar

Client ID ⓘ: 6ba06c1e1a30929fdda

Client secret ⓘ: df926bf913225ebbae9af7ba8d41fe19507eb079

Cert ⓘ: cert-built-in

Redirect URLs ⓘ: Add

Redirect URLs	Action
http://localhost:9527/callback	  

步骤 3：启用 Pulsar Manager 前端开关

启用此开关以将代码和状态发送到后端。

您可以在 `pulsar-manager/front-end/src/router/index.js` 的第 80 行找到该开关。

```
- // mode: 'history', // require service support
+ mode: 'history', // require service support
```

步骤 4：配置后端代码

在 `application.properties` 文件中配置 Casdoor 的设置，该文件可以在 `pulsar-manager/src/main/resources/application.properties` 的第 154 行找到。

```
casdoor.endpoint = http://localhost:8000
casdoor.clientId = <client id from previous step>
casdoor.clientSecret = <client secret from previous step>
casdoor.certificate = <client certificate from previous step>
casdoor.organizationName = pulsar
casdoor.applicationName = app-pulsar
```

在 ShenYu 中使用Cassoor

ShenYu有一个Casdoor插件，可以启用Casdoor的使用。

步骤1：部署Casdoor

首先，应部署Casdoor。您可以参考官方Casdoor文档的[服务器安装](#)。

成功部署后，请确保：

- Casdoor服务器正在<http://localhost:8000>上运行。
- 打开您喜欢的浏览器并访问<http://localhost:7001>以查看Casdoor登录页面。
- 通过输入admin和123，登录功能运行正常。

按照上述步骤，您可以通过以下步骤在您的应用中快速实现基于Casdoor的登录页面。

步骤2：配置Casdoor应用

1. 创建一个新的Casdoor应用或使用现有的一个
2. 添加您的重定向URL

Name : app-test → application name

Display name : app-test

Logo : 

Preview:

Home : →

Description :

Organization : built-in → organization name

Client ID : 663a84154e73d1fb156a → client id

Client secret : 84209d412a338a42b789c05a3446e623cb7262d → client secret

Cert : cert-built-in

Redirect URLs : Add

Redirect URL	Action
http://localhost:9195/http/hello → redirect url	[Delete]

3. 在证书编辑页面，您可以查看您的证书

Certificate : Copy certificate Download certificate

```
-----BEGIN CERTIFICATE-----
MIIE+TCCAUgBgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTABBgNVBAoTFENh
c2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENlcnQwHhcNMjEx
MDE1MDgxMTUyWhcNNDEXMDE1MDgxMTUyWjA2M0R0wGwYDVQQKExRDYXNkb29yIe9y
Z2FuaxphdGlvbjEVMBMGAEUEAxMMQ2FzZG9vcj8DZXj0MIIcjANBgkqhkiG9w0B
AQEFAAOCAg8AMiCgKCAGEAstnpb5E1/ymf0tRfSDSSE8IR7y+lw+RjIj74e5ej
rq4b8zMMyk7HeHCyZr/hmNewEVXnhXu1P0mBeQ5ypp/QGo8vgEmjAETNmzk1NjOQ
CjCYwUrasO/f/Mnl1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07
uvFMCJe5W8+0rKErZCKTR8+9VB3janeBz/zQePFvh79bfZate/hLirPK0Go9P1g
OvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRS8b/wUjNCUBD
PTSLVjC04WIIIf6Nkfx0Z7KvmbPstSj+btvqcsvRAGtvsB9h62Kptjs1Yn7GAuo
I3qt/4zoKbiURYxkQJXlvwCQsEftUuk5ew5zuPSIDRLoLByQTLbx0jqLAFNfW3g/
pzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4Gu
hRsnlsmkmUDeylZ9a8L9oj11YEQfM2JZEq+RvtUx+wB4y8K/tD1bcY+lfnG5rBpw
IDpS262boq4SRsvb3Z7bB0w4ZxvOfj/1VLoRftPbLifobhfr/AeZMHpiKOXvfz4
yE+hqzi6wdF0VR9xYc/RbSAf7323OsjYnjjEglnUtRohnRgCpjlk/Mt2Kt84Kb0
wn8CAwEAAaAMQMA4wDAYDVR0TAQH/BAlwADANBgkqhkiG9w0BAQsFAAOCAgEAn2lf
DKkLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgic4/LSdzuf4Awe6ve
C06lVdWSlis8UPUPdjmT2uMPSNjwLxG3QsrimMURNlwFLTfRem/heJe0Zgur9J1M
8haawdSdjH2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCvl
2nR42Fybap3O/g2JXMhNNRowZmNjgpsF7XVENCSuFO1jTywLaqjuXCg54lL7XVLG
omKNNNcc8h1FCelj/nbGMhodnFWKDTsJcbNmcOPNHo6ixzqMy/Hqc+mWv7maAG
Jtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisukftOPZgtH979XC4mdf0WPnOBLql
2DJ1zaBmjIGolvb7XNVKcUfdXYw85ZTQ5b9cli4e+6bmyWqQitlw+Ati/uFEV
Xzcj70B4IALX6xau1kLepV9O1GERizYrz5P9NJNA7Ko05AVMp9w0DQTkt+LbXnZE
HHnWKy8xHQKF9sR7YBPGLs/Ac6tviv5ua15Ogj/8dLRZ/veyFfGo2yZsl+hKVU5
nCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VYalWSalADosHAgMWFxFuWP+h
8XKXmzlxuHbTMQYtZPDgsps5aK+S4Q9wb8RRAYo=
-----END CERTIFICATE-----
```

步骤3：在ShenYu中使用Casdoor插件

1. 在ShenYu中配置Casdoor插件

Plugin

X

* Plugin: casdoor

casdoor Configuration

* application-name: app-test

* certificate: -----BEGIN CERTIFICATE-----\nMIIE+TCCAuGgAwI

* client_id: 6e3a84154e73d1fb156a

* client_secrect: a4209d412a33a842b7a9c05a3446e623cbb7262d

* casdoor endpoint: http://localhost:8000

* organization-name: test

* Role: Authentication

* Sort: 40

Status:

Cancel

Sure

注意：由于ShenYu只有一个单行输入框，每行证书都必须添加\n。

Certificate  :

[Copy certificate](#)

[Download certificate](#)

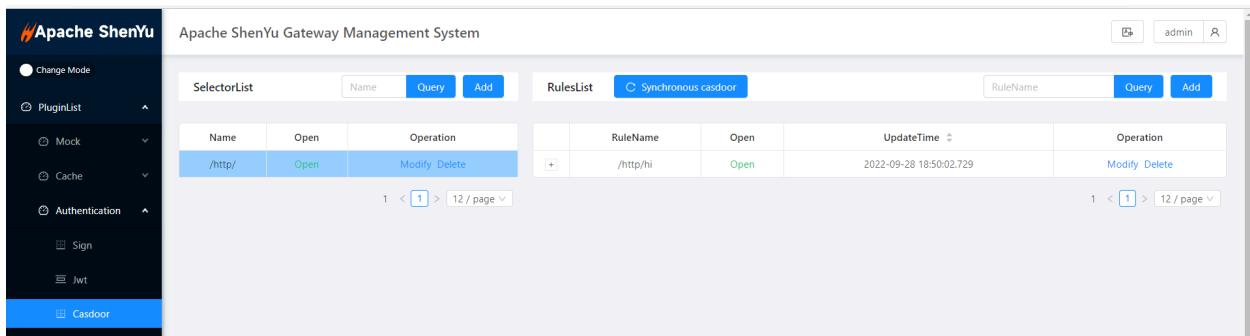
```
-----BEGIN CERTIFICATE-----\nMIIE+TCCAuGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENh\n\nc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENIcnQwHhcNMjEx\n\nc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENIcnQwHhcNMjEx\nMDE1MDgxMTUyWhcNNDEzMDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIE9y\nZ2FuaXphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vcibDZXJ0MIICljANBqkqkiG9w0B\nAQEFAOCAg8AMIICgKCAgEAsInpb5E1/yM0f1RfSDSSE8IR7y+lw+RJjl74e5ej\nrq4b8zMYk7HeHCyZr/hmNEwEVXnhXu1P0mB8eQ5yp/PGo8vgEmjaETNmzkl1NjOQ\nCjCYwUrasO/f/Mnl1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07\nuvFMCje5W8+0rKErZCKTR8+9VB3janeBz//zQePFVh79bFZate/hLirPK0Go9P1g\nOvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRSBb/wUjNCUBD\nPTSLVjC04WIISf6Nkfx0Z7KvmbPstSj+btvcqsvRAGtvdsB9h62Kptjs1Yn7GAuo\nl3qt/4zoKbiURYxkQJXlvwCQsEftUuk5ew5zuPSIDRLoLByQLbx0jqLAFnfW3g/\npzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMcdfx4Gu\nhRsnLsmkmUDeylZ9aBL9oj11YEQfM2JZEq+RVtUx+wB4y8K/tD1bcY+lfnG5rBpw\nIDpS262boq4SRVb3Z7b0w4ZxvOfj/1VLoRftjPbLlf0bhfr/AeZMHplKOXvfz4\nyE+hqzi68wdF0VR9xYc/RbSAf7323OsjYnjEgInUtRohnRgCpjlk/Mt2Kt84Kb0\nwn8CAwEAQMA4wDAYDVR0TAQH/BAIwADANBqkqkiG9w0BAQsFAAOCAgEAn2f\nDKkLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/Lsdzuf4Awe6ve\nC06IVdWSlis8UPUPdjmT2uMPSNjwLxG3QsrimMURNwFILTfRem/heJe0Zgur9J1M\n8haawdSdjH2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCvl\n2nR42Fyap3O/g2JXMhNNROwZmNjgpsF7XVENCSuFO1jTywLaqjuXCg54IL7XVLG\nomKNNNcc8h1FCeKj/nnbGMhodnFWKDTsJcbNmOPNHo6ixzqMy/Hqc+mWYv7maAG\nJtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisuKftOPZgtH979XC4mdf0WPnOBLql\n2DJ1zaBmjIGjolvb7XNVKcUfDXYw85TZQ5b9cl4e+6bmyWqQltlw+Ati/uFEV\nXzCj70B4IALX6xau1kLEpV9O1GERizYRz5P9NJNA7Ko5AVMp9w0DQTkt+LbXnZE\nHHnWKy8xHQKZF9sR7YPBGLs/Ac6tviv5ua15OgJ/8dLRZ/veyFfGo2yZsl+hKVU5\nnCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VyalWSalADosHAgMWfXuWP+h\n8XKXmzlxuHbTMQYtZPDgspS5aK+S4Q9wb8RRAYo=\n-----END CERTIFICATE-----
```

 here not need add \n

您可以复制它并粘贴到ShenYu Casdoor配置的证书中。

您不需要在Casdoor证书编辑页面保存它，因为它只是用于复制。

2. 配置ShenYu Casdoor插件



The screenshot shows the Apache ShenYu Gateway Management System interface. On the left, there's a sidebar with 'Change Mode' (radio button), 'PluginList' (dropdown), and several sub-options: 'Mock', 'Cache', 'Authentication' (with 'Sign' and 'Jwt' sub-options), and 'Casdoor' (which is selected and highlighted in blue). The main area has tabs: 'SelectorList' (selected) and 'RulesList'. Under 'RulesList', there's a sub-tab 'Synchronous casdoor'. Below these tabs is a search bar with 'RuleName' and buttons 'Query' and 'Add'. A table titled 'RulesList' displays one row of data:

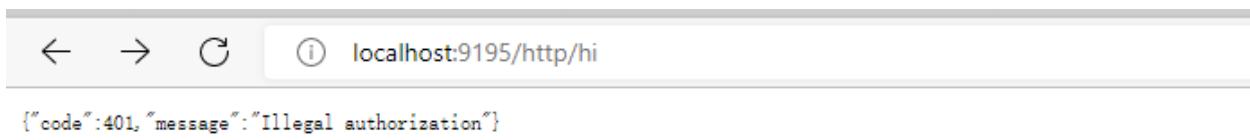
Name	Open	Operation	RuleName	Open	UpdateTime	Operation
/http/	Open	Modify Delete	/http/hi	Open	2022-09-28 10:50:02.729	Modify Delete

Pagination controls at the bottom show page 1 of 12.

您可以配置Casdoor配置所需的内容。

3. 获取服务并使用它

3.1 直接访问Web



The screenshot shows a browser window with the address bar containing 'localhost:9195/http/hi'. The page content is a JSON response: {"code":401, "message":"Illegal authorization"}

3.2 使用Casdoor登录

The screenshot shows a browser window with the URL `localhost:7001/login/oauth/authorize?client_id=6e3a84154e73d1fb156a&response_type=code&redirect_uri=http://localhost:9195/http/hi&scope=read&state=app-test`. The page displays the Casdoor logo and a "Continue with:" button next to a user icon labeled "admin (Admin)". Below this, there are fields for "username, Email or phone" and "Password". There are also links for "Auto sign in" (with a checked checkbox), "Forgot password?", and "Sign In". A small note at the bottom right says "No account? sign up now".

← ⌂ ⓘ localhost:9195/http/hi?code=822607b015cca2515b2b&state=app-test

hi! null! I'm Shenyu-Gateway System. Welcome!

3.3 在Headers中携带令牌

The screenshot shows the Postman application interface. At the top, there is a header bar with 'GET' and a dropdown menu. Below it, the URL 'http://localhost:9195/http/hi' is entered. On the right side of the header bar is a 'Send' button. The main area has tabs for 'Params', 'Authorization', 'Headers (8)', 'Body', 'Pre-request Script', 'Tests', and 'Settings'. The 'Headers (8)' tab is currently selected and underlined in red. A table below lists eight headers: 'Postman-Token', 'Host', 'User-Agent', 'Accept', 'Accept-Encoding', 'Connection', and 'Authorization'. The 'Authorization' row contains a value: 'eyJhbGciOiJSUzI1NjIwMjtpZCI6ImNlcnQtYn...'. A red arrow points from the text 'Your token' to this value. The 'Cookies' tab is also visible on the right. Below the table, there are tabs for 'Body', 'Cookies (1)', 'Headers (9)', and 'Test Results'. The 'Body' tab is selected. The response body is displayed as a single line of text: '1 hi! null! I'm Shenyu-Gateway System. Welcome!'. Above the response body, there is a status bar showing '200 OK', '27.76 s', and '337 B'. On the far right of the status bar is a 'Save Response' button with a dropdown arrow.

3.4 在Headers中保存名称、ID和组织

这使得将来使用它们更加方便。

ShardingSphere

shardingsphere-elasticsearch-ui已经集成了Casdoor。配置后即可使用。

步骤1：部署Casdoor

首先，应部署Casdoor。

您可以参考Casdoor 官方文档 [Server Installation](#)。

成功部署后，请确保：

- Casdoor服务器已成功运行在<http://localhost:8000>。
- 打开你最喜欢的浏览器并访问<http://localhost:7001>。你将看到Casdoor的登录页面。
- 输入 `admin` 和 `123` 来测试登录功能是否正常。

然后，你可以按照以下步骤在你自己的应用中快速实现基于Casdoor的登录页面。

步骤2：配置Casdoor应用并在ShardingSphere中配置应用

1. 创建或使用现有的Casdoor应用

填写表单并上传Casdoor logo

表单字段：

- Name: ShardingSphere
- Display name: ShardingSphere
- Logo URL: https://cdn.casbin.org/img/casdoor-logo_1185x256.png
- Home: (未输入)
- Description: (未输入)
- Organization: ShardingSphere
- Client ID: 3ed79fa530645fb0d3653
- Client secret: 54633c82b7796a4332c6976864c6c16bc3b05556
- Cert: cert-built-in
- Redirect URLs:
 - Add
 - Redirect URL: http://localhost:8080

预览效果：



说明：表单中所有带红色箭头的字段都是必填项。

RedirectURLs取决于你需要重定向到的URL。选中的数据将在下一步中使用。

2. 在证书编辑页面，你可以看到你的**Certificate**

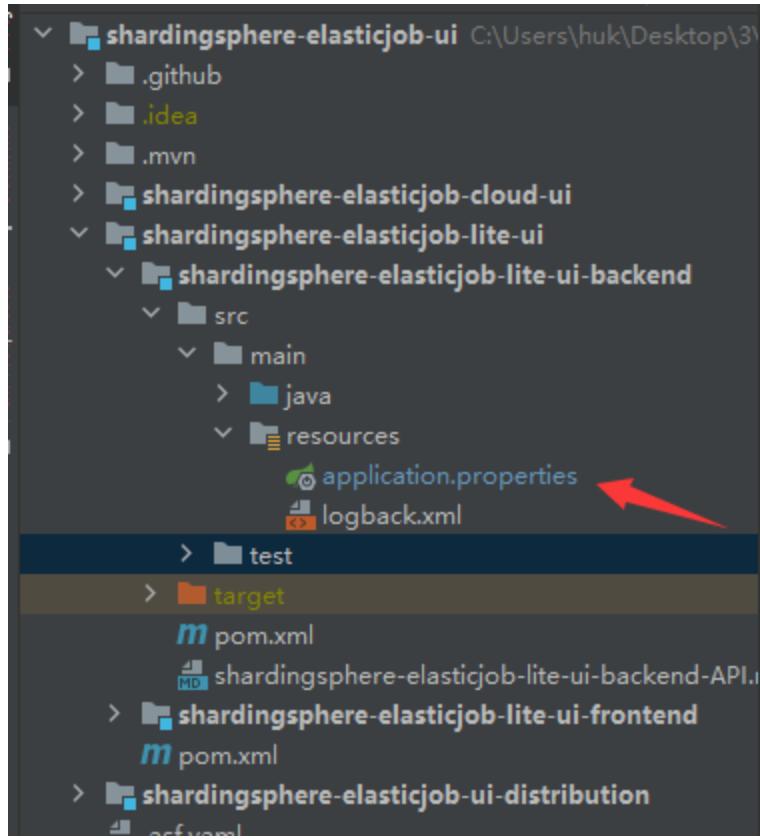
Certificate [?](#) : Private

[Copy certificate](#) [Download certificate](#)

-----BEGIN CERTIFICATE-----
MIIE+TCCAUgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENhc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENIcnQwHhcNMjExMDE1MDgxMTUyWhcNNDEmDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIE9yZ2FuaxphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vcibDZXJ0MIICjANBqkqhkiG9w0BAAQFAAOCAg8AMIIICgkCAGEAstnpb5E1/ym0f1RfSDSSE8IR7y+lw+Rjji74e5ejrq4b8zMYk7HeHCyZr/hmNEwEVXnhXu1P0mBeQ5ypp/QGo8vgEmjAETNmzkl1NjOQCjCYwUraso/f/Mn1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07uvFMCJe5W8+0rKErZCKTR8+9VB3janeBz/zQePFVh79bfZate/hLirPK0Go9P1gOvwloC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRSBb/wUjNCUBDPTSLvjC04WIISf6Nkf0Z7KvmbPstSj+btcqsvRAGtvdsB9h62Kptjs1Yn7GAuoI3qt/4zoKbiURYxkQJXlvwCQsEftUuk5ew5zuPSIDRLoLByQTLbx0jqLAFNfW3gpzSDjgd/60d6HTmvbZni4SmjdyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4GuhRsnLsmkmUDeylZ9aBL9oj11YEQfM2JZEq+RVtUx+wB4y8K/tD1bcY+lfnG5rBpwIDpS262boq4SRsvb3Z7bB0w4ZxvOfj/1VLoRftjPbLif0bhfr/AeZMHpIKOXvfz4yE+hqzi68wdF0VR9xYc/RbSAf7323OsjYnjEgInUtRohnRgCpjlk/Mt2Kt84Kb0wn8CAwEAAaMQMA4wDAYDVR0TAQH/BAIwADANBqkqhkiG9wOBAQsFAAOCAgEAn2IfDKkLX+F1vKRO+5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/Lsdzuf4Awe6veC06IVdWSlis8UPUPdmjT2uMPSNjwLxG3QsrimMURNwFILTfRem/heJe0Zgur9J1M8haawdSdjH2RgmFoDeE2r8NVRfhbR8KnCO1ddTJKuS1N0/irHz21W4jt4rxzCvl2nR42Fybab3O/g2JXMHNNR0wZmNjgpsf7XVENCSuFO1jTywLaqjuXCg54l7XVLGomKNNNCc8h1FCeKj/nnbGMhodnFWKDTsJcbNmcOPNHo6ixzqMy/Hqc+mWYv7maAGJtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisuKftOPZgtH979XC4mdf0WPnOBLql2DJ1za8mjigJolvb7XNVKcUfdXYw85ZTZQ5b9cl4e+6bmyWqQltwt+Ati/uFEVXzCj70B4IALX6xau1kLEpV9O1GERizYRz5P9NJNA7KoO5AVMp9w0DQTkt+LbXnZEHHnWKy8xHQKZF9sR7YBPGLs/Ac6tviv5Ua15OgJ/8dLRZ/veyFfGo2yZsl+hKVU5nCCJHBcAyFnm1hdvdwEdH33jDBjNB6ciotJZrf/3VYalWSalADosHAgMWfXuWP+h8XKXmzlkuHbTMQYtZPDgsps5aK+S4Q9wb8RRAYo=-----END CERTIFICATE-----

3. 在ShardingSphere中配置应用

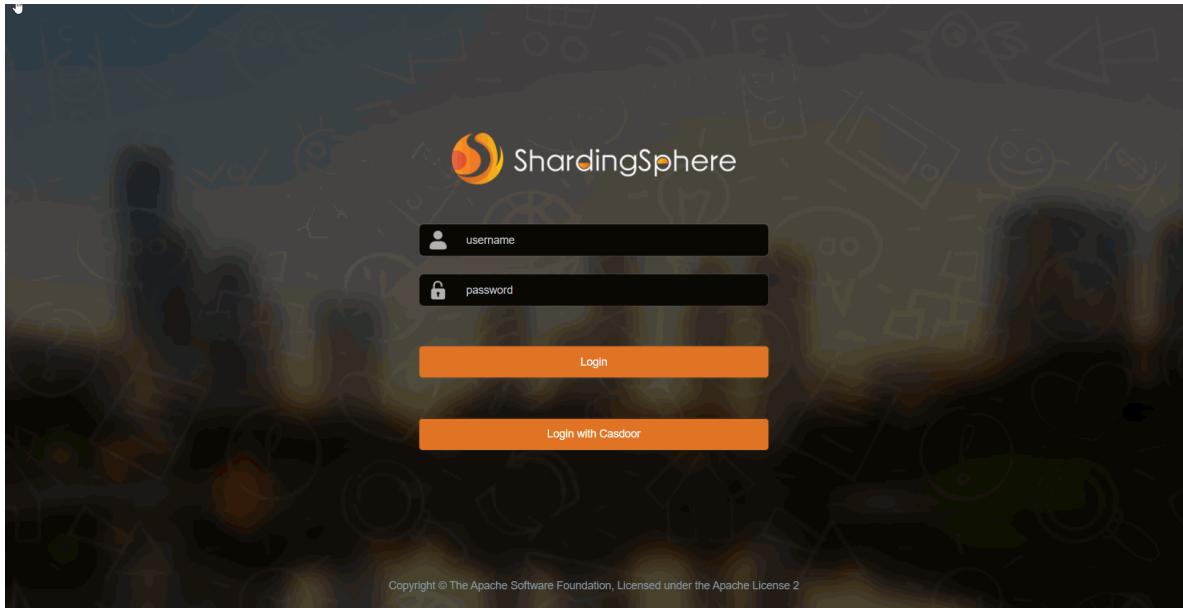
首先，我们需要找到我们需要配置的application.properties。



接下来，我们需要从Casdoor应用中复制数据并粘贴到应用中。

```
casdoor.endpoint=http://localhost:7001
casdoor.client-id=3ed79fa530645fdb3653
casdoor.client-secret=54633c82b7796a4332c6976864c6c16bc3b05556
casdoor.certificate=\n-----BEGIN CERTIFICATE-----\nMIIE+TCCAUgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMDYxHTAbBgNVBAoTFENh\n\nc2Rvb3IgT3JnYW5pemF0aW9uMRUwEwYDVQQDEwxDYXNkb29yIENlcnQwHhcNMjEx\n\MDExMDgxMTUyWhcNNDExMDE1MDgxMTUyWjA2MR0wGwYDVQQKExRDYXNkb29yIE9y\n\Z2FuaXphdGlvbjEVMBMGA1UEAxMMQ2FzZG9vcIBDZXJ0MIICIjANBgkqhkiG9w0B\n\AQEFFAOCAg8AMIIICgKCAGeAsInpb5E1/ym0f1RfSDSSE8IR7y+lw+RJjI74e5ej\n\rq4b8zMYk7HeHCyZr/hmNEwEVXnhXu1P0mBeQ5ypp/QGo8vgEmjAE TNmzkI1Nj0Q\n\AjCYwUras0/f/MnI1C0j13vx6mV1kHZjSrKsMhYY1vaxTEP3+VB8Hjg3MHFWrb07\n\uvFMCJe5W8+0rKErZCKTR8+9VB3janeBz//zQePFVh79bFZate/hLirPK0Go9P1g\n\OvwIoC1A3sarHTP4Qm/LQRt0rHqZFybdySpyWAQvhNaDFE7mTstRSBb/wUjNCUBD\n\PTSLvjC04W1lsf6Nufx0Z7KvmbPstSj+btvccsvRAGtvdsB9h62Kptjs1Yn7GAuo\n\I3qt/4zoKbiURYxkQJXIvwCQsEftUuk5ew5zuPS1DRLoLByQTLbx0JqLAFNfW3g/\n\pzSDjgd/60d6HTmvbZni4SmidyFhXCDb1Kn7N+xTojnfaNkwep2REV+RMc0fx4Gu\n\hRsnLsmkmUDeyIZ9aBL9oj1YEQfM2JZEq+RVtUx+wB4y8K/tD1bcY+IfnG5rBpw\n\IDpS262boq4SRSpb3Z7bB0w4Zxv0fJ/1VL0RftjPbLIf0bhfr/AeZMHpIK0Xvfz4\n\yE+hqzi68wdF0VR9xYc/RbSAf73230sjYnjjEgInUtRohnRgCpjIk/Mt2Kt84Kb0\n\wn8CAwEAaMQMA4wDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAgEAn2lf\n\DKkLX+F1vKRO/5gJ+Plr8P5NKuQkmwH97b8CS2gS1phDyNgIc4/LSdzuf4Awe6ve\n\CO6lVdWSIis8UPUPdjmt2uMPSNjwLxG3QsrimMURNwFLLTfRem/heJe0Zqur9J1M\n\8aaawdSdJjh2RgmFoDeE2r8NVRfhbR8KnC01ddTJKuS1N0/irHz21W4jt4rxzCvl\n\2nR42Fybap30/g2JXMhNNR0wZmNjgpsF7XVENCSuF01jTywLaqjuXcg54IL7XVLG\n\omKNNNcc8h1FCeKj/nnbGMhodnFWKDTsJcbNmcoPNHo6ixzqMy/Hqc+mWYv7maAG\n\Jtevs3qgMZ8F9Qzr3HpUc6R3ZYWDY/xxPisuKftOPZgtH979XC4mdf0WPn0BLql\n\2DJ1zaBmjiGJolyb7XNVKcUfDXYw85TZQ5b9clI4e+6bmyWqQItlw+Ati/uFEV\n\XzCj70B4lALX6xau1kEpV901GERizYRz5P9NJNA7Ko05AVMp9w0DQTkt+LbXnZE\n\HHnWKy8xHQKZF9sR7YBPGls/Ac6tviv5Ua150gJ/8dLRZ/veyFFGo2yZsI+hKVU5\n\ncCJHBcAyFnmlhdvdwEdH33jDBjNB6ciotJZrf/3VYaIWSalADosHAgMWfXuWP+h\n\8XKXmzlxuHbTMQYtZPDgspS5aK+S4Q9wb8RRAYo=\n-----END CERTIFICATE-----\ncasdoor.organization-name=ShardingSphere
casdoor.application-name=ShardingSphere
```

4. 测试一下



Apache IoTDB

Casdoor可以轻松连接到Apache IoTDB。

连接Casdoor的代码已经添加到Apache IoTDB Web Workbench中，所以我们只需要在后端配置application.yml文件并激活前端开关。

步骤1：部署Casdoor

首先，部署Casdoor。

您可以参考官方Casdoor文档中的服务器安装。

成功部署后，请确保：

- Casdoor服务器在<http://localhost:8000>成功运行。
- 打开您喜欢的浏览器并访问<http://localhost:7001>，您将看到Casdoor登录页面。
- 通过输入admin和123测试登录功能。

完成这些步骤后，您现在可以在您自己的应用中快速实现基于Casdoor的登录页面。

步骤2：配置Casdoor

要配置Casdoor，请参考[casdoor](#)（建议不要在您正在开发的浏览器中使用Casdoor的浏览器）。

您还应该创建一个组织和一个应用。参考[casdoor](#)进行操作。

2.1 创建一个组织

Name ⓘ: IoTDB

Display name ⓘ: IoTDB

Favicon ⓘ: URL ⓘ: <https://cdn.casbin.org/img/favicon.png>

Preview: 

Website URL ⓘ: <https://door.casdoor.com>

Password type ⓘ: plain

Password salt ⓘ:

2.2 创建一个应用

Name ⓘ: app_IoTDB

Display name ⓘ: app_IoTDB

Logo ⓘ: URL ⓘ: https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home ⓘ: [/](#)

Description ⓘ:

Organization ⓘ: built-in

Client ID ⓘ: 6f561b83d119be3e1e3c

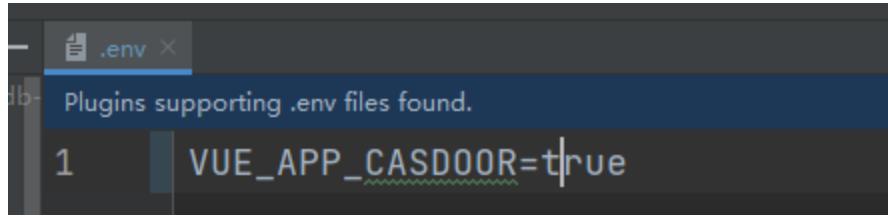
Client secret ⓘ: 242082e823b31a9b0d3a0a4a5a80cd5e415c75f7

Cert ⓘ: cert-built-in

步骤3：激活Apache IoTDB Web Workbench前端开关

打开此开关以将代码和状态发送到后端。

此开关可以在iotdb-web-workbench/fronted/.env文件中找到。



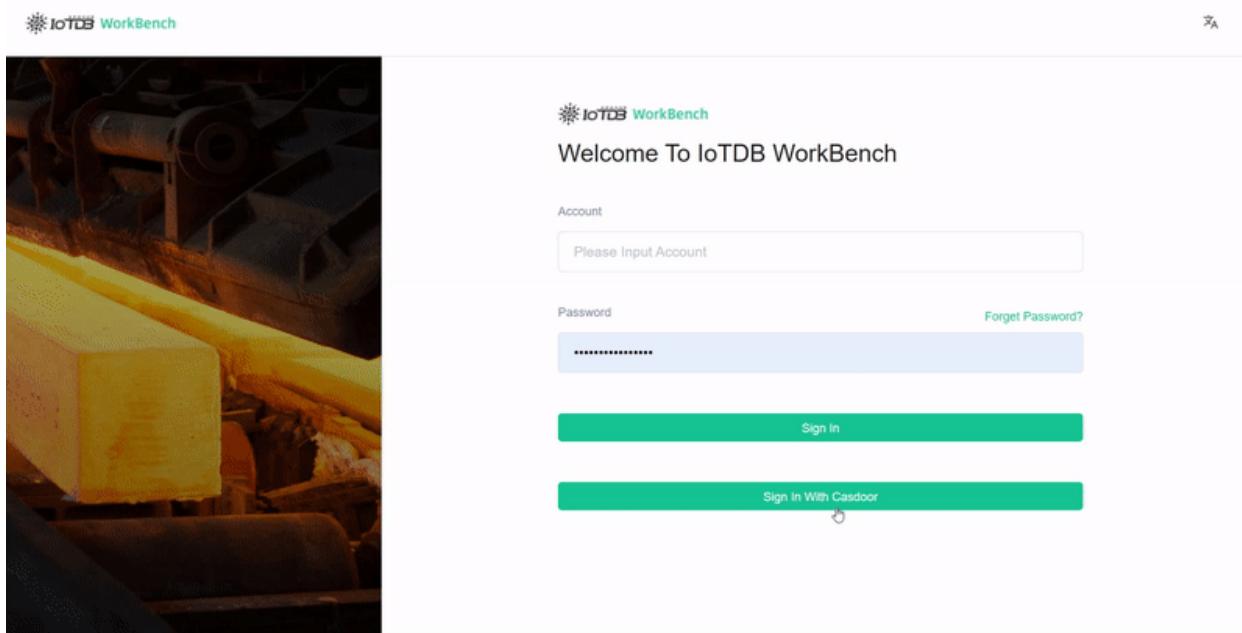
```
.env
Plugins supporting .env files found.
1 | VUE_APP_CASDOOR=true
```

步骤4：配置后端代码

您需要在iotdb-web-workbench/backend/src/main/resources/application.properties文件中配置Casdoor的设置。

```
casdoor.endpoint = http://localhost:8000
casdoor.clientId = <client id from previous step>
casdoor.clientSecret = <client secret from previous step>
casdoor.certificate=<client certificate from previous step>
casdoor.organizationName=IoTDB
casdoor.applicationName=app-IoTDB
```

结果



The image shows a composite view. On the left, there is a photograph of a large industrial machine, possibly a conveyor belt or a metalworking press, with a bright yellow component in the foreground. On the right, there is a screenshot of the IoTDB WorkBench login page. The page has a header with the IoTDB logo and "WorkBench". Below the header, it says "Welcome To IoTDB WorkBench". There are two input fields: "Account" with placeholder text "Please Input Account" and "Password" with placeholder text "*****". To the right of the password field is a "Forget Password?" link. Below the input fields are two buttons: a teal "Sign In" button and a green "Sign In With Casdoor" button with a small circular icon.

Apache DolphinScheduler

Casdoor是Apache DolphinScheduler支持的登录方式之一。

步骤1：部署Casdoor

首先，应部署Casdoor。您可以参考Casdoor官方文档的[服务器安装](#)。

成功部署后，请确保：

- Casdoor服务器在<http://localhost:8000>成功运行。
- 打开您喜欢的浏览器并访问<http://localhost:7001>。您将看到Casdoor的登录页面。
- 通过输入"admin"和"123"来测试登录功能。

部署完成后，您可以按照以下步骤在自己的应用中快速实现基于Casdoor的登录页面。

步骤2：配置Casdoor应用

1. 创建一个新的Casdoor应用或使用现有的一个。
2. 添加您的重定向URL（您可以在下一节中找到更多关于如何获取重定向URL的详细信息）。

Name ② : application_a6ftas → your application name

Display name ② : New Application - a6ftas

Logo ② : URL ② : https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home ② :

Description ② :

Organization ② : organization_carg1b → your organization name

Client ID ② : 3ed7314825ecf955cb19 → your client id

Client secret ② : ee9314ea228... → your client secret

Cert ② : cert-built-in

Redirect URLs ② : Redirect URLs Add
Redirect URL <http://localhost:3000/callback> → your redirect url

3. 添加所需的提供商并填写其他必要的设置。

在应用设置页面上，您将找到两个重要的值：`Client ID` 和 `Client secret`，如上图所示。我们将在下一步中使用这些值。

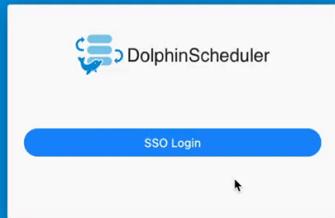
打开您喜欢的浏览器并访问`http://CASDOOR_HOSTNAME/.well-known/openid-configuration`以查看Casdoor的OIDC配置。

步骤3：配置DolphinScheduler

dolphinscheduler-api/src/main/resources/application.yaml

```
security:
  authentication:
    # Authentication types (supported types: PASSWORD, LDAP,
    CASDOOR_SSO)
    type: CASDOOR_SSO
  casdoor:
    # The URL of your Casdoor server
    endpoint:
    client-id:
    client-secret:
    # The certificate may be multi-line; you can use `|-` for ease
    certificate:
    # The organization name you added in Casdoor
    organization-name:
    # The application name you added in Casdoor
    application-name:
    # The DolphinScheduler login URL
    redirect-url: http://localhost:5173/login
```

现在，DolphinScheduler将自动将您重定向到Casdoor进行身份验证。



FireZone

Casdoor可以使用OIDC协议作为IDP连接各种应用。 在这里，我们将使用FireZone作为例子，向您展示如何使用OIDC连接到您的应用。

步骤1：部署Casdoor和FireZone

首先，应部署Casdoor和FireZone。

成功部署后，请确保以下内容：

1. 将FireZone URL (Signin → Security → Add OpenID Connect Provider) 设置为 FIREZONE_HOSTNAME。

The screenshot shows the Firezone configuration interface. On the left is a sidebar with navigation links: Configuration (Users, Devices, Rules), Settings (Defaults, Account, Customization, Security), and Diagnostics (WAN Connectivity). The main area is titled "Site Settings" with the sub-section "Site Defaults". It includes fields for "Allowed IPs" (172.21.0.0/16, 172.16.0.0/16), "DNS Servers" (172.16.250.155), "Endpoint" (localhost:8080, highlighted with a red arrow and labeled "FIREZONE_HOSTNAME"), "Persistent Keepalive" (0), and "MTU" (1280). A note at the bottom of the page states: "Configures the default AllowedIPs setting for devices. AllowedIPs determines which destination IPs get routed through Firezone. Specify a comma-separated list of IPs or CIDRs here to achieve specific routing rules." Another note says: "Comma-separated list of DNS servers to use for devices. Leaving this blank will omit the DNS section in generated device configs." A third note under "Endpoint" says: "IPv4 or IPv6 address that devices will be configured to connect to. Defaults to this server's public IP if not set."

2. Casdoor可以正常登录和使用。
3. **CASDOOR_HOSTNAME**: <http://localhost:8000>, 如果您使用默认的 **app.conf** 部署 Casdoor。

步骤2：配置Casdoor应用

1. 创建一个新的Casdoor应用或使用现有的一个。
2. 添加一个重定向URL:

例如，如果FireZone Provider中的Configid是TEST，那么重定向URL应该是
[http://\[FIREZONE_HOST\]/auth/oidc/\[PROVIDER_CONFIG_ID\]/callback/](http://[FIREZONE_HOST]/auth/oidc/[PROVIDER_CONFIG_ID]/callback/)。

Home ②:

Description ②:

Organization ②:

Client ID ②:

Client secret ②:

Cert ②:

Redirect URLs ②:

打开您喜欢的浏览器并访问: `http://[CASDOOR_HOSTNAME]/.well-known/openid-configuration`, 您将看到Casdoor的OIDC配置。

3. 配置FireZone: Security → Add OpenID Connect Provider

OIDC Config

Config ID
TEST

Label
TEST **ConfigID should be the PROVIDER_CONFIG_ID of the redirect URL**

Scope
openid email profile

Response type
code

Client ID
0159c45127541d48e433

Client secret
add1be9982640e048fcf46770d75674b918484af

Discovery Document URI
http://localhost:8000/.well-known/openid-configuration

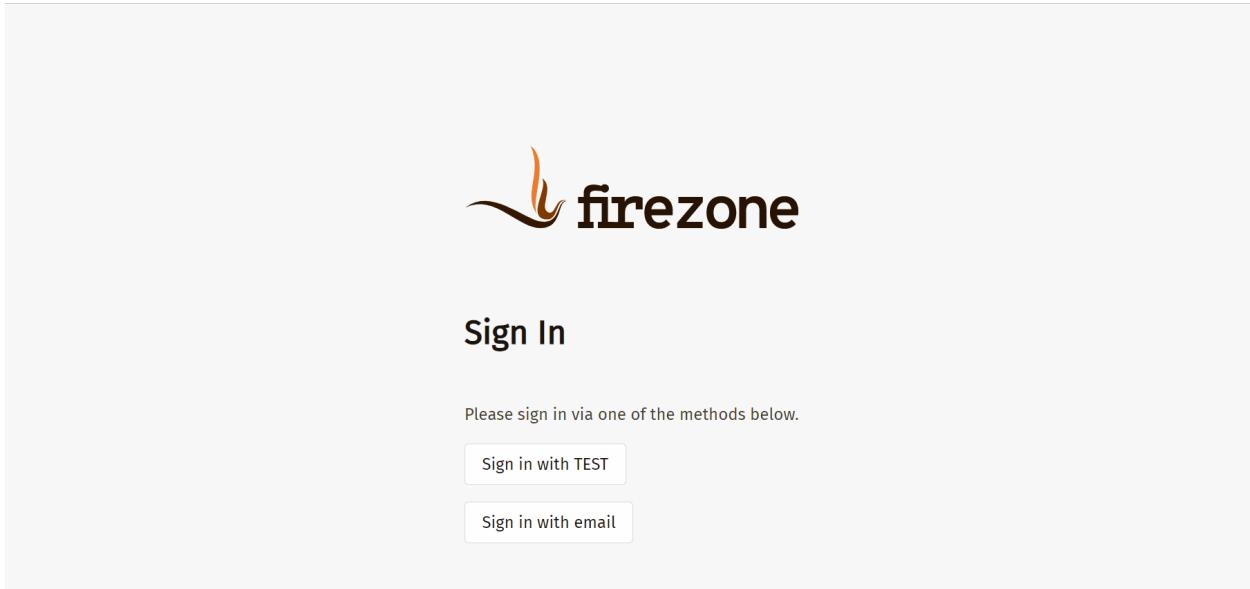
Auto create users

Save

- Discovery Document URI: FireZone Provider Discovery Document URI应该是 https://[CASDOOR_HOST]/.well-known/openid-configuration。
- Scopes: openid email profile
- ConfigID: ConfigID应该是重定向URL的PROVIDER_COONFIG_ID，并且应该对应Casdoor重定向URL。

- **Auto-create users**: 成功登录将自动创建用户。

退出FireZone并测试SSO



Cloud Foundry

在集成之前，我们需要在本地部署Casdoor。

然后，我们可以按照以下步骤在我们自己的应用中快速实现基于Casdoor的登录页面。

步骤1：配置Casdoor应用程序

1. 创建或使用现有的Casdoor应用程序。
2. 添加一个重定向URL: `http://CASDOOR_HOSTNAME/login`



3. 复制客户端ID；我们将在接下来的步骤中需要它。

步骤2：在Casdoor中添加用户

现在你有了应用程序，但没有用户，你需要创建一个用户并分配角色。

转到“用户”页面，然后点击右上角的“添加用户”。这将打开一个新页面，您可以在其中添加新用户。

在添加用户名和组织“Cloud Foundry”后保存用户（其他详细信息是可选的）。

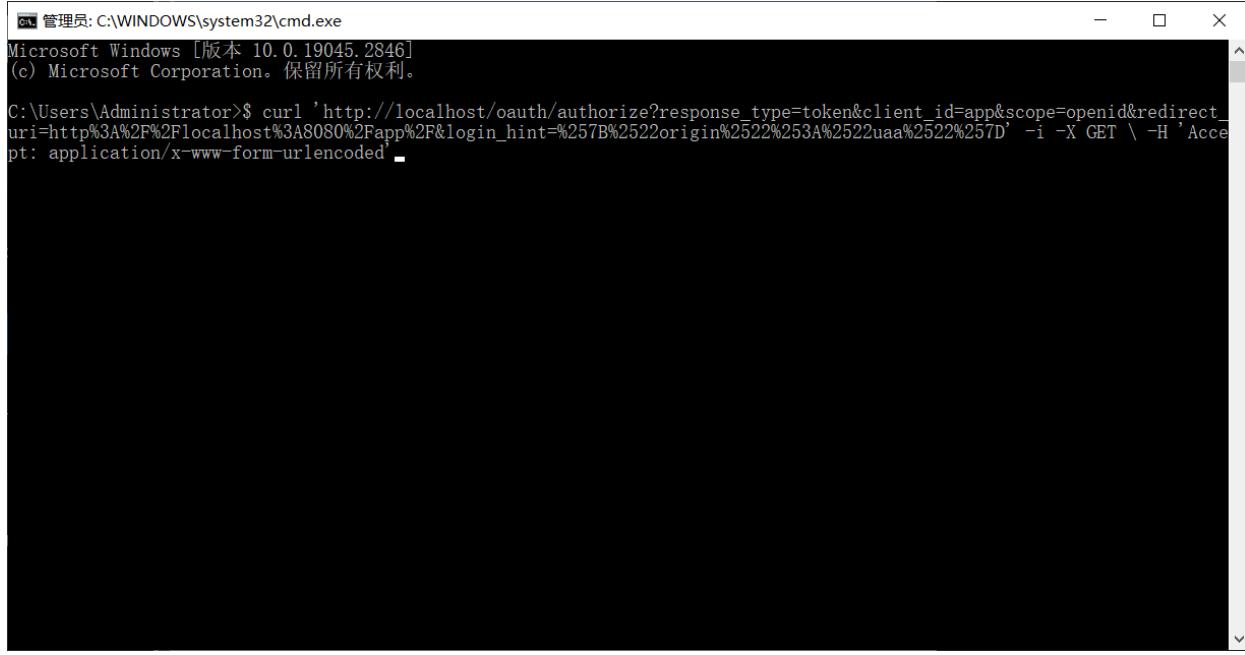
现在，你需要为你的用户设置一个密码，你可以通过点击“管理你的密码”来做到这一点。

为您的用户选择一个密码并确认它。

步骤3：构建Cloud Foundry应用

按照这些步骤启动Cloud Foundry。

- `$ git clone git://github.com/cloudfoundry/uaa.git`
- `$ cd uaa`
- `$./gradlew run`

A screenshot of a Windows Command Prompt window titled "管理员: C:\WINDOWS\system32\cmd.exe". The window shows the following command and its output:

```
Microsoft Windows [版本 10.0.19045.2846]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Administrator>$ curl 'http://localhost/oauth/authorize?response_type=token&client_id=app&scope=openid&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2Fapp%2F&login_hint=%257B%2522origin%2522%253A%2522uaa%2522%257D' -i -X GET \ -H 'Accept: application/x-www-form-urlencoded'
```

步骤4：集成Casdoor

现在打开另一个命令行并输入：

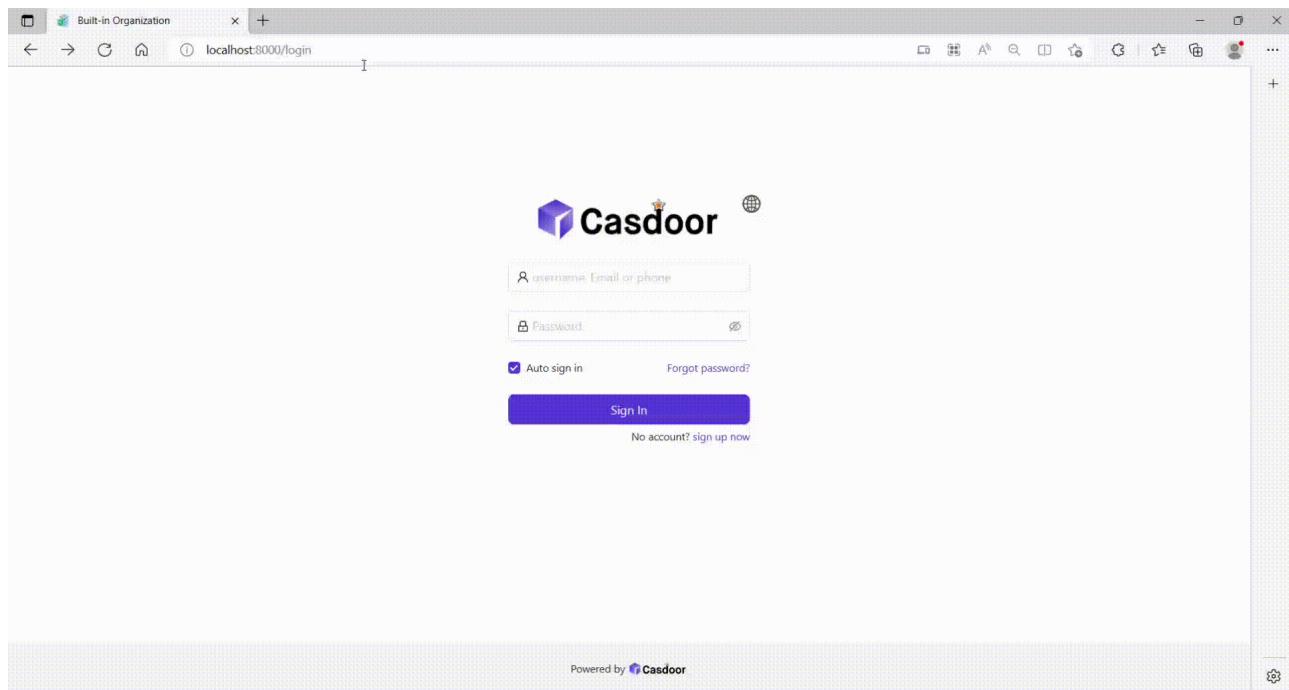
```
curl '<http://localhost/oauth/
authorize?response_type=token&client_id=app&scope=openid&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2Fapp%2F>' 
-i -X GET \
-H 'Accept: application/x-www-form-urlencoded'
```

我们已经获得了客户端ID和重定向URI；我们输入这些参数。

Parameter	Type	Constraints	Description
response_type	String	Required	Space-delimited list of response types. Here, token , i.e. an access token
client_id	String	Required	a unique string representing the registration information provided by the client
scope	String	Optional	requested scopes, space-delimited
redirect_uri	String	Optional	redirection URI to which the authorization server will send the user-agent back once access is granted (or denied), optional if pre-registered by the client

执行命令，我们可以得到下面的结果，这意味着我们已经成功地将Casdoor与Cloud Foundry集成。

```
HTTP/1.1 302 Found
Content-Security-Policy: script-src 'self'
Strict-Transport-Security: max-age=31536000
Set-Cookie: X-Uaa-CsrF=09mMqMDhcwHGLMufn84YA1; Path=/; Max-Age=86400; Expires=Fri, 5 May 2023 14:53:54 GMT; HttpOnly; SameSite=Lax
Cache-Control: no-store
Content-Language: en
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Location: http://localhost:8080/app/#token_type=bearer&access_token=eyJhbGciOiJIUzI1NiIsImprdsI6Imh0dHBzO18vbG9jYWxob3N0OjgwODAvdWFhL3Rva
```



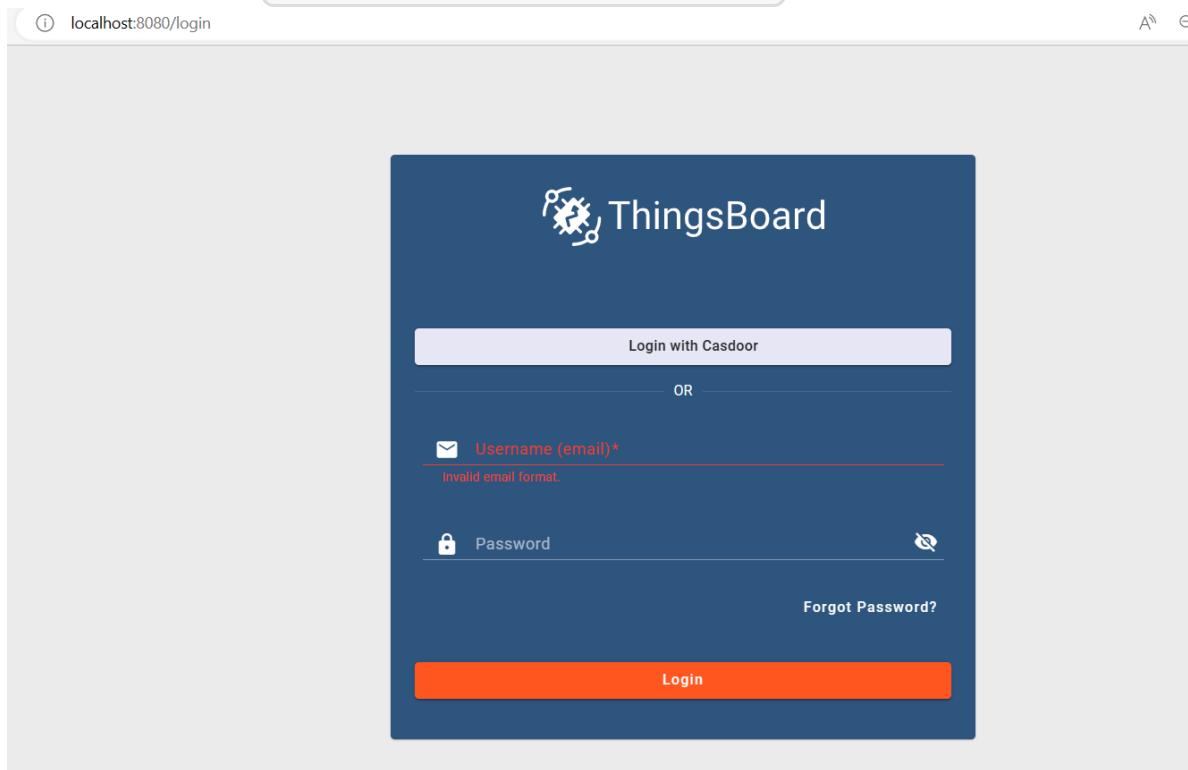
Thingsboard

在集成之前，我们需要在本地部署Casdoor。

然后，我们可以按照以下步骤在我们自己的应用中快速实现基于Casdoor的登录页面。

步骤1：配置Casdoor应用

1. 创建一个新的Casdoor应用或使用现有的应用。
2. 添加重定向URL: `http://CASDOOR_HOSTNAME/login`



3. 复制客户端ID和客户端密钥。 我们将在接下来的步骤中需要它们。

步骤2：在Casdoor中添加用户

现在你有了应用，你需要创建一个用户并分配一个角色。

转到“用户”页面，然后在右上角点击“添加用户”。这将打开一个新页面，您可以在其中添加新用户。

在添加用户名并选择组织“Thingsboard”后保存用户（其他详细信息可选）。

接下来，您需要为用户设置密码。您可以通过点击“管理您的密码”来做到这一点。

为用户选择一个密码并确认它。

步骤3：准备和构建Thingsboard应用

首先，Thingsboard只支持Java 11 (OpenJDK)。

您可以从以下链接下载：

[JDK下载页面](#)

要启动Thingsboard，请按照以下步骤操作（适用于Windows系统）：

- 下载并解压包。[下载包](#)
- 根据您的偏好在\thingsboard\conf\thingsboard.yml中配置Thingsboard，包括Kafka、PostgreSQL等的配置。
- 在Thingsboard文件夹的命令行中运行`install.bat -loadDemo`以安装并添加演示数据。

```
C:\Program Files (x86)\thingsboard>install.bat --loadDemo  
Detecting Java version installed.  
CurrentVersion 110  
Java 11 found!  
Installing thingsboard ...  
...  
ThingsBoard installed successfully!
```

- 在命令行中运行 `net start thingsboard` 以启动 Thingsboard。您应该看到以下输出：

```
The ThingsBoard Server Application service is starting.  
The ThingsBoard Server Application service was started successfully.
```

步骤4：集成Casdoor

现在打开 <http://localhost:8080> 并登录到管理员账户：

账户：sysadmin@thingsboard.org / 密码：sysadmin

成功登录后，点击页面左下角的 OAuth2 按钮。

The screenshot shows the ThingsBoard Home dashboard. On the left, a sidebar menu includes: Home, Tenants, Tenant profiles, Resources (with a dropdown arrow), Notification center, Settings, Security (with a dropdown arrow), General, Two-factor authentication, and OAuth2.

The main dashboard area has a title "Home". It displays several key metrics and links:

- Tenants**: Shows 2 tenants with a "+" button.
- Tenant profiles**: Shows 2 tenant profiles with a "+" button.
- CPU**: Shows 15% usage of 8 cores.
- Devices**: Shows 9 devices.
- Assets**: Shows 2 assets.
- Users**: Shows 8 users.
- Customers**: Shows 3 customers.
- Realtime - last h**: A chart showing CPU usage over time, ranging from 0% to 100%.
- Documentation**: Includes links to Getting started, Tenant profiles, API, and Widgets Library.
- Transport messages**: Shows history of transport messages from May 02 to May 05.
- Configured features**: Lists Email, SMS, Slack, OAuth 2, and 2FA.

按照以下方式填写空白：

Providers

Custom

Login provider*	Custom	Allowed platforms	Web, Android, iOS
Client ID*	e324f9a3f55e1adac4ef	Client secret*	28b3f98c1f55c1cc57f74b9b1a68b5d2e79

General

Access token URI*	http://localhost:8000/api/login/oauth/access_token	Authorization URI*	http://localhost:8000/login/oauth/authorize
JSON Web Key URI	http://localhost:8000/.well-known/jwks	User info URI	http://localhost:8000/api/userinfo

Mapper

Client authentication method*	POST
-------------------------------	------

Provider label*

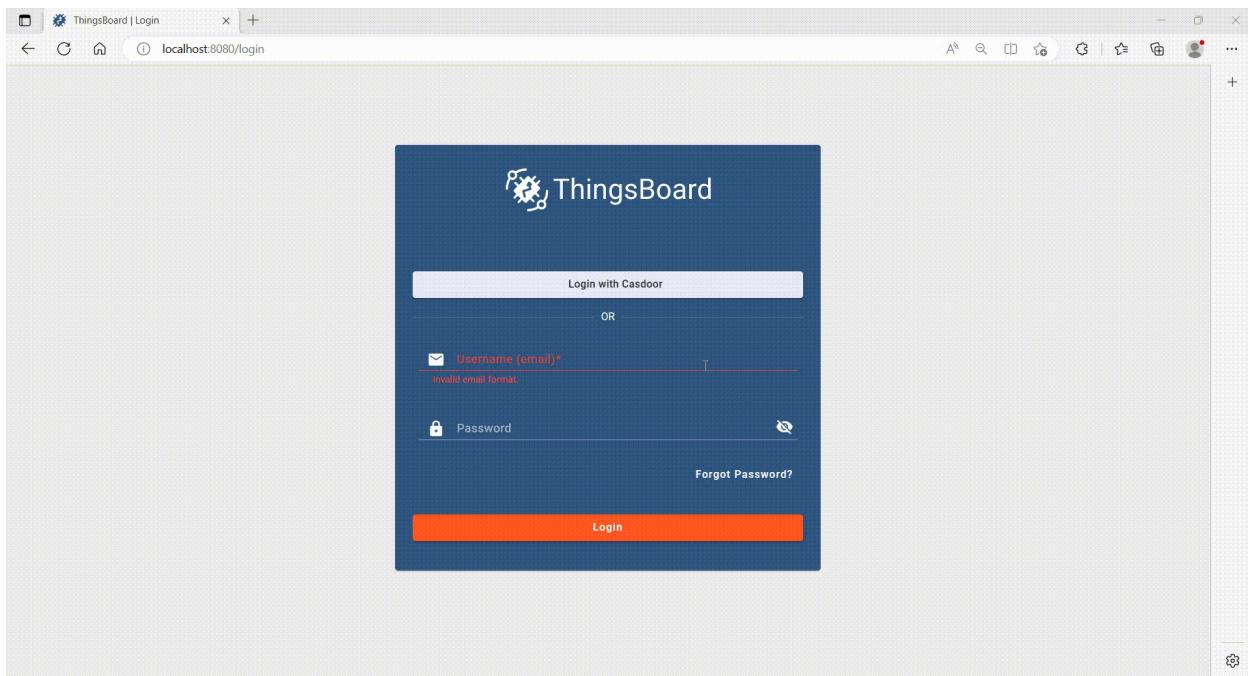
Casdoor	Login button icon
---------	-------------------

Allow user creation

您可以从以下链接获取这些值: [OIDC discovery URL](#)

```
{  
  "issuer": "https://door.casdoor.com",  
  "authorization_endpoint": "https://door.casdoor.com/login/oauth/authorize",  
  "token_endpoint": "https://door.casdoor.com/api/login/oauth/access_token",  
  "userinfo_endpoint": "https://door.casdoor.com/api/userinfo",  
  "jwks_uri": "https://door.casdoor.com/.well-known/jwks",  
  "introspection_endpoint": "https://door.casdoor.com/api/login/oauth/introspect",  
  "response_types_supported": ["code"]}
```

填写这些空白后，您已经成功将Casdoor与Thingsboard集成。当你登录到<http://localhost:8080>时，你应该看到以下内容：



JavaScript

Firebase

使用Casdoor作为身份提供者的Firebase项目

微信小程序

在 微信小程序中使用 Casdoor

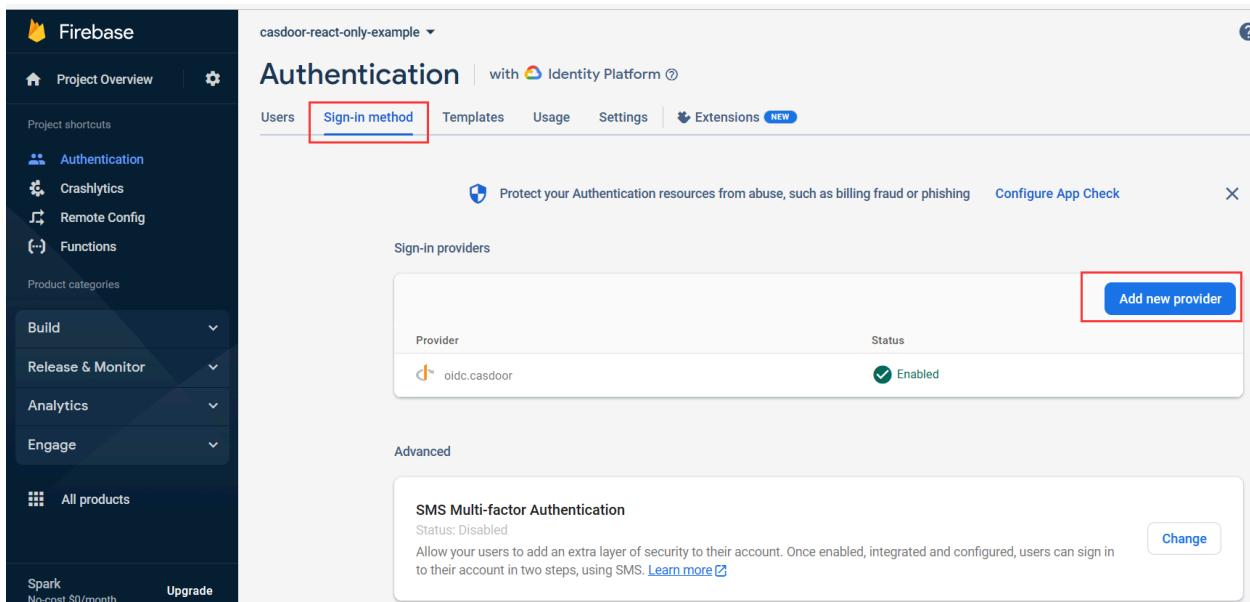
Firebase

Firebase支持OIDC作为身份提供者，您可以使用Casdoor作为Firebase web应用的OIDC提供者。

1. 创建一个Firebase项目

前往[Firebase控制台](#)创建一个项目。

1.1 添加Casdoor作为提供者



The screenshot shows the Firebase console interface for managing authentication methods. On the left, there's a sidebar with project settings like Project Overview, Authentication (which is selected), Crashlytics, Remote Config, Functions, Build, Release & Monitor, Analytics, Engage, and All products. The main area is titled 'Authentication' and shows 'casdoor-react-only-example' under 'with Identity Platform'. The 'Sign-in method' tab is active. Below it, there's a 'Sign-in providers' section with a table:

Provider	Status
oldc.casdoor	Enabled

A red box highlights the 'Add new provider' button at the top right of this section. At the bottom, there's an 'Advanced' section for SMS Multi-factor Authentication, which is currently disabled.

您需要首先启用“身份平台”功能，以在Firebase上启用OIDC集成。

在自定义提供者中选择[OpenID Connect](#)，填写以下信息：

名称 (按顺序)	描述	示例值
名称	可以是您喜欢的任何字符串	casdoor
客户端ID	Casdoor应用的客户端ID	294b09fbc17f95daf2fe
发行者 (URL)	Casdoor服务器URL	https://door.casdoor.com
客户端密钥	Casdoor应用的客户端密钥	dd8982f7046ccba1bbd7851d5c1ece4e52bf039d

door.casdoor.com/applications/casbin/app-vue-python-example

Casdoor Home User Management Identity Authorization Logging & Auditing Business & Payments Admin

Edit Application Save Save & Exit

Name ⓘ: app-vue-python-example

Display name ⓘ: Casdoor Vue Python Example

Logo ⓘ: URL ⓘ: https://cdn.casbin.org/img/casdoor-logo_1185x256.png

Preview: 

Home ⓘ: https://demo.gsoc.com.cn

Description ⓘ:

Organization ⓘ: casbin

Tags ⓘ:

Client ID ⓘ: 294b09fbc17f95daf2fe

Client secret ⓘ: dd8982f7046ccba1bbd7851d5c1ece4e52bf039d

Cert ⓘ: cert-built-in

上述示例值可以从Casdoor演示站点获取: [app-vue-python-example](#)



Enable

1 Define new OIDC provider

Grant type

Code flow Implicit flow (id_token)

Name

casdoor

Provider ID: oidc.casdoor

Client ID

294b09fbc17f95daf2fe

Issuer (URL)

https://door.casdoor.com

Client secret

dd8982f7046ccba1bbd7851d5c1ece4e52bf039d

Next



Configure OIDC integration

1.2 添加回调url

将回调URL添加到Casdoor应用的重定向URL：

The screenshot shows the 'OpenID Connect' provider configuration screen. At the top, there is a toggle switch labeled 'Enable' which is turned on. Below it, a section titled 'Define new OIDC provider' shows the provider details: Name: casdoor, Provider ID: oidc.casdoor, Client ID: 76dfa0e75796f8443b5e, Issuer (URL): https://fb-casdoor.firebaseio...'. A large blue button labeled '2 Configure OIDC integration' is present. Below this, a note says 'When completing set up, add this authorization callback URL to your OIDC app configuration.' followed by a 'Callback URL' input field containing 'https://casdoor-react-only-example.firebaseio.com/_/auth/handler' with a copy icon. A callout box below the URL says 'To complete set up, follow the steps for your platform' with links for Apple, Android, and Web. At the bottom right are 'Delete provider', 'Cancel', and 'Save' buttons.

The screenshot shows the configuration page for the application 'casbin/app-vue-python-example'. It includes fields for 'Tags', 'Client ID' (294b09fbc17f95daf2fe), 'Client secret' (dd8982f7046ccba1bbd7851d5c1ece4e52bf039d), and 'Cert' (cert-built-in). A red box highlights the 'Redirect URLs' section, which contains a table with three rows: 'Redirect URLs' (Add), 'Redirect URL' (localhost, 127.0.0.1:5000/callback, https://fb-casdoor.firebaseio.com/_/auth/handler). The URL 'https://fb-casdoor.firebaseio.com/_/auth/handler' is also highlighted with a red box. Other configuration options include 'Token format' (JWT), 'Token expire' (168 Hours), 'Refresh token expire' (0 Hours), and several toggle switches for 'Enable password' (on), 'Enable signup' (on), and 'Signin session' (on).

在这里，我们提供一个示例[casdoor-firebase-example](#)，供您在应用中使用Casdoor身

份验证。要查看如何在应用中使用Casdoor身份验证的更多详细信息，请参阅[Firebase 文档](#)。

微信小程序

① 信息

从1.41.0版本开始，Casdoor现在支持微信小程序。

介绍

由于微信小程序不支持标准的OAuth，因此无法重定向到自托管的Casdoor登录页面。因此，使用Casdoor进行微信小程序的过程与常规程序的过程不同。

本文档将解释如何将Casdoor集成到微信小程序中。您可以在GitHub上找到这个集成的例子：[casdoor-wechat-miniprogram-example](#)。有关更详细的信息，请参阅微信小程序登录文档。

配置包括以下名称：

`CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP地址，例如，
`https://door.casbin.com`。

步骤1：部署Casdoor

首先，应部署Casdoor服务器。

成功部署Casdoor后，您需要确保：

1. Casdoor可以正常访问和使用。
2. 将Casdoor的`origin`值(`conf/app.conf`)设置为`CASDOOR_HOSTNAME`。

```
conf > ⚙ app.conf
 8  dbName = casdoor
 9  redisEndpoint =
10 defaultStorageProvider =
11 isCloudIntranet = false
12 authState = "casdoor"
13 httpProxy = "127.0.0.1:10808"
14 verificationCodeTimeout = 10
15 initScore = 2000
16 logPostOnly = true
17 origin = "http://10.144.1.2:8000"| CASDOOR_HOSTNAME
```

步骤2：配置Casdoor应用程序

1. 在Casdoor中创建一个微信IDP，并提供微信小程序开发平台给你的APPID和APPSECRET。

New Provider [Save](#) [Save & Exit](#) [Cancel](#)

Name [?](#) : provider_Mini Program

Display name [?](#) : Mini Program

Category [?](#) : OAuth

Type [?](#) : WeChat Mini Program

Client ID [?](#) : ***

Client secret [?](#) : ***

Provider URL [?](#) : <https://github.com/organizations/xxx/settings/applications/1234567>

[Save](#) [Save & Exit](#) [Cancel](#)

2. 创建一个新的Casdoor应用程序，或使用一个已经存在的。
3. 将在上一步中创建的IDP添加到您想要使用的应用程序中。

❗ TIPS

为了方便，Casdoor默认将应用中的第一个微信类型的IDP视为微信小程序的IDP。

因此，如果你想在这个应用中使用微信小程序，不要在一个应用中添加多个微信类型的IDP。

步骤3：编写微信小程序代码

微信小程序提供了一个API，用于内部登录并获取代码。代码应该然后被发送到Casdoor。Casdoor将使用此代码从微信服务器检索信息（如OpenID和SessionKey）。

以下代码演示了如何完成上述过程：

```
// 在小程序中登录
wx.login({
  success: res => {
    // 这是需要发送给Casdoor的登录代码
    console.log(res.code)

    wx.request({
      url: `${CASDOOR_HOSTNAME}/api/login/oauth/access_token`,
      method: "POST",
      data: {
        "tag": "wechat_miniprogram", // 必填
        "client_id": "6825f4f0af45554c8952",
        "code": res.code,
        "username": this.data.userInfo.nickName, // 登录时更新用户资料。
        "avatar": this.data.userInfo.avatarUrl,
      },
      header: {
        "content-type": "application/x-www-form-urlencoded",
      },
      success: res => {
        console.log(res)
        this.globalData.accessToken = res.data.access_token // 获取
        Casdoor的访问令牌
      }
    })
  }
})
```

需要注意的是，`tag` 参数对于告知Casdoor这是来自微信小程序的请求是必须的。

上述代码在登录时包含了微信小程序用户的用户名和头像URI。您可以选择分别传递这两个参数，然后在成功登录并获取访问令牌后将它们传递给Casdoor：

```
WX.getUserProfile({
  desc: '将您的信息分享给Casdoor',
  success: (res) => {
    this.setData({
      userInfo: res.userInfo,
      hasUserInfo: true
    })
    console.log(app.globalData.accessToken)
    wx.request({
      url: `${CASDOOR_HOSTNAME}/api/update-user`, // Casdoor URL
      method: "POST",
      data: {
        "owner": "test",
        "name": "wechat-oGk3T5tIiMFo3SazC075f0HEiE7Q",
        "displayName": this.data.userInfo.nickName,
        "avatar": this.data.userInfo.avatarUrl
      },
      header: {
        "Authorization": "Bearer " + app.globalData.accessToken,
        // Bearer token
        "content-type": "application/json"
      },
      success: (res) => {
        console.log(res)
      }
    })
  }
})
```

此外，您可以将访问令牌用作您需要的任何Casdoor操作的持有人令牌。

① 提示

目前，Casdoor无法将现有账户绑定到微信小程序用户。在Casdoor从微信获取OpenID后，如果ID不存在，它将创建一个新用户，如果存在，它将使用现有用户。

Lua



在 APISIX 中使用 Casdoor

APISIX

目前，有两种方法可以使用Casdoor通过APISIX插件连接到APISIX并保护APISIX后面的API：使用APISIX的Casdoor插件或使用APISIX的OIDC插件。

通过 APISIX 的 Casdoor 插件连接 Casdoor

这个插件，`authz-casdoor`，可以保护APISIX后面的API，强制每一个请求都要经过身份验证，而无需修改API的代码。

如何启用它？

在创建路由时，您需要指定此插件并提供所有必需的字段。参见下面的示例。

```
curl "http://127.0.0.1:9180/apisix/admin/routes/1" -H "X-API-KEY:edd1c9f034335f136f87ad84b625c8f1" -X PUT -d '  
{"  
    "methods": ["GET"],  
    "uri": "/anything/*",  
    "plugins": {  
        "authz-casdoor": {  
            "endpoint_addr": "http://localhost:8000",  
            "callback_url": "http://localhost:9080/anything/callback",  
            "client_id": "7ceb9b7fda4a9061ec1c",  
            "client_secret": "3416238e1edf915eac08b8fe345b2b95cdba7e04"  
        }  
    },  
    "upstream": {  
        "type": "roundrobin",  
        "nodes": [{"host": "127.0.0.1", "port": 8000}],  
        "weight": 1  
    }  
}
```

在这个例子中，我们使用APISIX的管理员API，创建了一个指向"httpbin.org:80"的路由"/anything/*"，并启用了"authz-casdoor"插件。此路由现在已在Casdoor的身份验证保护之下。

属性

名称	类型	申请标准	默认	有效期	描述
endpoint_addr	字符串	必填			Casdoor的URL。
client_id	字符串	必填			Casdoor中的客户端ID。
client_secret	字符串	必填			Casdoor中的客户端密钥。
callback_url	字符串	必填			用于接收状态和代码的回调URL。

endpoint_addr 和 *callback_url* 不应以"/"结尾

在"authz-casdoor"插件的配置中，我们可以看到四个参数。

第一个是"callback_url"。这是OAuth2中的回调URL。应强调的是，这个回调URL **必须属于您为路由指定的"uri"**。例如，在这个例子中，<http://localhost:9080/anything/callback> 显然属于 "/anything/*"。只有通过这种方式，插件才能拦截并利用对callback_url的访问（这样插件就可以获取OAuth2中的代码和状态）。callback_url的逻辑完全由插件实现，因此无需修改服务器来实现此回调。

第二个参数 "endpoint_addr" 显然是 Casdoor 的 URL。第三个和第四个参数是 "client_id" 和 "client_secret"，您可以在注册应用程序时从 Casdoor 获取这些参数。

它是如何工作的？

假设一个从未访问过此路由的新用户即将访问它 (<http://localhost:9080/anything/d?param1=foo¶m2=bar>)。考虑到 "authz-casdoor" 已启用，此访问将首先由 "authz-casdoor" 插件处理。在检查会话并确认该用户尚未通过身份验证后，将会拦截此次访问。保留用户想要访问的原始 URL，他们将被重定向到 Casdoor 的登录页面。

在成功使用用户名和密码（或他们使用的任何其他方法）登录后，Casdoor 会将此用户重定向到带有 GET 参数 "code" 和 "state" 的 "callback_url"。因为 "callback_url" 是由插件知道的，所以当这次对 "callback_url" 的访问被拦截时，将会触发 OAuth2 中的 "Authorization code Grant Flow" 逻辑。这意味着插件将请求访问令牌以确认此用户是否真的已登录。经过这个确认后，插件将会把用户重定向到他们想要访问的原始 URL，这个 URL 是我们之前保存的。已登录的状态也将保留在会话中。

下次此用户想要访问此路由背后的 URL（例如，<http://localhost:9080/anything/d>），在发现此用户之前已经被认证后，这个插件不再重定向此用户。这样，用户可以在不受干扰的情况下访问此路由下的任何内容。

通过 APISIX 的 OIDC 插件连接 Casdoor

Casdoor 可以使用 OIDC 协议连接到 APISIX，本文档将向您展示如何操作。

以下是配置中使用的一些名称：

`CASDOOR_HOSTNAME`：部署 Casdoor 服务器的域名或 IP。

`APISIX_HOSTNAME`：部署 APISIX 的域名或 IP。

步骤1：部署Casdoor和APISIX

首先，部署Casdoor和APISIX。

在成功部署后，您需要确保：

1. 可以登录并正常使用Casdoor。
2. 将Casdoor的 origin 值 (conf/app.conf) 设置为 CASDOOR_HOSTNAME。

```
conf > ⚙ app.conf
 8  dbName = casdoor
 9  redisEndpoint =
10 defaultStorageProvider =
11 isCloudIntranet = false
12 authState = "casdoor"
13 httpProxy = "127.0.0.1:10808"
14 verificationCodeTimeout = 10
15 initScore = 2000
16 logPostOnly = true
17 | origin = "http://10.144.1.2:8000"|
               CASDOOR_HOSTNAME
```

步骤2：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序，或使用一个已经存在的。
2. 添加一个重定向URL：http://APISIX_HOSTNAME/REDIRECTWHATYOUWANT，并将 REDIRECTWHATYOUWANT 替换为所需的重定向URL。
3. 选择 "JWT-Empty" 作为令牌格式选项。
4. 添加所需的提供商并配置其他设置。

The screenshot shows the Casdoor application settings interface. It includes fields for Client ID (07860a229bd0b162cdfa), Client secret (ea021...:9373fe3e), Redirect URLs (localhost:9000/callback), and Token format (JWT-Empty). There is also a note to 'Select JWT-Empty'.

在应用设置页面上，您将找到如上图所示的Client ID和Client Secret值。 我们将在下一步中使用它们。

打开你最喜欢的浏览器并访问：http://CASDOOR_HOSTNAME/.well-known/openid-configuration， 在那里你会找到Casdoor的OIDC配置。

步骤3：配置APISIX

APISIX 拥有官方 OIDC 支持，由 [lua-resetyl-openidc](#) 实现。

您可以根据APISIX OIDC文档自定义设置。 以下路由设置将被使用：

```
# 使用您自己的X-Api-Key
$ curl -X POST APISIX_HOSTNAME/apisix/admin/routes -H "X-Api-Key: edd1c9f034335f136f87ad84b625c8f1" -d '{
  "uri": "/get",
  "name": "apisix_casdoor_test",
  "plugins": {
    "openid-connect": {
      "client_id": "客户端ID",
      "client_secret": "客户端密钥",
      "discovery": "http://CASDOOR_HOSTNAME/.well-known/openid-configuration",
      "introspection_endpoint_auth_method": "client_secret_basic",
      "logout_path": "/logout",
      "realm": "master",
      "redirect_uri": "http://APISIX_HOSTNAME/REDIRECTWHATYOUWANT",
      "bearer_only": false,
    }
  }
}'
```

现在，访问 `http://APISIX_HOSTNAME/get`，浏览器将会重定向你到Casdoor登录页面。成功登录后，你会看到已经向`httpbin.org`发送了一个请求，如下面的截图所示。

PHP

Zabbix

Using Casdoor for authentication in Zabbix

WordPress

Integrating CAS (Central Authentication Service) into WordPress using Casdoor (identity provider) and the wp-classify plugin.

禅道

在禅道中使用 Casdoor 进行身份验证

在ShowDoc中使用Casdoor作为OAuth2服务器

在ShowDoc中使用Casdoor作为OAuth2服务器

Flarum

使用OAuth2连接各种应用程序，如Flarum

Moodle

使用OAuth连接Moodle

Zabbix

Zabbix acts as a Service Provider (SP), while CASdoor acts as an Identity Provider (IdP). They communicate and collaborate through the SAML2 protocol to achieve single sign-on (SSO) functionality for users in Zabbix.

Step 1: Deploy Casdoor and Zabbix

Firstly, deploy [Casdoor](#) and [Zabbix](#). After a successful deployment, make sure:

1. Casdoor can be logged in and used successfully.
2. You can successfully log in and use Zabbix.

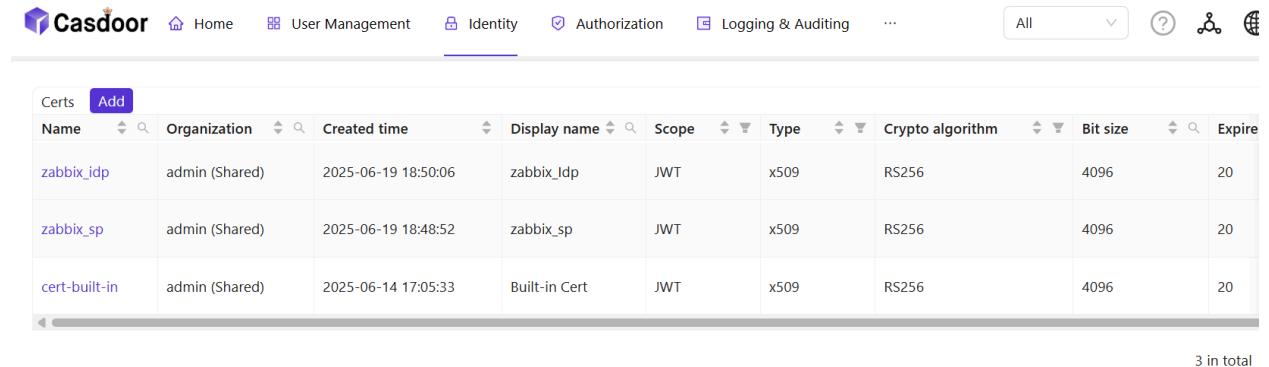
Step 2: Adding Certificates

To ensure the security of communication, certificates need to be configured between Zabbix and CASdoor. Private keys and certificates should be stored in the `/etc/zabbix/conf/certs/` directory, unless a custom path is provided in `zabbix.conf.php`.

By default, the `zabbix - web - nginx - mysql` Docker container looks for the following locations:

- `/etc/zabbix/conf/certs/sp.key` - SP private key file
- `/etc/zabbix/conf/certs/sp.crt` - SP certificate file
- `/etc/zabbix/conf/certs/idp.crt` - IDP certificate file

Creating Certificates in CASdoor: Log in to the CASdoor management interface and follow the system prompts to create two certificates. These two certificates will be used for communication encryption between Zabbix and CASdoor.



The screenshot shows the Casdoor management interface with the 'Certs' tab selected. The table lists three certificates:

Name	Organization	Created time	Display name	Scope	Type	Crypto algorithm	Bit size	Expire
zabbix_idp	admin (Shared)	2025-06-19 18:50:06	zabbix_Idp	JWT	x509	RS256	4096	20
zabbix_sp	admin (Shared)	2025-06-19 18:48:52	zabbix_sp	JWT	x509	RS256	4096	20
cert-built-in	admin (Shared)	2025-06-14 17:05:33	Built-in Cert	JWT	x509	RS256	4096	20

3 in total

Copying Certificates and Private Keys: Copy the created certificate and private key files to the Zabbix configuration directory `/etc/zabbix/conf/certs`. If you are using Docker for deployment, you can map local certificate files to the container using volume mounting.

Step 3:Configuring Zabbix

For SAML configuration in Zabbix, three required fields need to be set: `Single Sign - On`, `Issuer`, and `Public Certificate`.

Log in to the Zabbix management interface, click `User` → `authentication` → `SAML settings`.

Configure Zabbix according to the SAML metadata in the CASdoor configuration:

- idP entity ID (Issuer): Corresponds to `entityID="http://localhost:8000"`. This value identifies the entity ID of CASdoor, and Zabbix will communicate with CASdoor based on this ID.
- SSO service URL: Corresponds to `Location="http://localhost:8000/api/saml/redirect/admin/zabbix"`. This is the URL of the single sign - on service provided by CASdoor. When a user initiates a single sign - on request in Zabbix, they will be redirected to this URL for authentication.
- username attribute: The SAML attribute used as the username when logging in to Zabbix. Here, `Name` is used, indicating that Zabbix will use the `Name` attribute in the SAML assertion as the user's login name.
- SP entity ID: A unique SP ID that can be set arbitrarily. This ID is used to identify the Zabbix service provider and needs to be consistent with the

configuration in CASdoor.

Step 4: Configuring CASdoor

Some necessary configurations need to be made in CASdoor to ensure the normal operation of the integration with Zabbix.

Editing Name and Logo: Log in to the CASdoor management interface, find the relevant settings, and edit the application's name and logo for better presentation to users.

Screenshot of the CASdoor 'Edit Application' form showing configuration for the Zabbix integration:

Edit Application		Save	Save & Exit
Name ⓘ:	zabbix		
Display name ⓘ:	zabbix		
Is shared ⓘ:	<input checked="" type="checkbox"/>		
Logo ⓘ:	URL ⓘ:	https://blog.zabbix.com/wp-content/uploads/2020/06/zabbix_blog_327x44.png	
Preview:	 The logo consists of the words "ZABBIX BLOG" in a bold, sans-serif font. "ZABBIX" is in red and "BLOG" is in black.		
Home ⓘ:	Home		
Description ⓘ:			

Selecting a Certificate: In CASdoor, select `zabbix_idp` as the certificate for signing and encrypting SAML messages to ensure communication security.

Cert ⓘ: `zabbix_idp`

Redirect URL: Enter a unique name. In your SP (Zabbix), this may be called **Audience** or **Entity ID**. Ensure that the **Redirect URL** you enter here is consistent with that in your SP; otherwise, single sign - on may fail.

The screenshot shows a configuration interface for SAML settings. At the top, there's a header with "Redirect URLs" and a help icon. Below it is a section titled "Redirect URLs" with a "Add" button. A sub-section titled "Redirect URL" contains a text input field with the value "zabbix_sp_id".

Reply URL: Enter the URL of the ACS (Assertion Consumer Service) for validating SAML responses. This URL is the address where Zabbix receives SAML assertions sent by CASdoor.

The screenshot shows a configuration interface for SAML settings. It includes fields for "SAML reply URL" (set to "http://localhost:8080/index_sso.php?acs"), "Enable SAML compression" (disabled), "Enable SAML C14N10" (disabled), "Use Email as NameID" (disabled), and "Enable SAML POST binding" (enabled).

Step 5: Creating a Zabbix User

Create a test user in Zabbix to verify the single sign - on functionality.

1. Log in to the Zabbix management interface and find the user management module.
2. Create a user with the username "test" (you can customize the username; this

is just an example).

Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	P
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Yes (2025-06-20 03:21:35 PM)	Ok	Internal	Enabled	Disabled	Enabled	
guest			Guest role	Disabled, Guests, Internal	No	Ok	Internal	Disabled	Disabled	Disabled	
test	test		Guest role	Guests	No	Ok	System default	Disabled	Disabled	Enabled	

Step 6: Creating a CASdoor User

Add a user in CASdoor with the same username as the one set in Zabbix.

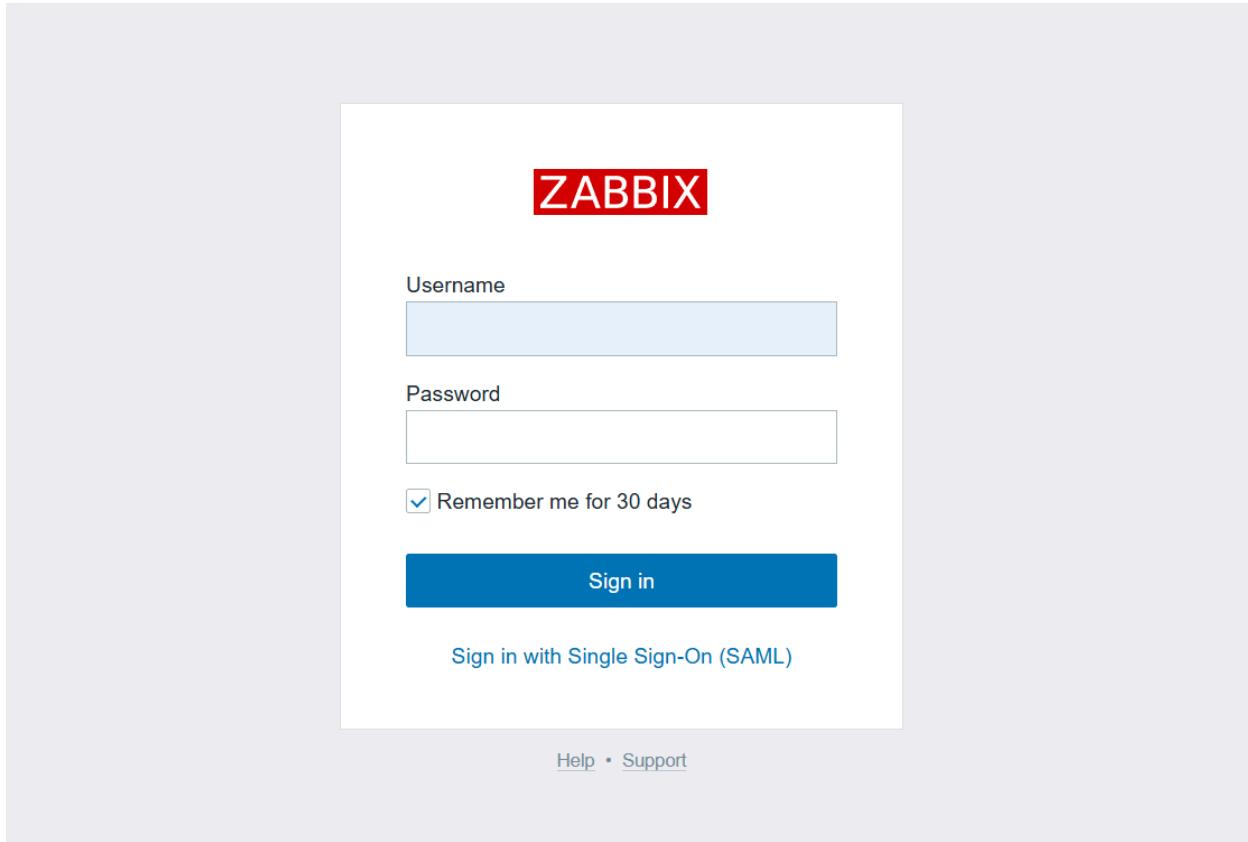
1. Log in to the CASdoor management interface and find the user management module.
2. Add a new user with the same username as the one created in Zabbix.
3. Select Zabbix and enter the user's email address.

Users									Add	Upload (xlsx)
Organization	Application	Name	Created time	Display name	Avatar	Email	Phone	Affiliation	Action	
built-in	zabbix	test	2025-06-18 17:06:54	test		jlapmu@example.com	17636092052	Example Inc.	<button>Edit</button>	<button>Delete</button>
built-in	app-built-in	admin	2025-06-14 17:05:33	Admin		admin@example.com	12345678910	Example Inc.	<button>Edit</button>	<button>Delete</button>

Step 7: Zabbix Login Process

After completing the above configurations and user creation, you can test the single sign - on functionality.

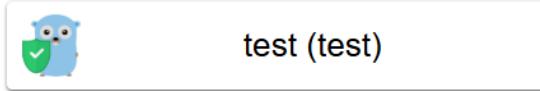
Open a browser and visit `localhost/index.php`.



Click `Sign in with Single Sign - On(SAML)`.

You will be redirected to the CASdoor page. On the CASdoor page, enter the corresponding username and password to log in.

Continue with :



Or sign in with another account :



[Password](#) [Code](#) [WebAuthn](#) [Face ID](#)

Auto sign in [Forgot password?](#)

[Sign In](#)

No account? [sign up now](#)

If the login is successful, you will be redirected back to

<https://localhost:8080/zabbix.index.php>, indicating that the single sign - on functionality is working properly.

The screenshot shows the Zabbix Global view dashboard. On the left, there's a sidebar with navigation links: Dashboards, Monitoring, Services, Inventory, Reports, Support, Integrations, Help, User settings, and Sign out. The main area has a title "Global view" and a breadcrumb "All dashboards / Global view". It features several widgets: "Top hosts by CPU utilization" (empty, showing "No data found"), "Performance" (error message: "No permissions to referred object or it does not exist!"), "System information" (Zabbix server is running: Yes, Zabbix frontend version: 7.2.7, New update available), a large digital clock "16:06" for Shanghai, a "Host availability" chart (0 Available, 0 Not ava..., 0 Mixed, 0 Unknown), a "Problems by severity" chart (0 Disaster, 0 High, 0 Average, 0 Warning, 0 Information, 0 Not class...), a "Current problems" table header (Time, Info, Host, Problem • Severity, Duration, Update, Actions, Tags), and a "Geomap" showing a map of Riga with various monitoring points.

Through the above steps, you can successfully complete the integration of Zabbix and CASdoor and achieve single sign - on functionality for users. If you encounter any problems during the configuration process, please refer to relevant documentation or community forums for help.

WordPress

This guide walks you through configuring CAS-based single sign-on (SSO) for WordPress, using:

- [wp-cassify](#): A WordPress plugin that enables CAS authentication, allowing users to log into WordPress via a CAS server (e.g., Casdoor).

Step 1: Deploy Casdoor and WordPress

First, deploy Casdoor (as the CAS server) and WordPress.

1.1 Deploy Casdoor

Refer to the official Casdoor installation guide: [Casdoor Server Installation](#).

After deployment:

1. Access the Casdoor web UI via its public/private URL (e.g.,
`http://<casdoor-server-ip>:8000`).
2. Log in with the default admin credentials (or your custom credentials set during deployment).
3. Confirm you can navigate the dashboard (e.g., access "Applications", "Users")—this ensures Casdoor is ready to act as a CAS IdP.

1.2 Deploy WordPress

Deploy WordPress using your preferred method:

- **Docker:** Use the official WordPress Docker image for quick setup (see [WordPress Docker Docs](#)).
 - **Traditional Hosting:** Install WordPress on a LAMP/LEMP stack (follow [WordPress Official Installation](#)).
1. Access the WordPress site via its URL (e.g., `http://<wordpress-server-ip>`).
 2. Complete the initial WordPress setup (create an admin account, site title).
 3. Log in to the WordPress Admin Dashboard (`http://<wordpress-server-ip>/wp-admin`) to confirm functionality.

Step 2: Create a Casdoor Application

Casdoor requires an "Application" to act as a bridge between the CAS server and WordPress. Follow these steps to create one:

1. Log in to the Casdoor Admin Dashboard.
2. Navigate to Applications > Add Application
3. Click Save to create the application.

The screenshot shows the Casdoor application configuration interface. The application is named "wordpress_cas" and has a display name of "wordpress_cas". It is not shared and has a logo pointing to https://cdn-icons-png.flaticon.com/128/174/174881.png. The home URL is empty. There is no description or organization provided. Tags are set to "built-in". Client ID is 842525b46c801cb8ad20 and Client secret is c0b093bd3b52640d13a23693202d4a9d3af2de47. Cert is set to "cert-built-in". Under Redirect URLs, there is one entry: "Redirect URL".

Step 3: Configure the wp-cassify Plugin

The wp-cassify plugin connects WordPress to your Casdoor CAS server. Follow these steps to install and configure it:

3.1 Install wp-cassify

1. Log in to the WordPress Admin Dashboard (<http://<wordpress-server-ip>/wp-admin>).
2. Navigate to Plugins > Add New.
3. In the search bar, type "wp-cassify" and select the plugin by "wp-cassify".
4. Click Install Now, then Activate to enable the plugin.

3.2 Configure wp-cassify Settings

1. In the WordPress Admin Dashboard, navigate to Settings > WP-Cassify (the plugin's configuration page).

2. Configure User General Settings.

wp-cassify Setting	Value to Enter
CAS Server Base URL	Your Casdoor CAS endpoint (e.g., <code>http://<casdoor-server-ip>:7001/cas/<organization name>/<application name></code>).
Create user if not exist	Enable

The screenshot shows the 'General Settings' section of the WP Classify plugin. It includes the following configuration items:

- CAS Server base url:** `http://192.168.101.4:7001/cas/built-in/wordpress_cas/` (Example: `https://you-cas-server/cas/`)
- CAS Version protocol:** 3 (Default value: 3)
- Disable CAS Authentication:**
- Create user if not exist:** Create wordpress user account if not exist.
- Log out on errors:** Disconnect cas user session on authentication errors without displaying any error message (silent mode).
- Enable Gateway Mode:** Enable support for auto-login (Gateway Mode).
- Enable SLO (Single Log Out):** Enable support for central logout (Single Sign Out).
- SSL Cipher used for query CAS Server with HTTPS Webrequest to validate service ticket:** `CURL_SSLVERSION_DEFAULT` (Default value: `CURL_SSLVERSION_DEFAULT`)
- Enable SSL Certificate Check:**
- cURL extra-options:** (This section is currently empty.)

A green status bar at the top indicates: "Settings saved successfully".

3. Configure User Attribute Synchronization.

WordPress User Field	Casdoor Attribute Name	Example Value
user_email	email	user@example.org
user_nickname	displayName	John Doe
display_name	displayName	John Doe

Users Attributes Synchronization Settings

Synchronize Wordpress User metas with CAS User attributes

Wordpress User Meta: user_nicename

CAS User Attribute:

- user_email|email
- user_nicename|displayName
- display_name|displayName

Double click on rule in list to edit it.

Add Attribute Mapping | Remove Attribute Mapping

Save options

Step 4: Test CAS Authentication

Verify the integration works by logging into WordPress via Casdoor:

1. Log out of the WordPress Admin Dashboard (if logged in).
2. Access the WordPress login page (<http://<wordpress-server-ip>/wp-admin/index.php>).
3. You'll be redirected to the Casdoor login page. Enter valid Casdoor user credentials.
4. After successful authentication, Casdoor will redirect you back to WordPress—you should now be logged in (as the synced user).

127.0.0.1:8167/wp-admin/profile.php

攻击25 home Howdy, alice

Dashboard Profile Collapse menu

Toolbar Show Toolbar when viewing site

Language Site Default

Name

Username Usernames cannot be changed.

First Name

Last Name

Nickname (required)

Display name publicly as

Contact Info

Email (required)
If you change this, an email will be sent at your new address to confirm it. The new address will not become active until confirmed.

Website

About Yourself

Biographical Info

Share a little biographical information to fill out your profile. This may be shown publicly.

The screenshot shows a WordPress profile edit screen. A red box highlights the 'Name' section, which includes fields for Username, First Name, Last Name, Nickname, and Display name publicly as. Below this is a 'Contact Info' section with an Email field containing '8op3zg@example.com'. The 'About Yourself' and 'Biographical Info' sections are also visible at the bottom.

禅道

Zentao是一个敏捷（scrum）项目管理系统/工具，但它本身不支持OIDC。要将Zentao与Casdoor SSO集成，我们需要使用一个名为[zentao-oidc](#)的第三方OIDC模块，本文档将向您展示如何操作。

步骤1：部署Casdoor和Zentao

首先，部署[Casdoor](#)和[Zentao](#)。成功部署后，请确保：

1. Casdoor 可以正常登录使用。
2. 您可以成功登录并使用Zentao。

步骤2：集成Zentao OIDC第三方模块

通过运行以下命令安装 [zentao-oidc](#)：

```
git clone https://github.com/casdoor/zentao-oidc.git
```

或者，您可以下载ZIP文件并解压它。

此模块用于将Zentao与OpenId的SSO进行集成。以下是如何使用它：

1. 将整个[oidc](#)目录复制到Zentao的模块中，并将其作为Zentao的一个模块使用。将下载的包重命名为“oidc”。
2. 配置过滤器。

由于Zentao框架会过滤URL中的参数并且不允许有空格，您需要将以下代码放在 `/config/my.php` 的末尾。

```
$filter->oidc = new stdclass();
$filter->oidc->index = new stdclass();
$filter->oidc->index->paramValue['scope'] = 'reg::any';
```

3. 修改 `/module/common/model.php`。

将 'oidc' 添加到匿名访问列表中，并在 `model.php` 的 `isOpenMethod` 方法中添加一行。

```
public function isOpenMethod($module, $method)
{
    if ($module == 'oidc' and $method == 'index') {
        return true;
    }
}
```

4. 如果你不希望看到Zentao的登录界面，可以直接前往Casdoor的登录界面。

修改 `/module/common/model.php` 中的 `public function checkPriv()` 的最后一行代码。

```
//返回 print(js::locate(helper::createLink('user', 'login',
"referer=$referer")));
返回 print(js::locate(helper::createLink('oidc', 'index',
"referer=$referer")));
```

5. 修改 `framework/base/router.class.php` 中的 `setSuperVars()` 方法，并注释掉以下语句。

```
public function setSuperVars()  
// unset($_REQUEST);
```

步骤3：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序，或使用一个已经存在的。
2. 添加您的重定向URL。

The screenshot shows the Casdoor application configuration interface. It includes fields for Client ID (d8d7715e24f077066a20), Client secret (redacted), Cert (cert-built-in), and Redirect URLs (http://127.0.0.1/zentao/oidc-index.html). There is also a 'Add' button for Redirect URLs.

Client ID ② :	d8d7715e24f077066a20				
Client secret ② :	[REDACTED]				
Cert ② :	cert-built-in				
Redirect URLs ② :	<table border="1"><tr><td>Redirect URLs</td><td>Add</td></tr><tr><td>Redirect URL</td><td>http://127.0.0.1/zentao/oidc-index.html</td></tr></table>	Redirect URLs	Add	Redirect URL	http://127.0.0.1/zentao/oidc-index.html
Redirect URLs	Add				
Redirect URL	http://127.0.0.1/zentao/oidc-index.html				

3. 添加您想要的提供商并填写其他所需设置。

步骤4：配置Zentao

在 `oidc` 目录中配置 `config.php` 文件。

```
$config->oidc->clientId = "<您的ClientId>";  
$config->oidc->clientSecret = "<您的ClientSecret>";  
$config->oidc->issuer = "http://localhost:8000";
```

在 `module/oidc` 中设置你的重定向URL，在 `public function index()` 方法中。

```
$oidc->setRedirectURL($path."/zentao/oidc-index.html");
```

① 备注

这里的URL是指调用 'index' 方法在 'oidc' 模块中。您还需要设置一个变量分隔符。默认情况下，框架使用破折号("-")。请参考官方的Zentao框架以获取更多详情。 "[zentaoPHP框架](#)"

在ShowDoc中使用Casdoor作为OAuth2服务器

在ShowDoc中使用Casdoor进行身份验证

ShowDoc是一个在线API文档和技术文档工具，非常适合IT团队使用。 ShowDoc使得使用Markdown语法编写美观的API文档、数据字典文档、技术文档、在线Excel文档等变得简单易行。

ShowDoc支持第三方认证，包括OAuth2。 这是一个实现此目标的教程。

步骤1：创建一个Casdoor应用

前往你的Casdoor并添加一个名为ShowDoc的新应用。 这是在Casdoor中创建ShowDoc应用程序的一个示例。

[Edit Application](#)[Save](#)[Save & Exit](#)Name [?](#) :

myApplication

Display name [?](#) :

myApplication

Logo [?](#) :URL [?](#) :https://cdn.casdoor.com/logo/casdoor-logo_1185x256.png

Preview:

Home [?](#) :Description [?](#) :Organization [?](#) :

built-in

Client ID [?](#) :

208d745196c23df9fd5b

Client secret [?](#) :

4c89f447af77bc276431ab885463ebcb8d6efc3c

Cert [?](#) :

cert-built-in

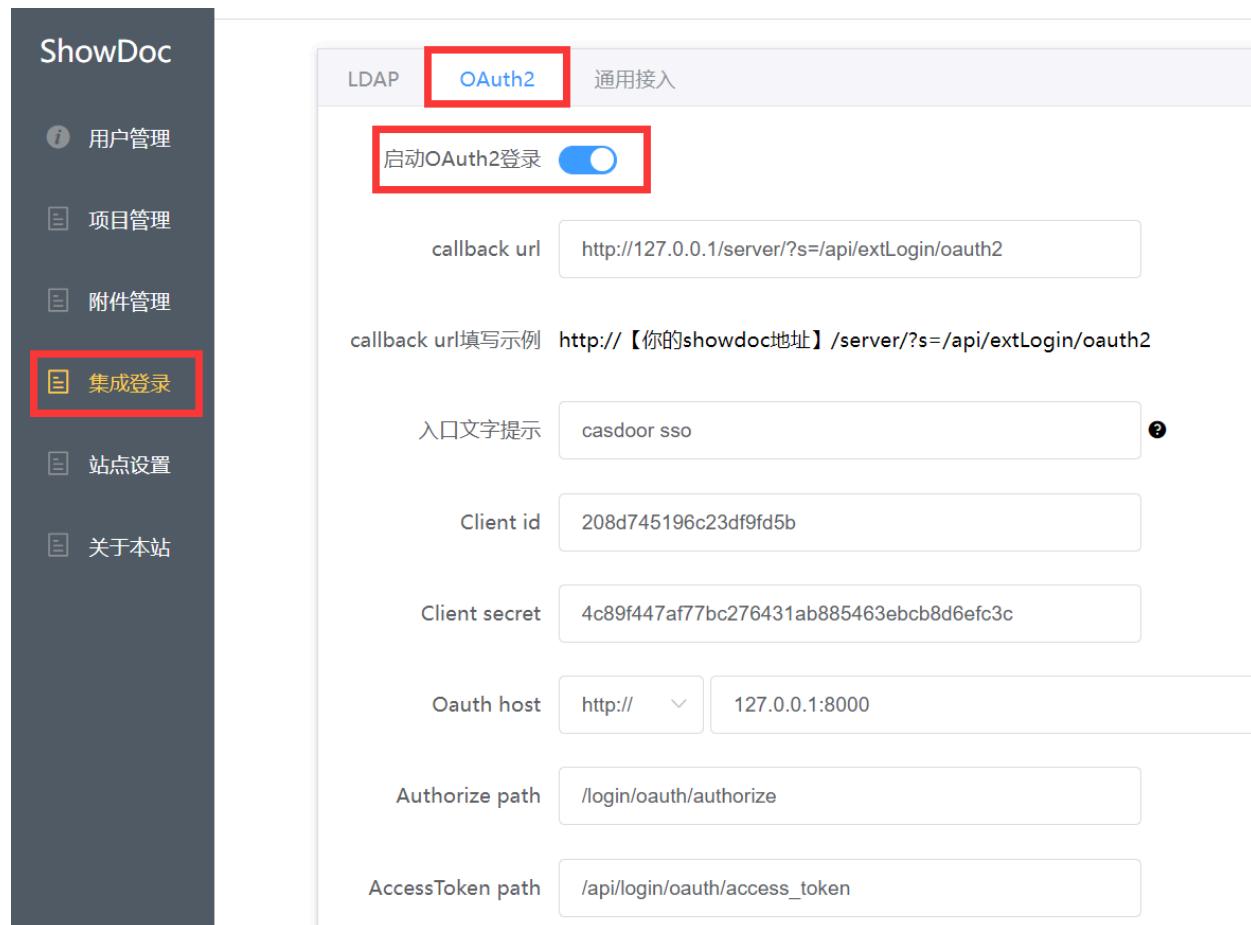
请记住下一步所需的[客户端 ID](#)和[客户端密钥](#)。

① 信息

请不要在此步骤中填写回调URL。 URL取决于下一步中ShowDoc的配置。 我们稍后会回来设置一个正确的回调URL。

步骤2：配置ShowDoc

首先，启用OAuth2登录按钮。然后，按照示例填写回调URL。在上一步中记住的client ID和client secret填入。



Authorize path、AccessToken path和User info path是必需的。您可以按照下面的示例来填写。

```
Authorize path: /login/oauth/authorize
AccessToken path: /api/login/oauth/access_token
User info path: /api/get-account
```

步骤3：在Casdoor中配置回调URL

返回到步骤1中的应用编辑页面，并添加你在ShowDoc中填写的回调URL。

The screenshot shows the 'Redirect URLs' configuration section in Casdoor. It includes a header 'Redirect URLs (2)', a 'Redirect URLs' button, an 'Add' button, a 'Redirect URL' input field containing the value 'http://127.0.0.1/server/?s=/api/extLogin/oauth2', and a small link icon next to the URL.

步骤4：尝试使用ShowDoc

你应该在登录页面上看到以下内容：

登录

 用户名/邮箱 密码 验证码[注册新账号](#)[casdoor sso](#)

恭喜您！ 您已完成所有步骤 按下'Casdoor SSO'按钮，您将被重定向到Casdoor登录页面。

Flarum

Casdoor可以使用OAuth2连接各种应用程序。 在这个例子中，我们将向您展示如何使用OAuth2将Flarum连接到您的应用程序。

以下是您需要的一些配置名称：

`CASDOOR_HOSTNAME`: 部署Casdoor服务器的域名或IP。

`Flarum_HOSTNAME`: 部署Flarum的域名或IP。

步骤1：部署Casdoor和Flarum

首先，部署Casdoor和Flarum。

成功部署后，请确保：

1. 您已经下载了Flarum插件[FoF Passport](#)。
2. Casdoor可以正常登录和使用。
3. 在`prod`模式下部署Casdoor时，您可以设置`CASDOOR_HOSTNAME = http://localhost:8000`。查看[生产模式](#)。

步骤2：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序或使用现有的一个。
2. 找到重定向URL：`<CASDOOR_HOSTNAME>/auth/passport`。
3. 将重定向URL添加到Casdoor应用程序：

The screenshot shows the Casdoor application settings page. It includes fields for 'Client ID' (014ae4bd048734ca2dea), 'Client secret' (f26a4115725867b7bb7b668c81e1f8fffae1544d), 'Cert' (cert-built-in), and a 'Redirect URLs' section containing a single entry: <your flarum install>/auth/passport.

在应用程序设置页面上，您会找到两个值：`Client ID` 和 `Client secret`。我们将在下一步中使用这些值。

打开您最喜欢的浏览器并访问：`http://CASDOOR_HOSTNAME.well-known/openid-configuration`。您将看到Casdoor的OIDC配置。

步骤3：配置Flarum

1. 安装插件[FoF Passport](#)。
2. 配置应用程序：

The screenshot shows the configuration page for the FoF Passport extension in Casdoor. At the top, there is a logo for 'FoF Passport' and a status indicator showing it is 'Enabled'. Below this, there are several configuration fields:

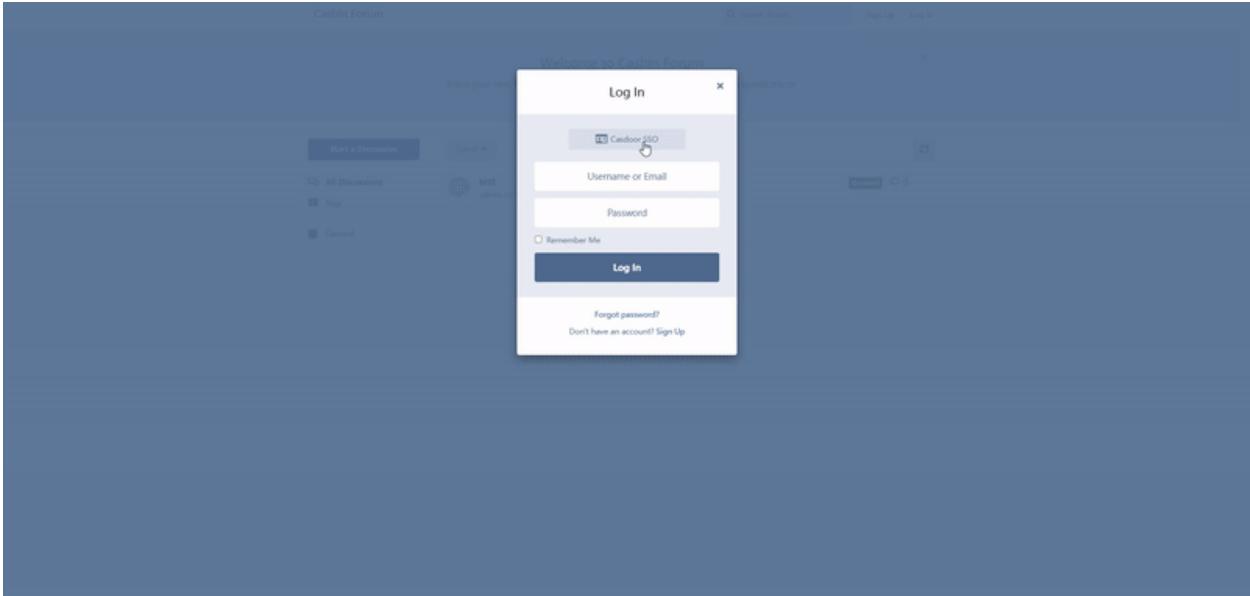
- OAuth authorization URL:** https://door.casdoor.com/login/oauth/authorize
- OAuth token URL:** https://door.casdoor.com/api/login/oauth/access_token
- Api URL providing user details when authenticated:** https://door.casdoor.com/api/user
- OAuth application ID:** 014ae4bd048734ca2dea
- OAuth application secret:** f26a4115725867b7bb7b668c81e1f8f7fae1544d
- OAuth scopes to request:** openid profile email
- Label for login button:** Casdoor SSO
- Icon for login button:** far fa-id-card

A blue 'Save Changes' button is located at the bottom left of the configuration area.

3. 在Casdoor应用程序页面中找到Client ID和Client Secret。

- Token server URL: http://**CASDOOR_HOSTNAME**/api/login/oauth/access_token
- Authorization server URL: http://**CASDOOR_HOSTNAME**/login/oauth/authorize
- UserInfo server URL: http://**CASDOOR_HOSTNAME**/api/get-account
- Scopes: address phone openid profile offline_access email

退出Flarum并测试SSO。



Moodle

Casdoor可以用来使用OAuth连接Moodle。

以下是一些配置设置：

- `CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。
- `Moodle_HOSTNAME`：部署Moodle的域名或IP。

步骤1：部署Casdoor和Moodle

首先，部署Casdoor和Moodle。

成功部署后，确保以下内容：

1. Casdoor可以登录并无问题地使用。
2. 在`prod`模式下部署Casdoor时，您可以将`CASDOOR_HOSTNAME`设置为`http://localhost:8000`。查看[生产模式](#)。

步骤2：配置Casdoor应用程序

1. 创建一个新的Casdoor应用程序或使用现有的一个。
2. 找到重定向URL：`Moodle_HOSTNAME/admin/oauth2callback.php`。
3. 将重定向URL添加到Casdoor应用程序。

有关OAuth的更多信息，请参阅[OAuth](#)。

步骤3：配置Moodle

1. 定位OAuth

The screenshot shows the Moodle Site administration interface. The 'Server' tab is selected. A red arrow points to the 'OAuth 2 services' link under the 'Server' category. A message at the top states 'Your site is not yet registered.' with a 'Register your site' button.

2. 配置此应用程序

The screenshot shows the 'Detailed instructions on configuring the common OAuth 2 services' section. It lists various configuration fields with their corresponding values for the Casdoor application. Red arrows point from the input fields to their respective placeholder text: 'Client ID' to 'your Client ID', 'Client secret' to 'your Client secret', 'Service base URL' to 'your Casdoor Home', and 'Logo URL' to 'https://cdn.casdoor.com/s'. Other fields shown include 'Name' (Casdoor), 'This service will be used' (Login page and internal services), 'Scopes included in a login request' (openid profile email), 'Scopes included in a login request for offline access' (openid profile email), 'Additional parameters included in a login request.', 'Additional parameters included in a login request for offline access.', 'Login domains', and two checkboxes for email verification.

3. 配置此映射

User field mappings for issuer: Casdoor

External field name	Internal field name	Edit
address	address	
email	email	
name	firstname	
phone	phone1	
picture	picture	
preferred_username	username	

Create new user field mapping for issuer "Casdoor"

o

4. 定位OAuth2插件

General Users Courses Grades **Plugins** Appearance Server Reports Development

Your site is not yet registered. [Register your site](#)

Plugins [Install plugins](#) [Plugins overview](#)

Activity modules

- [Manage activities](#)
- [Common activity settings](#)
- [Assignment](#)
- [Assignment settings](#)
- [Submission plugins](#)
- [Manage assignment submission plugins](#)
- [File submissions](#)
- [Online text submissions](#)
- [Feedback plugins](#)
- [Manage assignment feedback plugins](#)
- [Feedback comments](#)
- [Annotate PDF](#)
- [File feedback](#)
- [Offline grading worksheet](#)
- [Book](#)
- [Chat](#)
- [Database](#)
- [External tool](#)
- [Manage tools](#)
- [Feedback](#)
- [File](#)
- [Folder](#)
- [Forum](#)
- [Glossary](#)
- [HSP](#)
- [IMS content package](#)
- [Lesson](#)
- [Page](#)
- [Quiz](#)
- [General settings](#)
- [Safe Exam Browser templates](#)
- [Safe Exam Browser access rules](#)
- [SCORM package](#)
- [Text and media area](#)
- [URL](#)
- [Workshop](#)

Admin tools

- [Manage admin tools](#)
- [Accessibility](#)
- [Brickfield registration](#)
- [Accessibility toolkit settings](#)
- [Reports](#)
- [Recycle bin](#)

Antivirus plugins [Manage antivirus plugins](#)

Authentication [Manage authentication](#)

- [Email-based self-registration](#)
- [Manual accounts](#)
- [OAuth 2](#)

5. 启用OAuth2插件

Manage authentication

Available authentication plugins

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	2			Settings		
No login	0					
Email-based self-registration	0	⊕	↓	Settings		Uninstall
OAuth 2	8	⊕	↑	Settings	Test settings	

6. 如果你想阻止编辑Casdoor的电子邮件

Lock user fields

You can lock user data fields. This is useful for sites where the user data is maintained by the administrators manually by editing user records or uploading using the 'Upload users' facility. If you are locking fields that are required by Moodle, make sure that you provide that data when creating user accounts or the accounts will be unusable.

Consider setting the lock mode to 'Unlocked if empty' to avoid this problem.

Lock value (First name) auth_oauth2 field_lock_firstname	<input type="button" value="Unlocked"/> Default: Unlocked
Lock value (Last name) auth_oauth2 field_lock_lastname	<input type="button" value="Unlocked"/> Default: Unlocked
Lock value (Email address) auth_oauth2 field_lock_email	<input type="button" value="Locked"/> Default: Unlocked
Lock value (City/town) auth_oauth2 field_lock_city	<input type="button" value="Unlocked"/> Default: Unlocked
Lock value (Country) auth_oauth2 field_lock_country	<input type="button" value="Unlocked"/> Default: Unlocked
Lock value (Language) auth_oauth2 field_lock_lang	<input type="button" value="Unlocked"/> Default: Unlocked

here is switch to lock email

有关Moodle的更多信息，请参阅[Moodle](#)和[字段映射](#)。

退出Moodle并测试SSO。

MyMoodle Website





>

集成

>

Ruby

Ruby



GitLab

在自行开发的GitLab服务器中使用Casdoor进行身份验证

GitLab

Casdoor可以使用OIDC协议链接到自部署的GitLab服务器，本文档将向您展示如何操作。

⚠ 注意事项

正如[GitLab文档](#)所述，GitLab只能与使用HTTPS的OpenID提供商一起工作，因此你需要使用HTTPS部署Casdoor，例如将Casdoor放在配置了SSL证书的NGINX反向代理后面。Casdoor本身默认只通过HTTP在8000端口监听，没有HTTPS相关功能。

以下是在配置中提到的一些名称：

`CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP，例如，
`https://door.casbin.com`。

`GITLAB_HOSTNAME`：部署GitLab的域名或IP，例如，`https://gitlab.com`。

步骤1：部署Casdoor和GitLab

首先，应部署Casdoor和GitLab。

成功部署后，您需要确保：

1. Casdoor可以正常登录和使用。
2. 将Casdoor的`origin`值(`conf/app.conf`)设置为`CASDOOR_HOSTNAME`。

```
conf > ⚙ app.conf
 8  dbName = casdoor
 9  redisEndpoint =
10 defaultStorageProvider =
11 isCloudIntranet = false
12 authState = "casdoor"
13 httpProxy = "127.0.0.1:10808"
14 verificationCodeTimeout = 10
15 initScore = 2000
16 logPostOnly = true
17 origin = "http://10.144.1.2:8000"| CASDOOR_HOSTNAME
```

步骤2：配置Casdoor应用程序

1. 创建或使用现有的 Casdoor 应用程序。
2. 添加一个重定向URL: http://GITLAB_HOSTNAME/users/auth/openid_connect/callback。
3. 添加您想要的提供者并补充其他设置。

Description ② :	GitLab	
Organization ② :	built-in	
Client ID ② :	eab9...35b6	Client ID
Client secret ② :	95e7...b3a0188a5	Client secret
Redirect URLs ② :	Redirect URLs Add	
Redirect URL		
http://GITLAB_HOSTNAME/users/auth/openid_connect/callback		GitLab redirect url

值得注意的是，您可以在应用设置页面上获取两个值：[Client ID](#) 和 [Client secret](#)（参见上图），我们将在下一步中使用它们。

打开你最喜欢的浏览器并访问: [http://**CASDOOR_HOSTNAME**.well-known/openid-configuration](http://CASDOOR_HOSTNAME.well-known/openid-configuration), 在那里你将看到Casdoor的OIDC配置。

步骤3：配置GitLab

You can follow the steps below to set this up, or make custom changes according to [this document](#) (e.g., if you are installing GitLab using source code rather than the Omnibus).

1. 在 GitLab 服务器上, 打开配置文件。

```
sudo editor /etc/gitlab/gitlab.rb
```

2. 添加提供商配置。 (HOSTNAME URL应包含http或https)

```
gitlab_rails['omniauth_providers'] = [
  {
    name: "openid_connect",
    label: "Casdoor", # 可选的登录按钮标签, 默认为 "Openid Connect"
    args: {
      name: "openid_connect",
      scope: ["openid", "profile", "email"],
      response_type: "code",
      issuer: "<CASDOOR_HOSTNAME>",
      client_auth_method: "query",
      discovery: true,
      uid_field: "preferred_username",
      client_options: {
        identifier: "<YOUR CLIENT ID>",
        secret: "<YOUR CLIENT SECRET>",
        redirect_uri: "<GITLAB_HOSTNAME>/users/auth/openid_connect/callback"
      }
    }
  }
]
```

3. 重新启动 GitLab 服务器。
4. 每个已注册用户都可以打开 `GITLAB_HOSTNAME/-/profile/account` 并连接 Casdoor 账户。

The screenshot shows the 'User Settings > Account' page in GitLab. On the left, there's a sidebar with options like Profile, Account (which is selected), Applications, Chat, Access Tokens, Emails, Password, Notifications, SSH Keys, GPG Keys, and Preferences. The main content area has sections for 'Two-Factor Authentication' (Status: Disabled) and 'Social sign-in'. Under 'Social sign-in', it says 'Activate signin with one of the following services' and shows a 'Connect Casdoor' button, which is highlighted with a red box.

5. 完成！现在，您可以使用 Casdoor 登录到您自己的 GitLab。

The screenshot shows the GitLab login page. It features the GitLab logo and the text 'A complete DevOps platform'. Below that, it says 'GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.' A note indicates 'This is a self-managed instance of GitLab.' To the right is the login form with fields for 'Username or email' and 'Password', and checkboxes for 'Remember me' and 'Forgot your password?'. Below the form is a link 'Don't have an account yet? Register now'. At the bottom, there's a 'Sign in with' section containing a 'Casdoor' button, which is highlighted with a red box.



> 集成 >

Haskell

Haskell



Hasura

在集成之前，我们需要在本地部署Casdoor。

Hasura

在集成之前，我们需要在本地部署Casdoor。

然后我们可以按照以下步骤在我们自己的应用中快速实现基于Casdoor的登录页面。

配置Casdoor应用程序

1. 创建或使用现有的Casdoor应用程序。
2. 添加一个重定向URL: `http://CASDOOR_HOSTNAME/login`



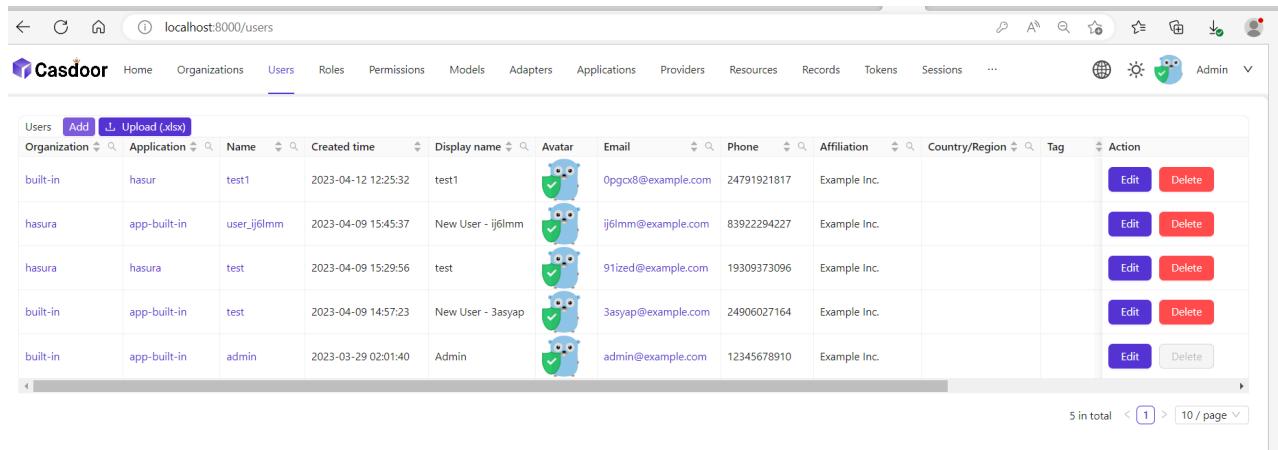
The screenshot shows the 'Redirect URLs' section of the Casdoor configuration interface. It has a single entry: 'Redirect URL' set to '`http://localhost:8080/login`'. There are buttons for 'Edit' and 'Delete' at the bottom right.

3. 复制客户端ID；我们将在接下来的步骤中需要它。

在Casdoor中添加一个用户

现在你有了应用程序，但没有用户。这意味着你需要创建一个用户并分配角色。

转到“用户”页面，然后点击右上角的“添加用户”。这将打开一个新页面，您可以在其中添加新用户。



The screenshot shows the 'Users' management page in Casdoor. It lists five users with the following details:

Organization	Application	Name	Created time	Display name	Avatar	Email	Phone	Affiliation	Country/Region	Tag	Action
built-in	hasur	test1	2023-04-12 12:25:32	test1		0pgcx8@example.com	24791921817	Example Inc.			<button>Edit</button> <button>Delete</button>
hasura	app-built-in	user_ij6lmm	2023-04-09 15:45:37	New User - ij6lmm		ij6lmm@example.com	83922294227	Example Inc.			<button>Edit</button> <button>Delete</button>
hasura	hasura	test	2023-04-09 15:29:56	test		91ized@example.com	19309373096	Example Inc.			<button>Edit</button> <button>Delete</button>
built-in	app-built-in	test	2023-04-09 14:57:23	New User - 3asyap		3asyap@example.com	24906027164	Example Inc.			<button>Edit</button> <button>Delete</button>
built-in	app-built-in	admin	2023-03-29 02:01:40	Admin		admin@example.com	12345678910	Example Inc.			<button>Edit</button> <button>Delete</button>

At the bottom, it says '5 in total' and has navigation buttons for page 1 of 10.

在添加用户名并添加Hasura组织（其他详细信息可选）后保存用户。

现在你需要为你的用户设置一个密码，你可以通过点击“管理你的密码”来做到这一点。

为您的用户选择一个密码并确认。

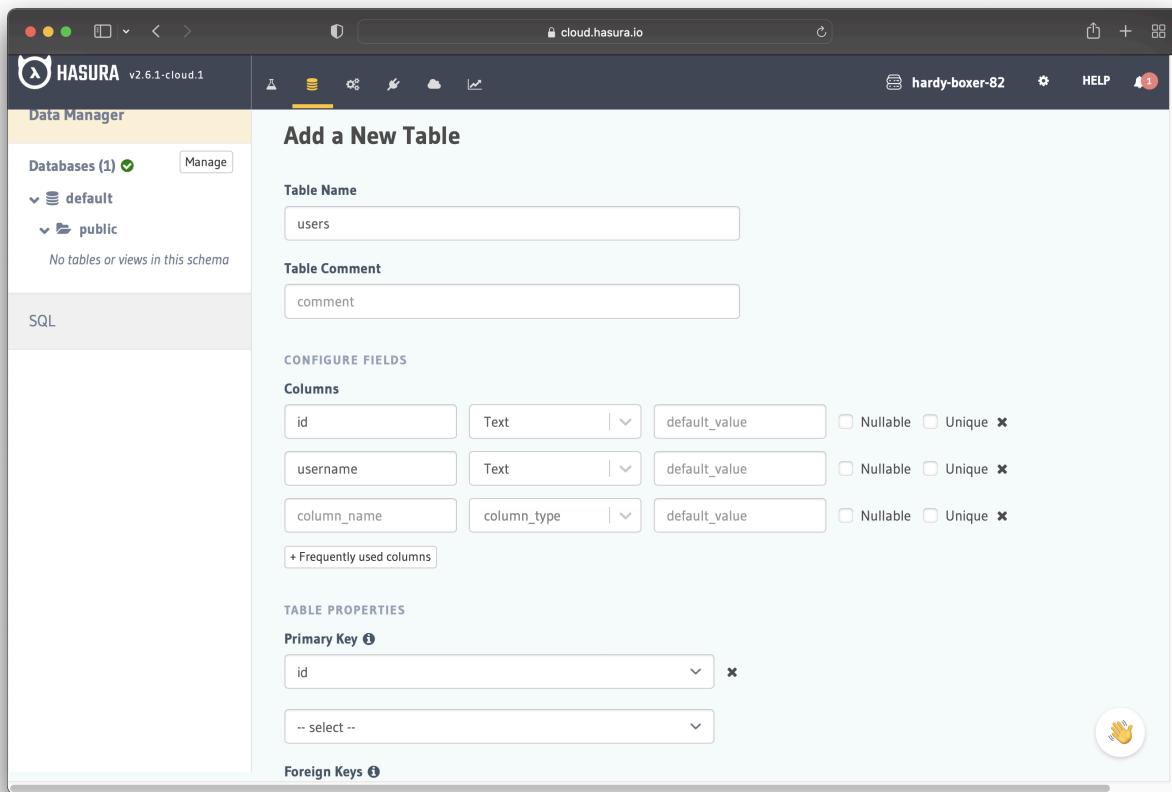
构建Hasura应用

通过Docker或Hasura Cloud启动Hasura。

现在创建一个带有以下列的 `users` 表:

- `id` 类型为文本（主键）
- `username` 类型为文本

参考下面的图片作为参考。



下一步是为应用创建一个 `user` 角色。 用户应该只能看到他们自己的记录，而不能看到其他人的记录。

按照下图所示配置 `user` 角色。 For more information, read about [configuring permission rules in Hasura](#).

The screenshot shows the Hasura Cloud interface with the 'DATA' tab selected. A table lists roles and their permissions:

Role	insert	select	update	delete
admin	✓	✓	✓	✓
user	✗	✗	✗	✗

Below the table, under 'Role: user Action: select', there is a section titled 'Row select permissions' with a note '- with custom check'. It shows a JSON query:

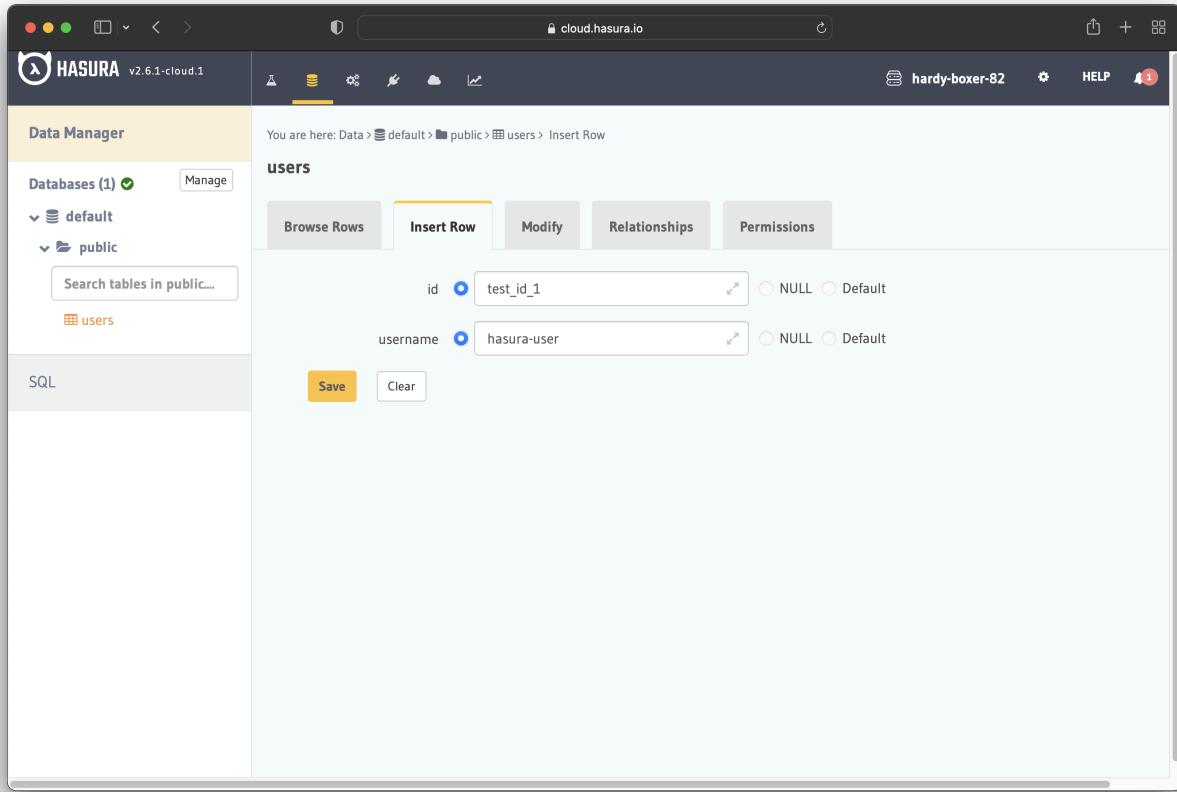
```
1  {"id": {"_eq": "X-Hasura-User-Id"}}

{
  "id": {
    "eq": "X-Hasura-User-Id"
  }
}
```

Under 'Column select permissions', it says '- all columns' and shows 'Allow role user to access columns' with checkboxes for 'id' (checked) and 'username'.

这样，用户就不能读取其他人的记录。他们只能访问他们自己的。

出于测试目的，添加一个虚拟用户。这是为了确保当你使用JWT令牌时，你只能看到你自己的用户详情，而不能看到其他用户的详情。



现在你需要在Hasura中设置`JWT_SECRET`。

用Casdoor配置Hasura

在这一步，你需要将`HASURA_GRAPHQL_JWT_SECRET`添加到Hasura。

为此，转到Hasura docker-compose.yaml，然后按照下面的方式添加新的`HASURA_GRAPHQL_JWT_SECRET`。

`HASURA_GRAPHQL_JWT_SECRET`应该是以下格式。记住将`<Casdoor endpoint>`更改为你自己的Casdoor的URL（如`https://door.casdoor.com`）

```
HASURA_GRAPHQL_JWT_SECRET: '{"claims_map": {  
    "x-hasura-allowed-roles": {"path": "$.roles"},  
    "x-hasura-default-role": {"path": "$.roles[0]"},  
    "x-hasura-user-id": {"path": "$.id"}  
}, "jwk_url": "<Casdoor endpoint>/.well-known/jwks"}'
```

保存更改并重新加载docker。

```
## enable debugging mode. It is recommended to disable this in production
HASURA_GRAPHQL_DEV_MODE: "true"
HASURA_GRAPHQL_ENABLED_LOG_TYPES: startup, http-log, webhook-log, websocket-log, query-log
HASURA_GRAPHQL_ADMIN_SECRET: myadminsecretkey
HASURA_GRAPHQL_JWT_SECRET: '{"claims_map": {
  "x-hasura-allowed-roles": ["user", "editor"],
  "x-hasura-default-role": "user",
  "x-hasura-user-id": "4ec7ccee-ec7b-4191-a78d-e11f50686f8b"
}, "jwk_url": "https://door.casdoor.com/.well-known/jwks"}
```

获取JWT令牌

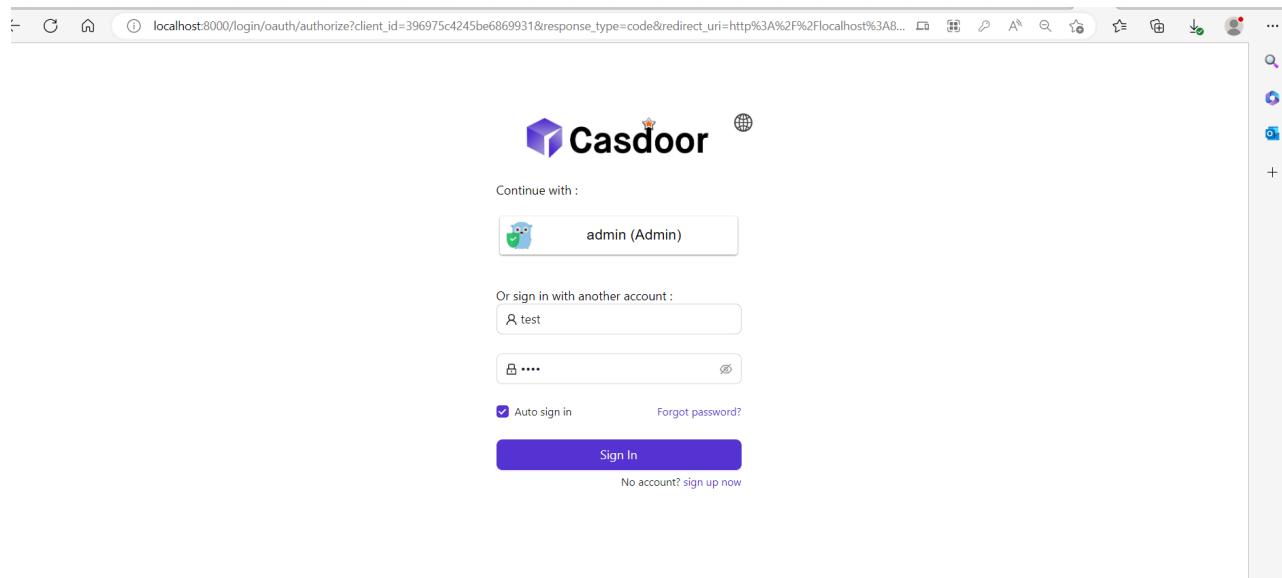
由于没有客户端实现，你可以通过以下URL获取你的访问令牌：

```
http://localhost:8000/login/oauth/authorize?client\_id=<client ID>&response\_type=code&redirect\_uri=http%3A%2F%2Flocalhost%3A8080%2Flogin&scope=read&state=app-built-in<public certificate>
```

将client ID更改为你之前复制的ID，并输入Casdoor的公共证书，你可以在Casdoor的Certs页面中找到。

然后输入你之前为Hasura创建的用户名和密码。

点击“登录”



返回到Casdoor/Token页面。

localhost:8000/tokens

Name	Created time	Application	Organization	User	Authorization code	Access token	Action
b6ea3e35-abcf-41d8-a1a2-01f00fd8264b	2023-04-12 13:06:53	hasura	hasura	test	433b504b4f6a593e4a11	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
16024557-df21-4779-bfb9-959e5dae078c	2023-04-12 12:51:47	hasura	built-in	test1	2879fbcc282019cf7f23c	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
f3cb1070-c2d4-40f0-8bc0-59919d26d162	2023-04-11 15:04:00	hasura	hasura	test	2a370971798d403fc6ef	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
64993582-2322-4df7-ab20-cb23201bc77b	2023-04-11 00:37:22	springboot	built-in	admin	a2396037c3ba4fd9221e	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
f65a3813-a655-47f0-9c9a-f08ce4607815	2023-04-11 00:31:37	springboot	built-in	admin	d048c7f9cd1469fd829d	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
5828069e-15eb-4c92-933c-feeda8ed621c	2023-04-11 00:06:54	springboot	built-in	admin	7cc27dc752cc4188ac8d	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
2277e0f2-7e78-462f-a654-3c53759784af	2023-04-11 00:05:17	springboot	built-in	admin	56141e709a06931b7faa	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
55bd324a-6039-40f6-b707-255d78ae911	2023-04-11 00:05:07	springboot	built-in	admin	9a1413bc172591a64353	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>
4b30acbe-fa22-4387-8098-9a46e70f6972	2023-04-10 23:59:19	springboot	built-in	admin	88b0997b675917f20fdc	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0e	<button>Edit</button> <button>Delete</button>

找到你之前输入的用户名，然后点击“编辑”

复制访问令牌

Edit Token		<button>Save</button>	<button>Save & Exit</button>
Name:	b6ea3e35-abcf-41d8-a1a2-01f00fd8264b		
Application:	hasura		
Organization:	hasura		
User:	test		
Authorization code:	433b504b4f6a593e4a11		
Access token:	eyJhbGciOiJSUzI1NlsltmpZC16ImNlcnQtYnVpbHQtaW4iLCj0eXAIoJKV1QiQeyJvd25lci6lmhhc3VYSlslm5hbWUiOj0ZXN0IwiY3JlYXRIZFRpbWUiOilyMDIzLTA0LTAsVDE1OjI5OjU2KzA4OjAwIwidXBkYXRIZFRpbWUiOiiLCjPZC16jRly		
Expires in:	604800		
Scope:	read		
Token type:	Bearer		
<button>Save</button>		<button>Save & Exit</button>	

现在你可以使用访问令牌来发出经过身份验证的请求。 Hasura返回了适当的用户，而不是从数据库返回所有用户。

HASURA v2.22.0 API DATA ACTIONS REMOTE SCHEMAS EVENTS SETTINGS HELP Allow List

GraphQL REST

> GraphQL Endpoint
Request Headers

ENABLE	KEY	VALUE
<input type="checkbox"/>	Hasura-Client-Name	casdoor
<input checked="" type="checkbox"/>	content-type	application/json
<input type="checkbox"/>	x-hasura-admin-secret	*****
<input checked="" type="checkbox"/>	Authorization	Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6ImNlcnQtYnVpbHQtaW4iLCJ0eXAiOiJV1QfQeyJvd25ci6lmhhc3VyYSlsIm5hbWL
Enter Key		Enter Value

Explorer X GraphiQL ▶ Prettify History Explorer Code Exporter REST Derive action Analyze ◀ Docs

query MyQuery {
 users {
 id
 username
 }
}

1
2
3
4
5
6
7

{
 "data": {
 "users": [
 {
 "id": "4ec7ccce-ec7b-4191-a78d-e11f50686f8b",
 "username": "test"
 }
]
 }
}

QUERY VARIABLES

Python



JumpServer

使用CAS连接JumpServer

JumpServer

Casdoor可以用来连接JumpServer。

以下是配置中的一些名称：

`CASDOOR_HOSTNAME`：部署Casdoor服务器的域名或IP。

`JumpServer_HOSTNAME`：部署JumpServer的域名或IP。

步骤1：部署Casdoor和JumpServer

首先，部署Casdoor和JumpServer。

部署成功后，请确保以下内容：

1. Casdoor可以正常登录和使用。
2. 在`prod`模式下部署Casdoor时，可以将`CASDOOR_HOSTNAME`设置为
`http://localhost:8000`。查看[生产模式](#)。

步骤2：配置Casdoor应用

1. 创建一个新的Casdoor应用或使用现有的应用。
2. 找到一个重定向URL：`CASDOOR_HOSTNAME/cas/你的组织/你的应用/login`。
3. 将你的重定向URL添加到Casdoor应用：`JumpServer_HOSTNAME`。

有关[CAS](#)的更多信息，请参考文档。

步骤3：配置JumpServer

1. 找到Auth:

The screenshot shows the 'Auth' configuration page in the JumpServer web interface. The left sidebar has a 'Auth' link highlighted with a red arrow. The main content area has a 'CAS' tab highlighted with a red arrow. The 'Basic' section contains fields for 'Server url' (http://101.43.192.216:8000/cas/jump/jumpServer/login), 'Proxy server url' (http://8.140.18.157), and 'Version' (3). The 'Other' section contains a 'Logout completely' toggle switch and a 'User attr map' code editor containing the following JSON:

```
1 = [
2   "uid": "username"
3 ]
```

Below the code editor are 'Create user if not' and 'Submit' buttons.

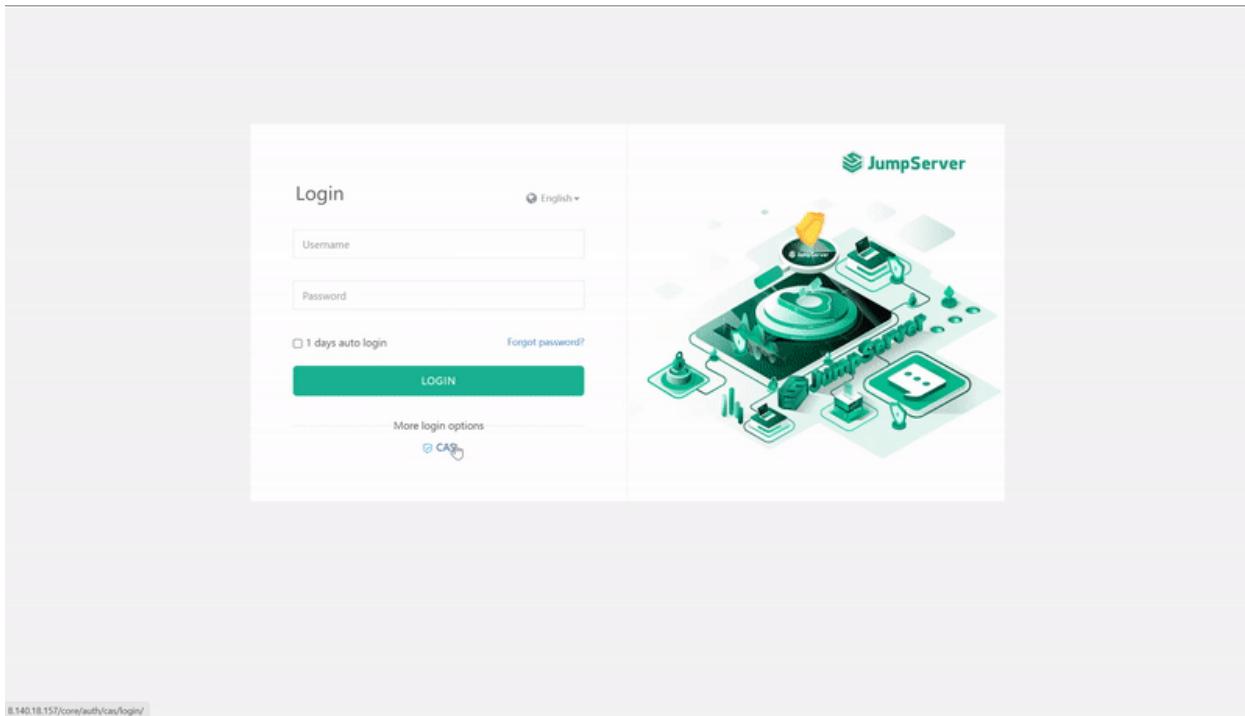
2. 配置此应用：

The screenshot shows the same 'Auth' configuration page as the previous one, but with additional red annotations. Red arrows point to the 'Enable CAS Auth' toggle switch, the 'Server url' field, and the 'User attr map' code editor. Above the 'Enable CAS Auth' switch is the label 'your casdoor'. Above the 'Server url' field is the label 'your orgnazition'. Above the 'User attr map' code editor is the label 'your application'.

- /login 端点: <https://door.casdoor.com/cas/casbin/cas-java-app/login>。
- /logout 端点: <https://door.casdoor.com/cas/casbin/cas-java-app/logout>。
- /serviceValidate 端点: <https://door.casdoor.com/cas/casbin/cas-java-app/serviceValidate>。
- /proxyValidate 端点: <https://door.casdoor.com/cas/casbin/cas-java-app/proxyValidate>。

有关**CAS**和**JumpServer**的更多信息，请参考文档。

退出JumpServer并测试SSO:





>

监控

监控

Web UI

在Casdoor网页上监控运行时信息

Prometheus

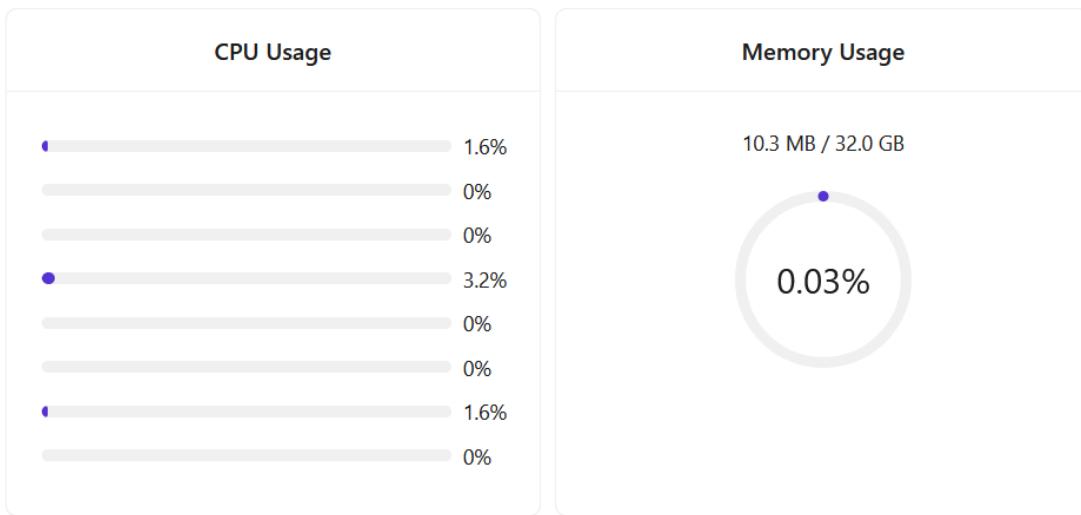
使用Prometheus收集有关运行Casdoor的信息。

Web UI

您可以在[Casdoor网页](#)上监控Casdoor的运行时信息，包括CPU使用率，内存使用率，API延迟和API吞吐量。

在UI上，您可以查看以下信息：

- CPU使用率和内存使用率



- API延迟，包括计数次数和平均延迟

API Latency				
Method	Endpoint	Latency (ms)	Avg Latency (ms)	Throughput (req/s)
GET	/api/get-cert	3	0.667	
GET	/api/get-certs	27	1.333	
GET	/api/get-chats	27	1.519	
GET	/api/get-default-application	3	5.333	
GET	/api/get-email-and-phone	1	1.000	
GET	/api/get-global-providers	58	1.202	

- API吞吐量，包括总吞吐量和每个API的吞吐量

API Throughput			
Total Throughput: 2			
Name	Method	Throughput	
/api/get-prometheus-info	GET	1	
/api/get-system-info	GET	1	

Prometheus

要收集Casdoor的运行时指标，如API吞吐量，API延迟，CPU使用率，内存使用率等，您需要配置您的Prometheus配置文件。

```
global:  
  scrape_interval: 10s # 获取指标的时间间隔  
  
scrape_configs:  
  - job_name: 'prometheus'  
    static_configs:  
      - targets: ['localhost:9090']  
  - job_name: 'casdoor' # 要监控的应用程序的名称  
    static_configs:  
      - targets: ['localhost:8000'] # Casdoor部署的后端地址  
    metrics_path: '/api/metrics' # 收集指标的路径
```

配置成功后，您将在Prometheus中找到以下信息：





>

国际化

国际化

Casdoor支持多种语言. 通过部署[Crowdin](#) 翻译, 我们可以提供 西班牙语、法语、德语、中文、印尼语、日语、韩语等等的支持.

Casdoor使用官方的 Crowdin cli 来同步Crowdin 的翻译。 如果您想要添加对其他语言的支持, 请提交您在 [社区](#) 中的提案。 此外, 如果您想要帮助我们加快翻译工作, 请考虑帮助我们翻译 [Crowdin](#)。



贡献者指南

欢迎使用 Casdoor！此文档作为如何为Casdoor做出贡献的指南。

如果您发现任何不正确或缺失的信息，请留下您的评论或建议。

参与其中

有许多方式可以为Casdoor做贡献。以下列出了一些贡献方式：

- 使用Casdoor并报告问题。在使用Casdoor时，如果遇到任何问题 - 无论是错误还是建议 - 请在[GitHub Discussions](#)或[Discord](#)上报告，然后再在GitHub上提交问题。

① 信息

在报告问题时，请使用英语详细描述您的问题。

- 帮助编写文档。开始从文档工作做起是一个好的选择。
- 帮助解决问题。我们有一个表格，其中包含适合初学者的简单任务，位于[Casdoor Easy Tasks](#)，并用不同的标签标记不同级别的挑战。

贡献

如果你准备创建一个PR，这里是贡献者的工作流程：

1. 将其分叉到你自己的仓库。

2. 将你的分支克隆到本地仓库。
3. 创建一个新的分支并在其上工作。
4. 保持你的分支同步。
5. 提交你的更改。 确保你的提交信息简洁明了。
6. 将你的提交推送到你的分叉仓库。
7. 创建从您的分支到我们的**master**分支的合并请求。

合并请求

在你开始之前

Casdoor以GitHub作为其开发平台，拉取请求是主要的贡献来源。

在开启拉取请求之前，你需要了解一些事情：

- 您首次创建拉取请求时，需要签署**CLA**。
- 解释为什么你要提交这个拉取请求，以及它将对仓库产生什么影响。
- 只允许一个提交。如果PR做的事情超过一件，请将其拆分。
- 如果有任何新添加的文件，请在新文件的顶部包含Casdoor许可证。

```
// Copyright 2022 The Casdoor Authors. All Rights Reserved.  
//  
// Licensed under the Apache License, Version 2.0 (the "License");  
// you may not use this file except in compliance with the License.
```

Semantic PRs

您的合并请求应遵循常规承诺的样本。 基本要求是有PR 标题或至少一个 提交消息。 例如，三个常用的PR标题如下：

⚠ 注意事项

PR标题必须为小写。

1. 修复：一个类型的提交 `fix` 修复了你的代码库中的一个错误。

```
fix: prevent racing of requests
```

2. 特性：一个类型的提交 `feat` 向代码库引入了一个新的功能。`

```
feat: allow provided config object to extend other configs
```

3. 文档：一个类型的提交 `docs` 添加或改进文档。

```
docs: correct spelling of CHANGELOG
```

有关更多详细信息，请参阅[Conventional Commits](#)页面。

将PRs与Issues关联

您可以将拉取请求链接到问题，以显示正在进行的修复，并在合并拉取请求时自动关闭问题。

使用关键词将拉取请求链接到问题

您可以通过在拉取请求说明或提交消息中使用支持的关键词将拉取请求链接到议题。 拉取请求**必须**在默认分支上。

- close
- fix
- resolve

例如，在同一个仓库中的一个问题：

```
Fix: #902
```

有关更多详细信息，请参阅[将 Pull Request 链接到问题](#)。

修改PRs

您的PR可能需要修改。 当代码需要更改时，请修改同一PR；不要关闭PR并开启一个新的。 这是一个例子：

- 在你的本地修改代码。
- 修改你的提交。

```
git commit --amend
```

- 推送代码到远程仓库

```
git push --force
```

然后，你就成功地修改了PR！

相关代码

一些原则：

- 可读性：重要的代码应该有良好的文档记录。代码风格应与现有的一致。

命名规则

例如，变量名使用 `signupUrl`，UI 使用 `Signup URL`。

如何更新i18n数据？

请注意，我们使用 [Crowdin](#) 作为翻译平台，使用 `i18next` 作为翻译工具。当你在 `web/` 目录中使用 `i18next` 添加字符串时，你可以运行 `i18n/generate_test.go` 来自动生成 `web/src/locales/**/data.json`。

运行 `i18n/generate_test.go`：

```
cd i18n && go test
```

默认情况下，所有语言都以英文填写。在你的PR被合并后，我们鼓励你帮助翻译新添加的字符串在 `web/src/locales/zh/data.json` 通过 [Crowdin](#)。

⚠ 注意事项

如果你对某种语言不熟悉，请不要翻译它；保持文件原样。

许可证书

通过向Casdoor做出贡献，您同意您的贡献将根据Apache许可证进行许可。